Cisco | Networking Academy®
Mind Wide Open™

CAPITULO I – "DISEÑO DE LAN"

1.0 INTRODUCCIÓN DEL CAPITULO.-

1.0.1 INTRODUCCIÓN DEL CAPITULO.-

Para pequeñas y medianas empresas, la comunicación digital de datos, voz y video es esencial para la supervivencia de la empresa. En consecuencia, una LAN con un diseño apropiado es un requisito fundamental para hacer negocios en el presente. El usuario debe ser capaz de reconocer una LAN bien diseñada y seleccionar los dispositivos apropiados para admitir las especificaciones de las redes de una empresa pequeña o mediana.

En este capítulo, el usuario comenzará a explorar la arquitectura de la LAN conmutada y algunos de los principios que se utilizan para diseñar una red jerárquica. El usuario aprenderá sobre las redes convergentes. También aprenderá cómo seleccionar el switch correcto para una red jerárquica y qué switches Cisco son los más adecuados para cada capa de red. Las actividades y los laboratorios confirman y refuerzan su aprendizaje.

En este capítulo aprenderá a:

- Describir cómo una red jerárquica admite las necesidades de voz, video y datos de una pequeña o mediana empresa.
- Describir las funciones de cada uno de los tres niveles del modelo de diseño de una red jerárquica, los pricipios de diseño de una red jerárquica (conectividad agregada, diámetro de la red y redundancia) y el concepto de una red convergente.
- Aportar ejemplos de cómo la voz y el video sobre IP afectan al diseño de la red.
- Seleccionar los dispositivos apropiados para operar en cada nivel de la jerarquía, incluyendo componentes de voz y video.
- Hacer coincidir el switch de Cisco adecuado con cada capa en el modelo de diseño de red jerárquica.

1.1 ARQUITECTURA DE LA LAN CONMUTADA.-

1.1.1 MODELO DE REDES JERÁRQUICAS.-

La construcción de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico. En comparación con otros diseños de redes, una red jerárquica se administra y expande con más facilidad y los problemas se resuelven con mayor rapidez.

El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo. Un ejemplo de diseño de red jerárquico de tres capas se observa en la figura.

Capa de acceso

La capa de acceso hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red. Esta capa de acceso puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.

Pase el mouse sobre el botón Acceso en la figura.

Capa de distribución

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales (VLAN) definidas en la capa de acceso. Las VLAN permiten al usuario segmentar el tráfico sobre un switch en subredes separadas. Por ejemplo, en una universidad el usuario podría separar el tráfico según se trate de profesores, estudiantes y huéspedes. Normalmente, los switches de la capa de distribución son dispositivos que presentan disponibilidad y redundancia altas para asegurar la fiabilidad. Aprenderá más acerca de las VLAN, los dominios de broadcast y el enrutamiento entre las VLAN, posteriormente en este curso.

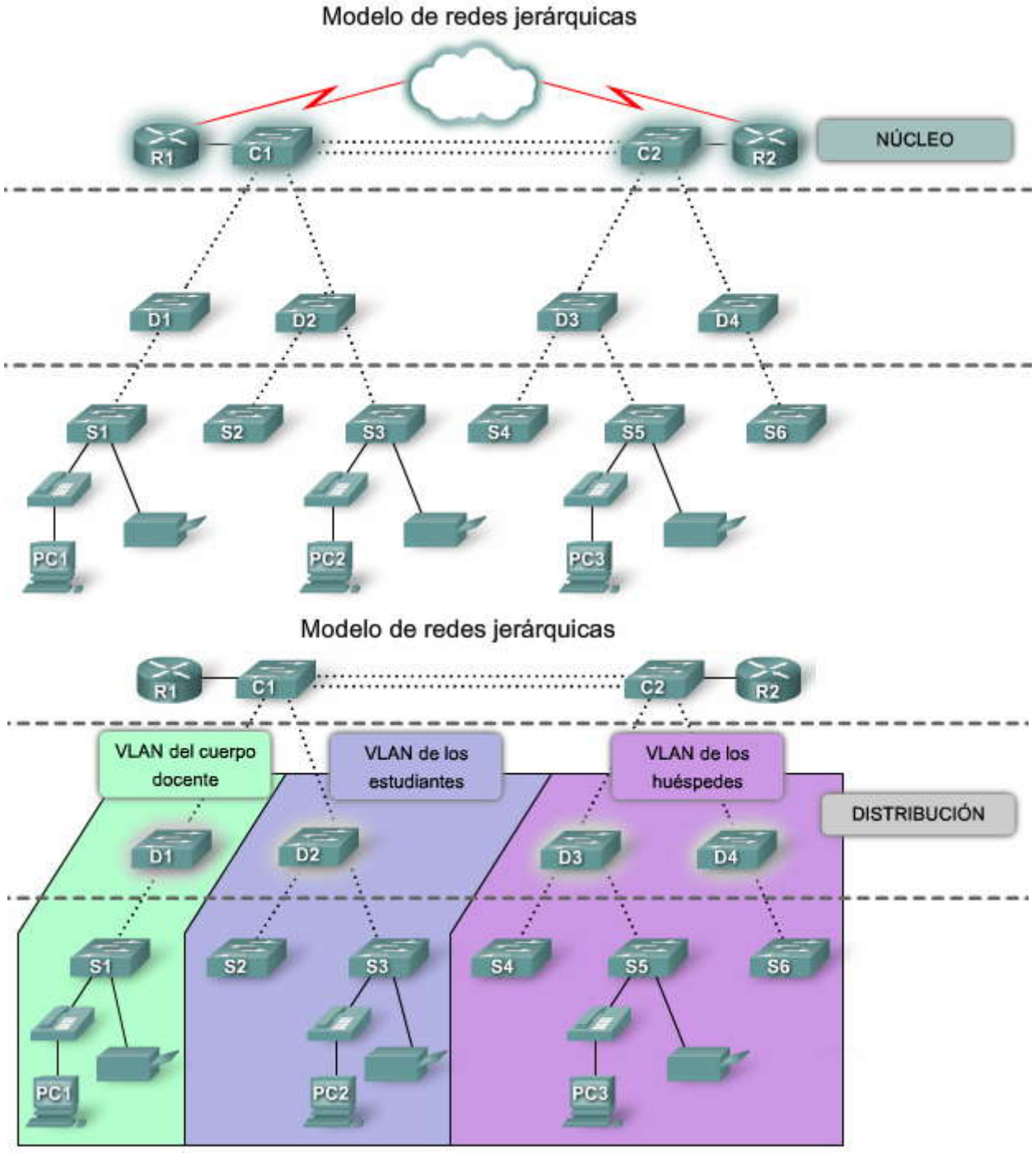
Pase el mouse sobre el botón Distribución en la figura.

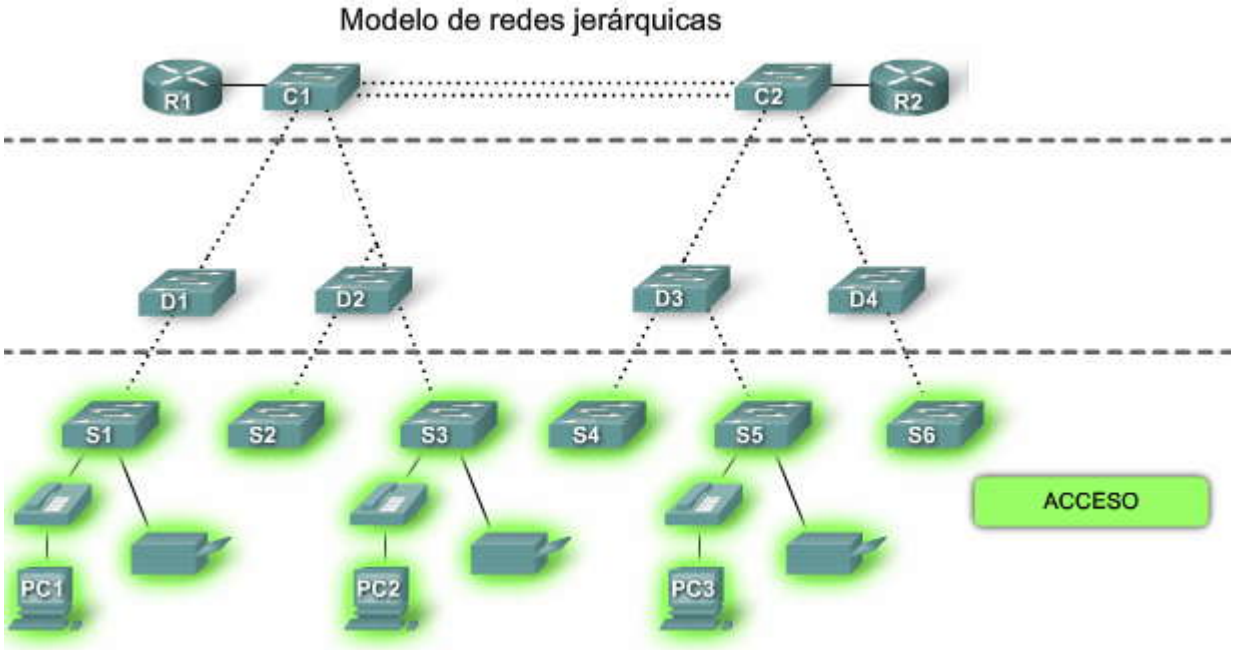
Capa núcleo

La capa núcleo del diseño jerárquico es la backbone de alta velocidad de la internetwork. La capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico

de todos los dispositivos de la capa de distribución, por lo tanto debe poder reenviar grandes cantidades de datos rápidamente.

Pase el mouse por el botón Núcleo en la figura.
Nota: En redes más pequeñas, no es inusual que se implemente un modelo de núcleo colapsado, en el que se combinan la capa de distribución y la capa núcleo en una capa.





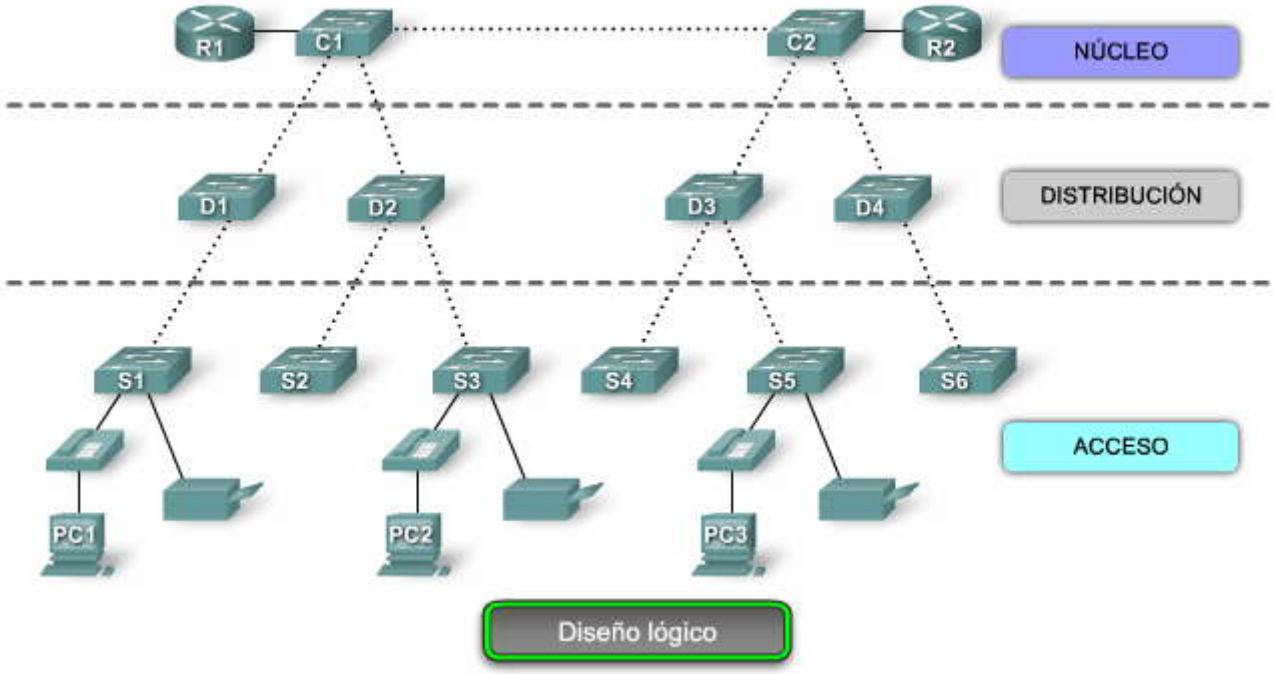
Red jerárquica en una empresa mediana

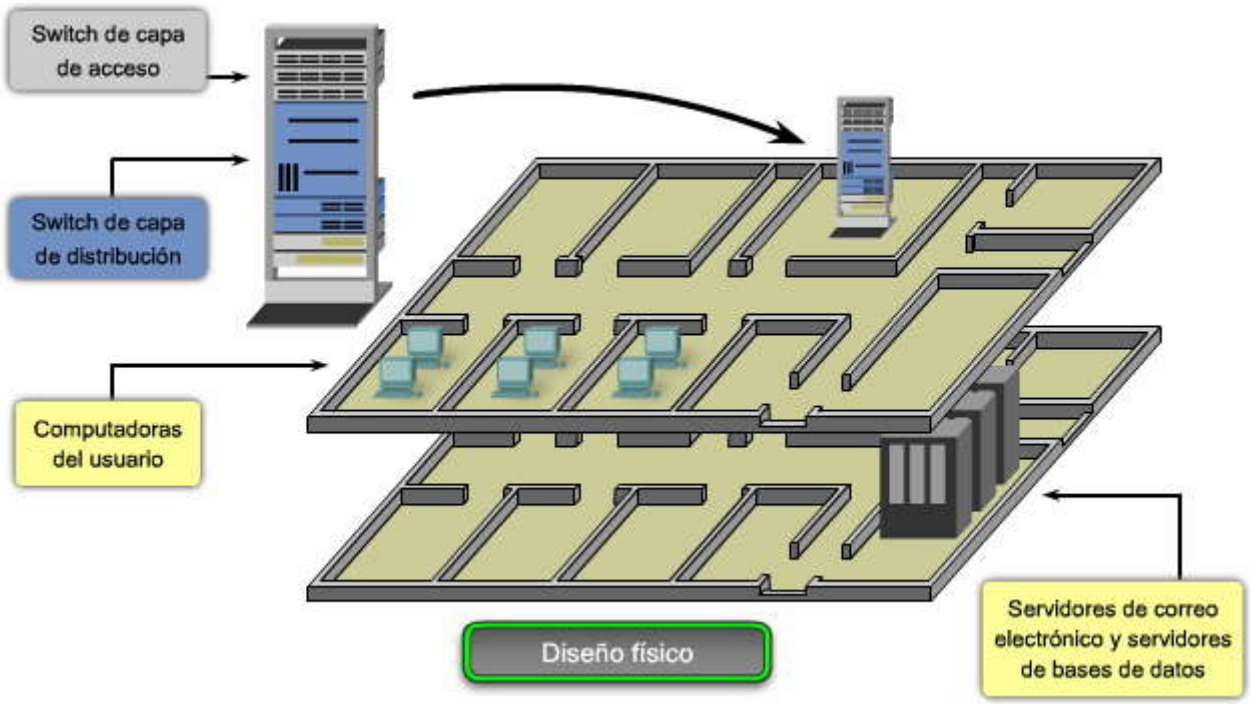
Examinemos un modelo de red jerárquica aplicada a una empresa. En la figura, las capas de acceso, de distribución y núcleo se encuentran separadas en jerarquías bien definidas. Esta representación lógica contribuye a que resulte fácil ver qué switches desempeñan qué función. Es mucho más difícil ver estas capas jerárquicas cuando la red se instala en una empresa.

Haga clic en el botón Diseño físico en la figura.

La figura muestra dos pisos de un edificio. Las computadoras del usuario y los dispositivos de la red que necesitan acceso a la red se encuentran en un piso. Los recursos, como servidores de correo electrónico y servidores de bases de datos, se ubican en otro piso. Para asegurar que cada piso tenga acceso a la red, se instalan la capa de acceso y los switches de distribución en los armarios de cableado de cada piso y se conectan a todos los dispositivos que necesitan acceso a la red. La figura muestra un pequeño bastidor de switches. El switch de la capa de acceso y el switch de la capa de distribución se encuentran apilados uno sobre el otro en el armario de cableado.

Aunque no se muestran los switches de la capa núcleo y otros switches de la capa de distribución, es posible observar cómo la distribución física de una red difiere de la distribución lógica de una red.





Beneficios de una red jerárquica

Existen muchos beneficios asociados con los diseños de la red jerárquica.

Escalabilidad

Las redes jerárquicas escalan muy bien. La modularidad del diseño le permite reproducir exactamente los elementos del diseño a medida que la red crece. Debido a que cada instancia del módulo es consistente, resulta fácil planificar e implementar la expansión. Por ejemplo, si el modelo del diseño consiste en dos switches de la capa de distribución por cada 10 switches de la capa de acceso, puede continuar agregando switches de la capa de acceso hasta tener 10 switches de la capa de acceso interconectados con los dos switches de la capa de distribución antes de que necesite agregar switches adicionales de la capa de distribución a la topología de la red. Además, a medida que se agregan más switches de la capa de distribución para adaptar la carga de los switches de la capa de acceso, se pueden agregar switches adicionales de la capa núcleo para manejar la carga adicional en el núcleo.

Redundancia

A medida que crece una red, la disponibilidad se torna más importante. Puede aumentar radicalmente la disponibilidad a través de implementaciones redundantes fáciles con redes jerárquicas. Los switches de la capa de acceso se conectan con dos switches diferentes de la capa de distribución para asegurar la redundancia de la ruta. Si falla uno de los switches de la capa de distribución, el switch de la capa de acceso puede conmutar al otro switch de la capa de distribución. Adicionalmente, los switches de la capa de distribución se conectan con dos o más switches de la capa núcleo para asegurar la disponibilidad de la ruta si falla un switch del núcleo. La única capa en donde se limita la redundancia es la capa de acceso. Habitualmente, los dispositivos de nodo final, como PC, impresoras y teléfonos IP, no tienen la capacidad de conectarse con switches múltiples de la capa de acceso para redundancia. Si falla un switch de la capa de acceso, sólo se verían afectados por la interrupción los dispositivos conectados a ese switch en particular. El resto de la red continuaría funcionando sin alteraciones.

Rendimiento

El rendimiento de la comunicación mejora al evitar la transmisión de datos a través de switches intermediarios de bajo rendimiento. Los datos se envían a través de enlaces del puerto del switch agregado desde la capa de acceso a la capa de distribución casi a la velocidad de cable en la mayoría de los casos. Luego, la capa de distribución utiliza sus capacidades de conmutar el alto rendimiento para reenviar el tráfico hasta el núcleo, donde se enruta hacia su destino final. Debido a que las capas núcleo y de distribución realizan sus operaciones a velocidades muy altas, no existe contención para el ancho de banda de la red. Como resultado, las redes jerárquicas con un diseño apropiado pueden lograr casi la velocidad de cable entre todos los dispositivos.

Seguridad

La seguridad mejora y es más fácil de administrar. Es posible configurar los switches de la capa de acceso con varias opciones de seguridad del puerto que proveen control sobre qué dispositivos se permite conectar a la red. Además, se cuenta con la flexibilidad de utilizar políticas de seguridad más avanzadas en la capa de distribución. Puede aplicar las políticas de control de acceso que definen qué protocolos de comunicación se implementan en su red y dónde se les permite dirigirse. Por ejemplo, si desea limitar el uso de HTTP a una comunidad de usuarios específica conectada a la capa de acceso, podría aplicar una política que bloquee el tráfico de HTTP en la capa de distribución. La restricción del tráfico en base a protocolos de capas más elevadas, como IP y HTTP, requiere que sus switches puedan procesar las políticas en esa capa. Algunos switches de la capa de acceso admiten la funcionalidad de la Capa 3, pero en general es responsabilidad de los switches de la capa de distribución procesar los datos de la Capa 3, porque pueden procesarlos con mucha más eficacia.

Facilidad de administración

La facilidad de administración es relativamente simple en una red jerárquica. Cada capa del diseño jerárquico cumple funciones específicas que son consistentes en toda esa capa. Por consiguiente, si necesita cambiar la funcionalidad de un switch de la capa de acceso, podría repetir ese cambio en todos los switches de la capa de acceso en la red porque presumiblemente cumplen las mismas funciones en su capa. La implementación de switches nuevos también se simplifica porque se pueden copiar las configuraciones del switch entre los dispositivos con muy pocas modificaciones. La consistencia entre los switches en cada capa permite una recuperación rápida y la simplificación de la resolución de problemas. En algunas situaciones especiales, podrían observarse inconsistencias de configuración entre los dispositivos, por eso debe asegurarse de que las configuraciones se encuentren bien documentadas, de manera que pueda compararlas antes de la implementación.

Capacidad de mantenimiento

Debido a que las redes jerárquicas son modulares en naturaleza y escalan con mucha facilidad, son fáciles de mantener. Con otros diseños de la topología de la red, la administración se torna altamente complicada a medida que la red crece. También, en algunos modelos de diseños de red, existe un límite en cuanto a la extensión del crecimiento de la red antes de que se torne demasiado complicada y costosa de mantener. En el modelo del diseño jerárquico se definen las funciones de los switches en cada capa haciendo que la selección del switch correcto resulte más fácil. La adición de switches a una capa no necesariamente significa que se evitará un cuello de botella u otra limitación en otra capa. Para que una topología de red de malla completa alcance el rendimiento máximo, es necesario que todos los switches sean de alto rendimiento porque es fundamental que cada switch pueda cumplir todas las funciones en la red. En el modelo jerárquico, las funciones de los switches son diferentes en cada capa. Se puede ahorrar dinero con el uso de switches de la capa de acceso menos costosos en la capa inferior y gastar más en los switches de la capa de distribución y la capa núcleo para lograr un rendimiento alto en la red.

Escalabilidad
- Las redes jerárquicas pueden expandirse con facilidad

Redundancia
- La redundancia a nivel del núcleo y de la distribución asegura la disponibilidad de la ruta

Rendimiento
- El agregado del enlace entre los niveles y núcleo de alto rendimiento y switches de nivel de distribución permite casi la velocidad del cable en toda la red

Seguridad
- La seguridad del puerto en el nivel de acceso y las políticas en el nivel de la distribución hacen que la red sea más segura

Facilidad de administración
- La consistencia entre los switches en cada nivel hace que la administración sea más simple

Facilidad de mantenimiento
- La modularidad del diseño jerárquico permite que la red escale sin volverse demasiado complicada

1.1.2 PRINCIPIOS DE DISEÑO DE REDES JERÁRQUICAS.-

Principios de diseño de redes jerárquicas

Sólo porque aparentemente una red presenta un diseño jerárquico, no significa que la red esté bien diseñada. Estas guías simples le ayudan a diferenciar entre redes jerárquicas con un buen diseño y las que presentan un diseño deficiente. La intención de esta sección no es proporcionarle todas las destrezas y el conocimiento que necesita para diseñar una red jerárquica sino ofrecerle una oportunidad de comenzar a practicar sus destrezas a través de la transformación de una topología de red plana en una topología de red jerárquica.

Diámetro de la red

Al diseñar una topología de red jerárquica, lo primero que debe considerarse es el diámetro de la red. Con frecuencia, el diámetro es una medida de distancia pero en este caso se utiliza el término para medir el número de dispositivos. El diámetro de la red es el número de dispositivos que un paquete debe cruzar antes de alcanzar su destino. Mantener bajo el diámetro de la red asegura una latencia baja y predecible entre los dispositivos.

Pase el mouse por el botón Diámetro de la red en la figura.

En la figura, la PC1 se comunica con la PC3. Es posible que existan hasta seis switches interconectados entre la PC1 y la PC3. En este caso, el diámetro de la red es 6. Cada switch en la ruta introduce cierto grado de latencia. La latencia del dispositivo de red es el tiempo que transcurre mientras un dispositivo procesa un paquete o una trama. Cada switch debe determinar la dirección MAC de destino de la trama, verificar la tabla de la dirección MAC y enviar la trama al puerto apropiado. Aunque el proceso completo se produce en una fracción de segundo, el tiempo se acrecienta cuando la trama debe cruzar varios switches.

En el modelo jerárquico de tres capas, la segmentación de la Capa 2 en la capa de distribución prácticamente elimina el diámetro de la red como consecuencia. En una red jerárquica, el diámetro de la red siempre va a ser un número predecible de saltos entre el dispositivo origen y el dispositivo destino.

Agregado de ancho de banda

Cada capa en el modelo de redes jerárquicas es una candidata posible para el agregado de ancho de banda. El agregado de ancho de banda es la práctica de considerar los requisitos de ancho de banda específicos de cada parte de la jerarquía. Después de que se conocen los requisitos de ancho de banda de la red, se pueden agregar enlaces entre switches específicos, lo que recibe el nombre de agregado de enlaces. El agregado de enlaces permite que se combinen los enlaces de puerto de los switches múltiples a fin de lograr un rendimiento superior entre los switches. Cisco cuenta con una tecnología de agregado de enlaces específica llamada EtherChannel, que permite la consolidación de múltiples enlaces de Ethernet. Un análisis de EtherChannel excede el alcance de este curso. Para obtener más información, visite: http://www.cisco.com/en/US/tech/tk389/tk213/tsd_technology_support_protocol_home.html.

Pase el mouse por el botón Agregado de ancho de banda en la figura.

En la figura, las computadoras PC1 y PC3 requieren una cantidad significativa de ancho de banda porque se utilizan para desarrollar simulaciones de condiciones climáticas. El administrador de la red ha determinado que los switches S1, S3 y S5 de la capa de acceso requieren un aumento del ancho de banda. Estos switches de la capa de acceso respetan la jerarquía y se conectan con los switches de distribución D1, D2 y D4. Los switches de distribución se conectan con los switches C1 y C2 de la capa núcleo. Observe cómo los enlaces específicos en puertos específicos se agregan en cada switch. De esta manera, se suministra un aumento del ancho de banda para una parte específica, seleccionada de la red. Observe que en esta figura se indican los enlaces agregados por medio de dos líneas de puntos con un óvalo que las relaciona. En otras figuras, los enlaces agregados están representados por una línea de puntos única con un óvalo.

Redundancia

La redundancia es una parte de la creación de una red altamente disponible. Se puede proveer redundancia de varias maneras. Por ejemplo, se pueden duplicar las conexiones de red entre los dispositivos o se pueden duplicar los propios dispositivos. Este capítulo explora cómo emplear rutas de redes redundantes entre los switches. Un análisis de la duplicación de los dispositivos de red y del empleo de protocolos especiales de red para asegurar una alta disponibilidad excede el alcance de este curso. Para acceder a un análisis interesante acerca de la alta disponibilidad, visite: http://www.cisco.com/en/US/products/ps6550/products_ios_technology_home.html.

La implementación de los enlaces redundantes puede ser costosa. Imagine que cada switch en cada capa de la jerarquía de la red tiene una conexión con cada switch de la capa siguiente. Es improbable que sea capaz de implementar la redundancia en la capa de acceso debido al costo y a las características limitadas en los dispositivos finales pero puede crear redundancia en las capas de distribución y núcleo de la red.

Pase el mouse por el botón Enlaces redundantes en la figura.

En la figura, los enlaces redundantes se observan en la capa de distribución y en la capa núcleo. En la capa de distribución existen dos switches de capa de distribución, el mínimo requerido para admitir redundancia en esta capa. Los switches de la capa de acceso, S1, S3, S4 y S6, se encuentran interconectados con los switches de la capa de distribución. Esto protege su red si falla uno de los switches de distribución. En caso de falla, el switch de la capa de acceso ajusta su ruta de transmisión y reenvía el tráfico a través del otro switch de distribución.

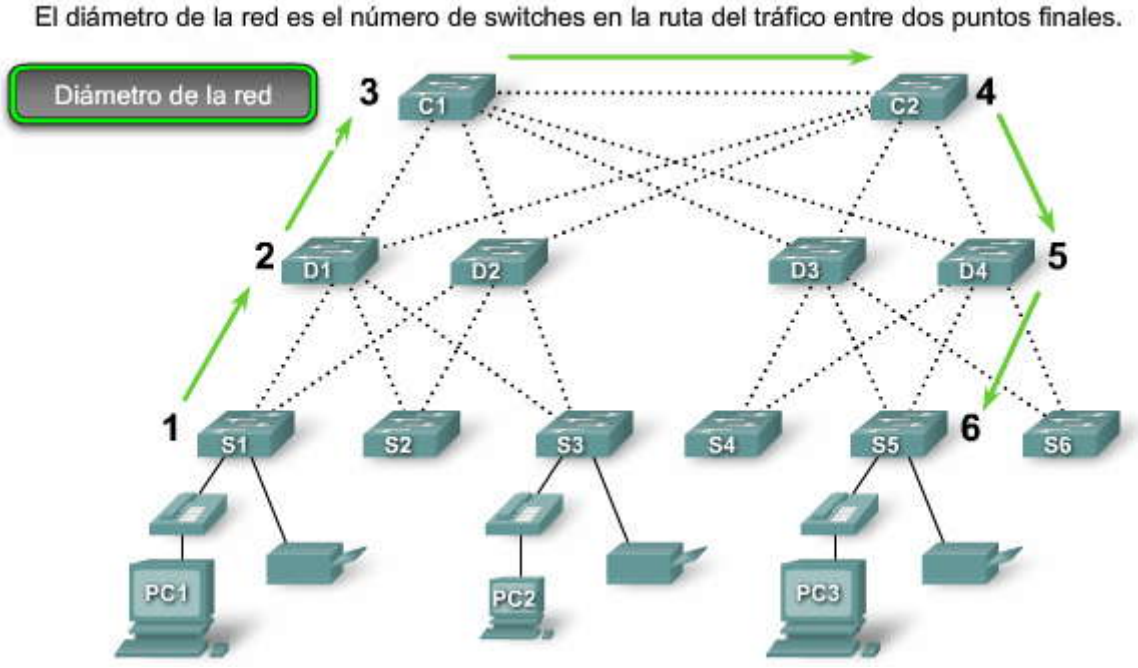
Ciertas situaciones de falla de la red nunca pueden impedirse, por ejemplo si la energía eléctrica se interrumpe en la ciudad entera o el edificio completo se derrumba debido a un terremoto. La redundancia no intenta abordar estos tipos de desastres. Para obtener más información acerca de cómo una empresa puede continuar funcionando y recuperarse de un desastre, visite: http://www.cisco.com/en/US/netsol/ns516/networking_solutions_package.html.

Comience en la capa de acceso

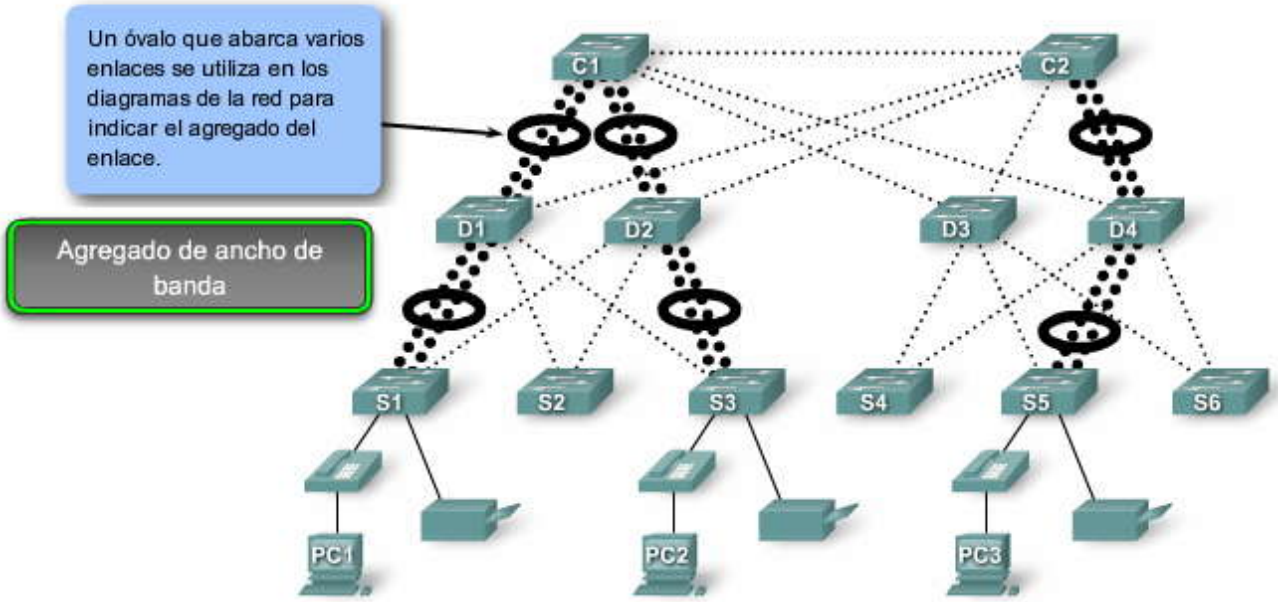
Imagine que se requiere un diseño nuevo de redes. Los requisitos de diseño, como el nivel de rendimiento o la redundancia necesaria, están determinados por las metas comerciales de la organización. Una vez que se documentan los requisitos de diseño, el diseñador puede comenzar a seleccionar el equipo y la infraestructura para implementar el diseño.

Cuando se inicia la selección del equipo en la capa de acceso, puede asegurarse de que se adapta a todos los dispositivos de la red que necesitan acceso a la red. Después de tener en cuenta todos los dispositivos finales se tiene una mejor idea de cuántos switches de la capa de acceso se necesitan. El número de switches de la capa de acceso y el tráfico estimado que cada uno genera ayuda a determinar cuántos switches de la capa de distribución se necesitan para lograr el rendimiento y la redundancia necesarios para la red. Después de determinar el número de switches de la capa de distribución, se puede identificar cuántos switches de núcleo se necesitan para mantener el rendimiento de la red.

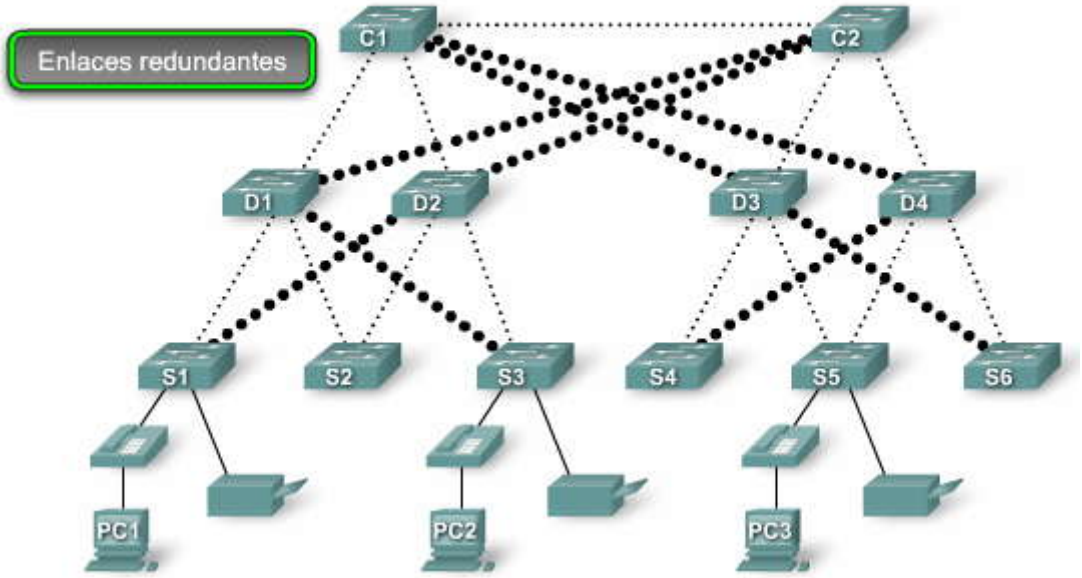
Un análisis exhaustivo acerca de cómo determinar qué switch seleccionar en base al análisis del flujo de tráfico y cuántos switches de núcleo se requieren para mantener el rendimiento queda fuera del alcance de este curso. Para una buena introducción al diseño de red, lea este libro que se encuentra disponible en Ciscopress.com: Top-Down Network Design, de Priscilla Oppenheimer (2004).



El agregado de ancho de banda se implementa normalmente al combinar varios enlaces paralelos entre dos switches en un enlace lógico.



Las redes modernas utilizan enlaces redundantes entre las capas de redes jerárquicas a fin de asegurar la disponibilidad de la red.



1.1.3 ¿QUÉ ES UNA RED CONVERGENTE?.-

Las empresas pequeñas y medianas adoptan la idea de ejecutar servicios de voz y video en sus redes de datos. Observemos cómo la voz y el video sobre IP (VoIP) afectan una red jerárquica.

Equipos heredados

La convergencia es el proceso de combinación de las comunicaciones con voz y video en una red de datos. Las redes convergentes han existido durante algún tiempo pero sólo fueron factibles en grandes organizaciones empresariales debido a los requisitos de infraestructura de la red y a la compleja administración necesaria para hacer que dichas redes funcionen en forma continua. Los costos de red asociados con la convergencia eran altos porque se necesitaba un hardware de switches más costoso para admitir los requisitos adicionales de ancho de banda. Las redes convergentes también necesitaban una administración extensiva en relación con la Calidad de Servicio (QoS), porque era necesario que el tráfico de datos con voz y video se clasificara y priorizara en la red. Pocas personas contaban con la experiencia profesional en cuanto a redes de datos, voz y video para hacer que la convergencia fuese factible y funcional. Además, el equipo antiguo obstaculiza el proceso. La figura muestra un switch antiguo de una empresa telefónica. En la actualidad, la mayoría de las empresas telefónicas ha cambiado a switches digitales. Sin embargo, existen muchas oficinas que aún utilizan teléfonos análogos por lo que todavía tienen armarios de cableado de teléfonos análogos. Debido a que aún no se han reemplazado los teléfonos análogos,

también observará que debe admitir tanto el sistema telefónico PBX antiguo como los teléfonos IP. Con lentitud se reemplazará esta clase de equipamiento por switches modernos de teléfonos IP.

Haga clic en el botón Tecnología avanzada en la figura.

Tecnología avanzada

La convergencia de redes de voz, video y datos se ha vuelto muy popular recientemente en el mercado empresarial pequeño y mediano debido a los avances en la tecnología. En el presente resulta más fácil implementar y administrar la convergencia y su adquisición es menos costosa. La figura muestra una combinación de switch y de teléfono VoIP de alta tecnología apropiada para una empresa mediana de entre 250 y 400 empleados. La figura también muestra un switch Cisco Catalyst Express 500 y un teléfono Cisco 7906G adecuados para empresas pequeñas y medianas. Esta tecnología VoIP solía presentar un precio razonable para empresas y entidades gubernamentales.

La transferencia a una red convergente puede ser una decisión difícil si la empresa ya realizó una inversión en redes de voz, video y datos separadas. El abandono de una inversión que aún funciona resulta arduo pero la convergencia de voz, video y datos en una infraestructura de red única presenta varias ventajas.

Un beneficio de una red convergente es la existencia de sólo una red para administrar. Con las redes de voz, video y datos separadas, los cambios realizados en la red deben coordinarse a través de redes. Además, existen costos adicionales que resultan del uso de tres conjuntos de cableado de redes. El uso de una red única significa que el usuario sólo debe administrar una infraestructura conectada por cables.

Otro beneficio es el menor costo de implementación y administración. Es menos costoso implementar una infraestructura de red única que tres infraestructuras de redes distintas. La administración de una red única es también menos costosa. Tradicionalmente, si una empresa cuenta con una red separada de voz y datos, necesita a un grupo de personas que administren la red de voz y otro grupo que administre la red de datos. Con una red convergente, se necesita a un grupo que administra tanto la red de voz como la de datos.

Haga clic en el botón Opciones nuevas en la figura.

Opciones nuevas

Las redes convergentes ofrecen opciones que no existían con anterioridad. Ahora se pueden unir las comunicaciones de voz y video directamente en el sistema de la computadora personal de un empleado, según se observa en la figura. No es necesario contar con un aparato telefónico o un equipo para videoconferencias caros. Se puede lograr la misma función con el uso de un software especial integrado con una computadora personal. Las herramientas de telesoftware, como Cisco IP Communicator, ofrecen mucha flexibilidad a las empresas. La persona que se encuentra en la parte superior izquierda de la figura utiliza una herramienta de telesoftware en la computadora. Cuando se utiliza el software en lugar de un teléfono físico, una empresa puede realizar la conversión a redes convergentes con rapidez porque no hay gastos de capital en la adquisición de teléfonos IP y de los switches necesarios para accionar los teléfonos. Con la incorporación de cámaras Web económicas, se pueden agregar videoconferencias al telesoftware. Éstos son sólo algunos ejemplos proporcionados por una cartera más amplia de soluciones de comunicación que redefinen el proceso comercial en la actualidad.

Redes separadas de voz, video y datos

Como se puede ver en la figura, una red de voz contiene líneas telefónicas aisladas que ejecutan un switch PBX para permitir la conectividad telefónica a la Red pública de telefonía conmutada (PSTN). Cuando se agrega un teléfono nuevo, se debe ejecutar una línea nueva de regreso al PBX. El switch del PBX se ubica habitualmente en el armario de cableado de Telco, separado de los armarios de cableado de datos y video. Los armarios de cableado con frecuencia se separan porque el personal de apoyo necesita acceso a cada sistema. Sin embargo, mediante el uso de una red jerárquica apropiadamente diseñada y la implementación de políticas de QoS que dan prioridad a los datos de audio, los datos de voz se pueden converger en una red de datos existente con muy poco o ningún impacto en la calidad del audio.

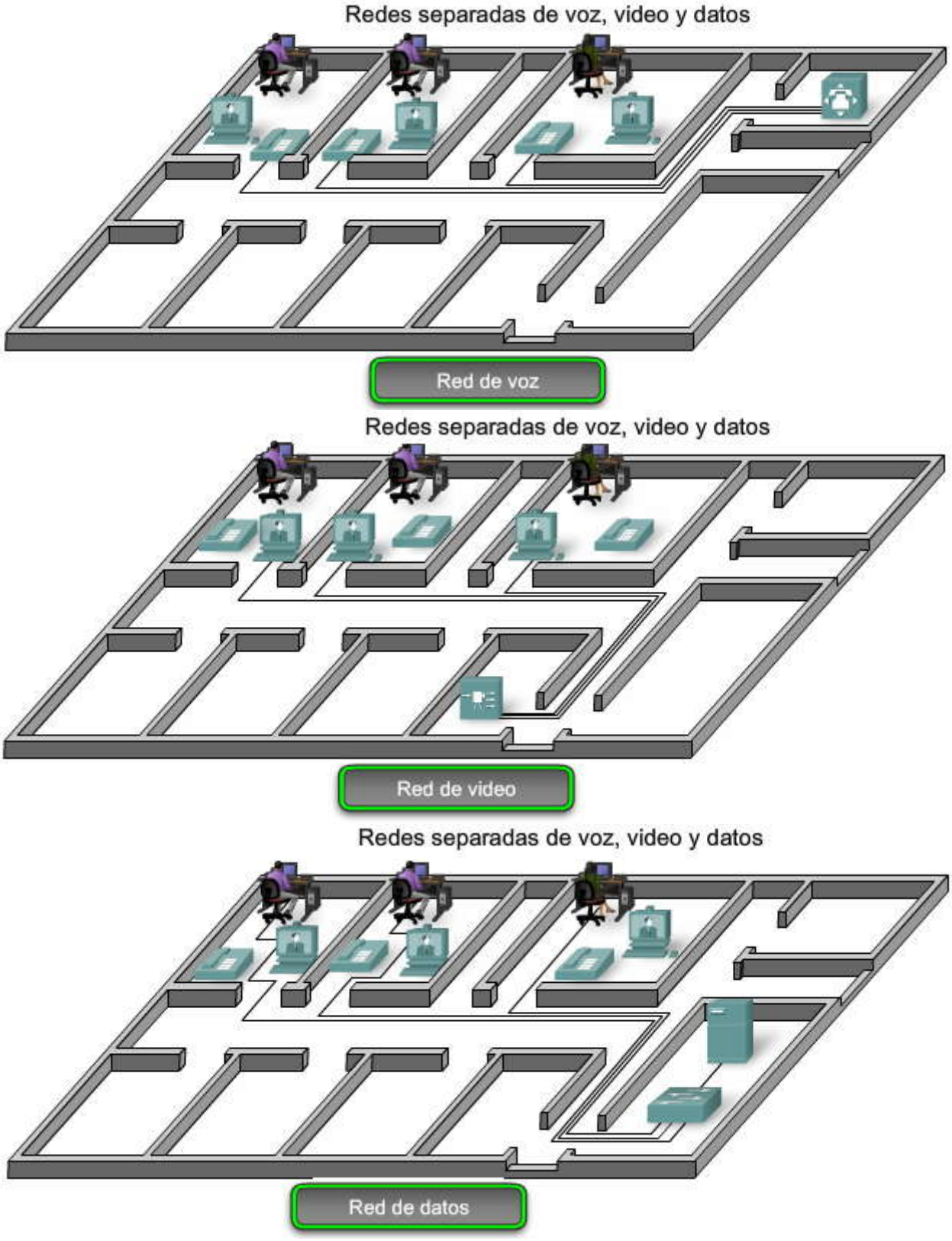
Haga clic en el botón Red de video en la figura para ver un ejemplo de una red de video separada.

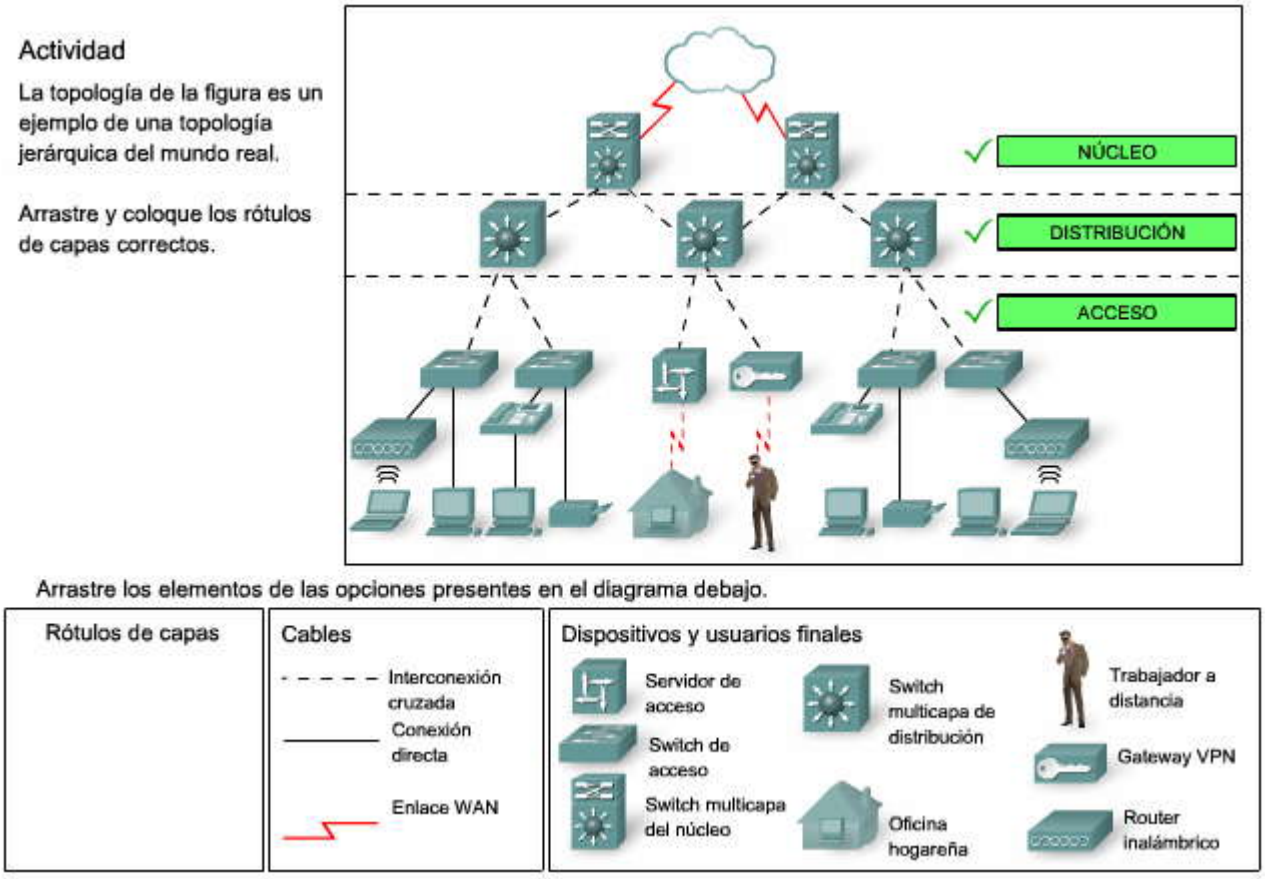
En esta figura, el equipo para videoconferencias está conectado por cable en forma separada de las redes de voz y de datos. Los datos de videoconferencias pueden consumir un ancho de banda significativo en una red. Como resultado, se mantuvieron las redes de videos por separado para permitir que los equipos de videoconferencias funcionen a toda velocidad sin competir por el ancho de banda con los flujos de voz y de datos. Mediante el uso de una red jerárquica

apropiadamente diseñada y la implementación de políticas de QoS que dan prioridad a los datos de video, puede hacerse que dichos datos converjan en una red de datos existente con muy poco o ningún impacto en la calidad del video.

Haga clic en el botón Red de datos en la figura para ver un ejemplo de una red de datos separada.

La red de datos interconecta las estaciones de trabajo y los servidores en una red para facilitar el uso compartido de recursos. Las redes de datos pueden consumir un ancho de banda de datos significativo y éste es el motivo por d cual las redes de voz, video y datos se mantuvieron separadas por tan largo tiempo. Ahora que las redes jerárquicas con el diseño apropiado pueden incluir los requerimientos de ancho de banda de las comunicaciones por voz, video y datos al mismo tiempo;tiene sentido hacer que converjan en una única red jerárquica.





1.2 RELACIÓN ENTRE SWITCHES Y LAS FUNCIONES DE LA LAN.-

1.2.1 CONSIDERACIONES PARA LOS SWITCHES DE REDES JERÁRQUICAS.-

Análisis de flujo de tráfico

Para seleccionar el switch apropiado para una capa en una red jerárquica, es necesario contar con especificaciones que detallen los flujos de tráfico objetivo, las comunidades de usuario, los servidores de datos y los servidores de almacenamiento de datos.

Las empresas necesitan una red que pueda satisfacer los requerimientos del desarrollo. Una empresa puede comenzar con algunas PC interconectadas de manera que puedan compartir datos. A medida que la empresa contrata más empleados, los dispositivos, como PC, impresoras y servidores, se agregan a la red. La incorporación de los nuevos dispositivos implica un aumento en el tráfico de la red. Algunas compañías reemplazan sus sistemas telefónicos existentes por sistemas telefónicos VoIP convergentes, lo que agrega un tráfico adicional.

Cuando se selecciona el hardware de switch, se determina qué switches se necesitan en las capas núcleo, distribución y acceso para adaptarse a los requerimientos del ancho de banda de red. Su plan debe considerar los requerimientos de ancho de banda en el futuro. Adquiera el hardware del switch Cisco apropiado para incorporar tanto las necesidades actuales como las futuras. Para contribuir con la elección más precisa de los switches apropiados, realice y registre los análisis de flujo de tráfico de forma regular.

Análisis del flujo de tráfico

El análisis del flujo de tráfico es el proceso de medición del uso del ancho de banda en una red y el análisis de datos con el fin de lograr ajustes del rendimiento, planificación de la capacidad y toma de decisiones con respecto a las mejoras del hardware. El análisis del flujo de tráfico se realiza con el uso de software para análisis de flujo de tráfico. Aunque no existe una definición exacta de flujo de tráfico de la red, a efectos del análisis del flujo de tráfico, es posible decir que el tráfico de la red es la cantidad de datos enviados durante un cierto período de tiempo. Todos los datos de la red contribuyen con el tráfico, independientemente de su propósito u origen. El análisis de los diferentes orígenes del tráfico y su influencia en la red, permite realizar ajustes más exactos y actualizar la red para lograr el mejor rendimiento posible.

Los datos del flujo de tráfico pueden utilizarse para ayudar a determinar exactamente cuánto tiempo puede continuar utilizando el hardware de la red existente antes de que tenga sentido actualizarlo para adaptarse según los requerimientos adicionales de ancho de banda. Al tomar las decisiones con respecto a qué hardware adquirir, se deben tener en cuenta las

densidades de puerto y las tasas de reenvío del switch para asegurarse de lograr una capacidad de crecimiento adecuada. La densidad de puerto y las tasas de reenvío se explican más adelante en este capítulo.

Existen muchas formas de controlar el flujo de tráfico en una red. Se pueden controlar manualmente los puertos individuales de switch para obtener la utilización del ancho de banda con el tiempo. Al analizar los datos de flujo de tráfico se deben determinar los requerimientos de flujo de tráfico futuro en base a la capacidad en ciertos momentos del día y a dónde se genera y se envía la mayor cantidad de datos. Sin embargo, para obtener resultados exactos es necesario registrar datos suficientes. El registro manual de los datos del tráfico es un proceso tedioso que requiere mucho tiempo y diligencia. Afortunadamente existen algunas soluciones automatizadas.

Herramientas de análisis

Se encuentran disponibles muchas herramientas de análisis de flujo de tráfico que registran automáticamente los datos de flujo de tráfico en una base de datos y realizan un análisis de tendencias. En redes mayores, las soluciones del conjunto del software constituyen el único método eficaz para realizar el análisis de flujo de tráfico. La figura exhibe un resultado de muestra obtenido del Solarwinds Orion 8.1 NetFlow Analysis, que controla el flujo de tráfico en una red. Al recopilar datos mediante el software, se puede observar exactamente cómo se desempeña cada interfaz en un punto de tiempo dado en la red. Con el uso de los cuadros incluidos, se pueden identificar los problemas de flujo de tráfico visualmente. Este proceso es mucho más sencillo que tener que interpretar los números en una columna de datos de flujo de tráfico.

Para obtener una lista de algunas herramientas comerciales de recopilación y de análisis de flujo de tráfico, visite http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/commercial/index.shtml.

Para obtener una lista de algunas herramientas freeware de recopilación y de análisis de flujo de tráfico, visite http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/freeware/index.shtml.

Análisis del flujo de tráfico

Análisis de las comunidades de usuarios

El análisis de las comunidades de usuarios es el proceso de identificación de varios grupos de usuarios y su influencia en el rendimiento de la red. La forma en que se agrupan los usuarios afecta los aspectos relacionados con la densidad de puerto y con el flujo de tráfico, que a su vez influye en la selección de los switches de la red. La densidad de puerto se explica con posterioridad en este capítulo.

En un edificio típico de oficinas, los usuarios finales se agrupan de acuerdo con la función que cumplen en su trabajo porque necesitan un acceso similar a los recursos y aplicaciones. Es posible que el Departamento de Recursos Humanos (HR) se encuentre en un piso de un edificio de oficinas mientras que el Departamento de Finanzas está en otro. Cada departamento tiene un número diferente de usuarios y de necesidades de aplicación y requiere de acceso a los diferentes recursos de datos disponibles a través de la red. Por ejemplo, cuando se seleccionan switches para los armarios de cableado de los departamentos de Recursos Humanos y de Finanzas, se debería elegir un switch que tuviese los puertos suficientes para satisfacer las necesidades del departamento y que fuese lo suficientemente poderoso para adaptarse a los requerimientos

de tráfico para todos los dispositivos en ese piso. Además, un buen plan de diseño de redes considera el crecimiento de cada departamento para asegurar que existen puertos de switch lo suficientemente abiertos que se pueden utilizar antes de la próxima actualización planificada de la red.

Como se muestra en la figura, el Departamento de Recursos Humanos requiere 20 estaciones de trabajo para sus 20 usuarios. Eso se traduce en 20 puertos de switch necesarios para conectar las estaciones de trabajo a la red. Si se seleccionase un switch apropiado de la capa de acceso para adaptarse al Departamento de Recursos Humanos, probablemente se elegiría un switch de 24 puertos, que cuenta con los puertos suficientes para incluir las 20 estaciones de trabajo y los enlaces a los switches de la capa de distribución.

Crecimiento Futuro

Pero este plan no informa acerca del crecimiento futuro. Considere qué sucederá si se agregan cinco empleados al Departamento de Recursos Humanos. Un plan de redes sólido incluye la tasa de crecimiento de personal en los pasados cinco años para poder anticipar el crecimiento futuro. Con ese concepto en mente, se debe adquirir un switch que pueda incluir más de 24 puertos, como es el caso de los switches apilables o modulares que pueden escalar.

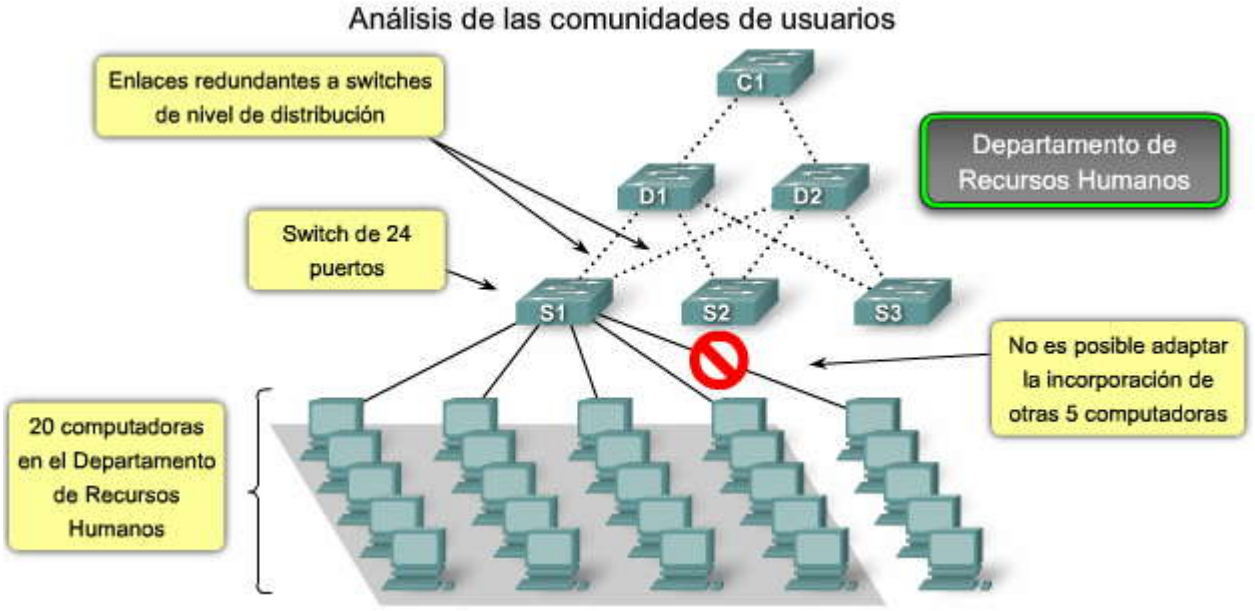
Además de observar el número de dispositivos en un cierto switch en una red, se debe investigar el tráfico de red generado por las aplicaciones de los usuarios finales. Algunas comunidades de usuarios utilizan aplicaciones que generan mucho tráfico de red mientras que otras comunidades de usuarios no lo hacen. Mediante la medición del tráfico de red generado para todas las aplicaciones en uso por las diferentes comunidades de usuarios y la determinación de la ubicación del origen de los datos, se puede identificar el efecto de sumar más usuarios a esa comunidad.

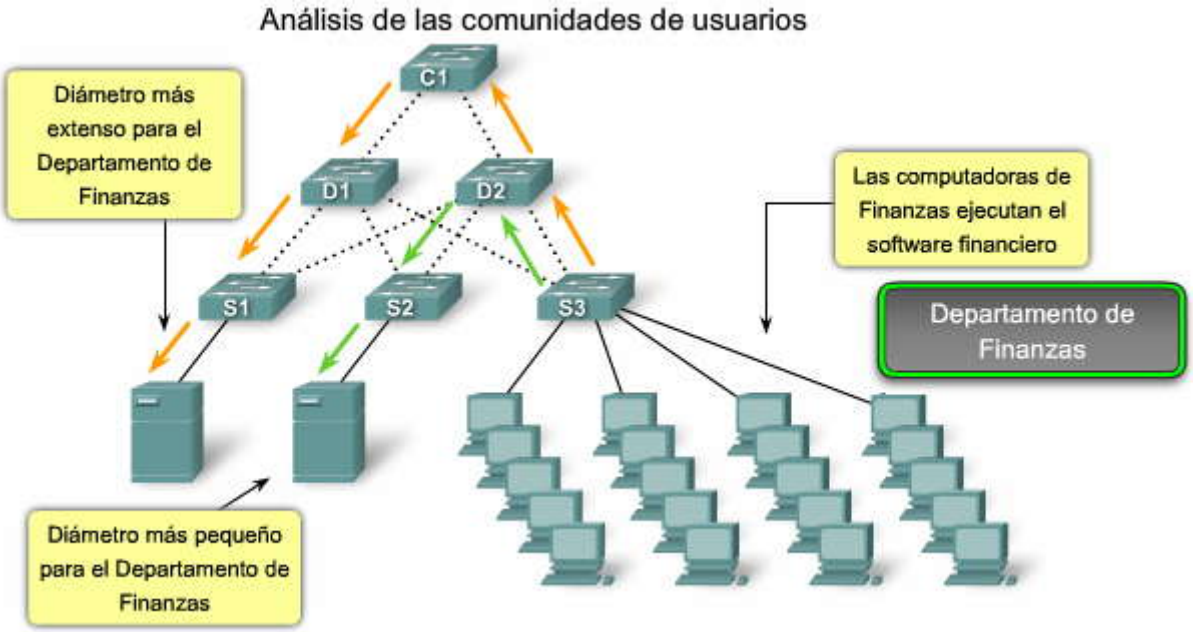
Una comunidad de usuarios que pertenece a un grupo de trabajo en una empresa pequeña queda admitida por un par de switches y en general se conecta al mismo switch que el servidor. En empresas o compañías medianas, las comunidades de usuarios son admitidas por muchos switches. Los recursos que las comunidades de usuarios de empresas o compañías medianas necesitan podrían ubicarse en áreas geográficamente separadas. En consecuencia, la ubicación de las comunidades de usuarios influye en el lugar donde se localizan los almacenamientos de datos y los servidores centrales.

Haga clic en el botón Departamento de Finanzas en la figura.

Si los usuarios de Finanzas están utilizando una aplicación intensiva de red y que intercambia datos con un servidor específico en la red, es posible que resulte útil ubicar a la comunidad de usuarios de Finanzas cerca de ese servidor. Al ubicar a los usuarios cerca de sus servidores y de sus medios de almacenamiento de datos, se puede reducir el diámetro de la red para sus comunicaciones y, por consiguiente, reducir el impacto de su tráfico a través del resto de la red.

Una complicación del análisis del uso de la aplicación según las comunidades de usuarios es que el uso no siempre está unido por departamentos o ubicación física. Es posible que se deba analizar el impacto de la aplicación a través de muchos switches de la red para determinar su impacto general.





Análisis de los medios de almacenamiento de datos y de los servidores de datos

Al analizar el tráfico en una red, se debe considerar dónde se ubican los medios de almacenamiento y los servidores de datos de manera que se pueda determinar el impacto del tráfico en la red. Los medios de almacenamiento de datos pueden ser servidores, redes de almacenamiento de datos (SAN), almacenamiento adjunto a redes (NAS), unidades de copia de respaldo en cinta o cualquier otro dispositivo o componente en los que se almacenan grandes cantidades de datos.

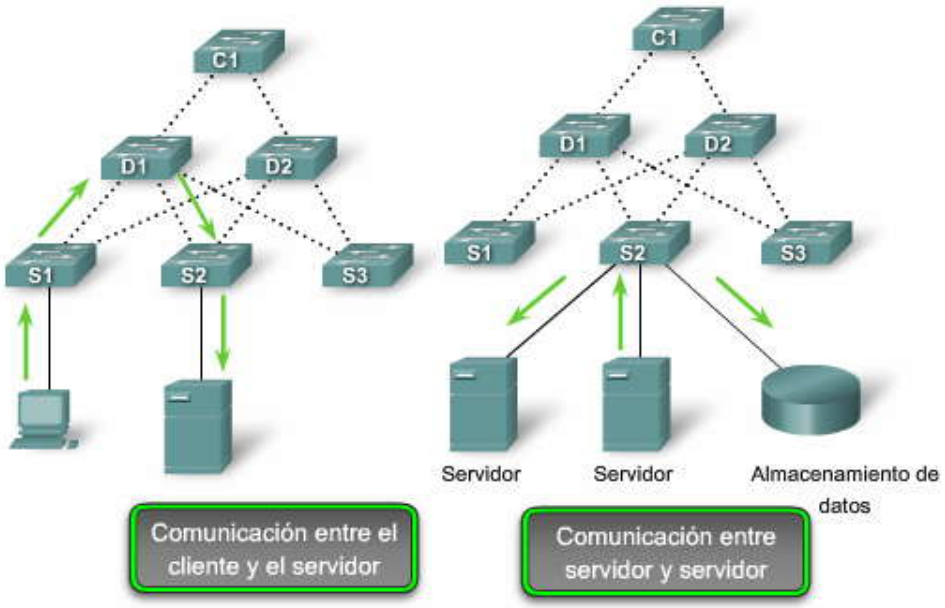
Al considerar el tráfico para los medios de almacenamiento y los servidores de datos, se debe considerar tanto el tráfico según el modelo cliente-servidor como el tráfico entre servidor y servidor.

Según se observa en la figura, el tráfico entre el cliente y el servidor es el tráfico generado cuando el dispositivo de un cliente accede a los datos de los medios de almacenamiento o de los servidores de datos. El tráfico entre el cliente y el servidor habitualmente atraviesa múltiples switches para alcanzar su destino. El agregado de ancho de banda y las tasas de reenvío del switch son factores importantes que se deben considerar cuando se intenta eliminar cuellos de botella para este tipo de tráfico.

Haga clic en el botón Comunicación entre servidor y servidor en la figura.

El tráfico entre servidor y servidor es el tráfico generado entre los dispositivos de almacenamiento de datos en la red. Algunas aplicaciones del servidor generan volúmenes muy altos de tráfico entre los almacenamientos de datos y otros servidores. Para optimizar el tráfico entre servidor y servidor, los servidores que necesitan acceso frecuente a ciertos recursos se deben ubicar a muy corta distancia uno del otro, para que el tráfico que generan no afecte el rendimiento del resto de la red. Los medios de almacenamiento y los servidores de datos habitualmente se ubican en los centros de datos dentro de una empresa. Un centro de datos es un área segura del edificio donde se ubicanlos servidores, los medios de almacenamiento de datos y otros equipos de la red. Un dispositivo puede ubicarse físicamente en el centro de datos pero puede representarse en una ubicación totalmente diferente en la topología lógica. El tráfico a través de bs switches del centro de datos con frecuencia es muy alto debido al tráfico entre servidor y servidor y entre el servidor y el cliente que atraviesa los switches. Como resultado, los switches seleccionados para los centros de datos deben ser switches de más alto rendimiento que los switches que se hallan en los armarios de cableado en la capa de acceso.

Al examinar las rutas de los datos para varias aplicaciones utilizadas por diferentes comunidades de usuarios, se pueden identificar los cuellos de botella potenciales cuando el rendimiento de la aplicación puede verse afectado por el ancho de banda inadecuado. Para mejorar el rendimiento, se podrían agregar enlaces para adaptarse al ancho de banda o reemplazar los switches más lentos por switches más rápidos que puedan manejar la carga del tráfico.

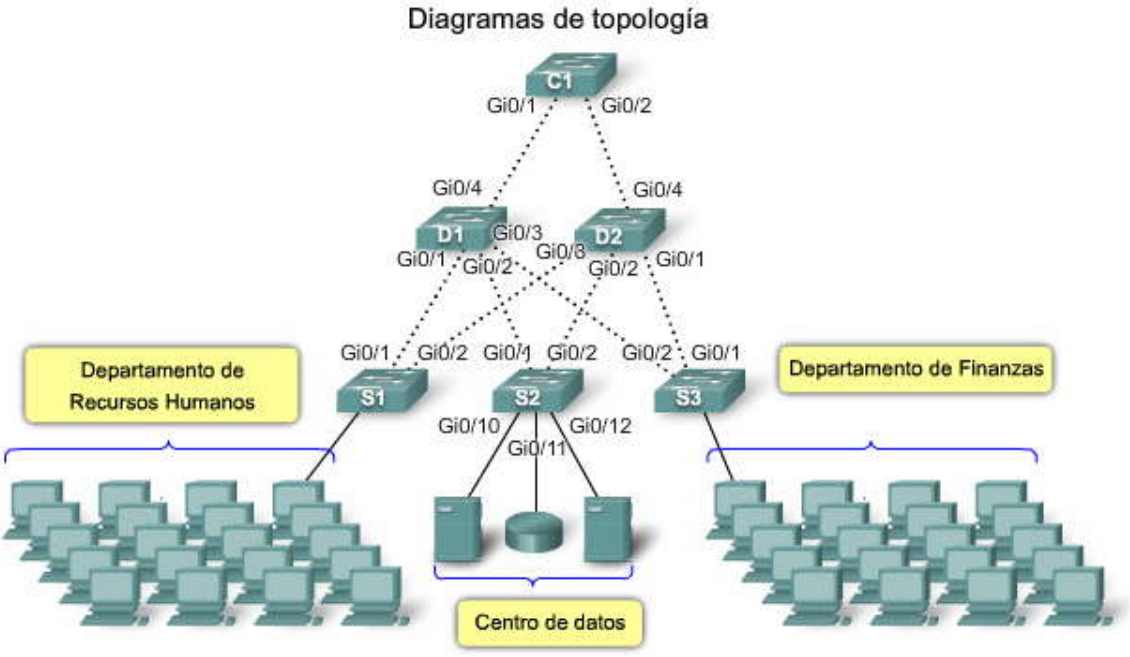


Diagramas de topología

Un diagrama de topología es una representación gráfica de la infraestructura de una red. Un diagrama de topología muestra cómo se interconectan todos los switches e incluye detalles de qué puerto del switch interconecta los dispositivos. Un diagrama de topología muestra de forma gráfica toda ruta redundante o todos los puertos agregados entre los switches que aportan resiliencia y rendimiento. Demuestra dónde y cuántos switches están en uso en su red, así como también identifica su configuración. Los diagramas de topología también pueden contener información acerca de las densidades de los dispositivos y de las comunidades de usuarios. Al tener un diagrama de topología, se pueden identificar visualmente los potenciales cuellos de botella en un tráfico de red de manera que se pueda centrar la recopilación de datos del análisis de tráfico en áreas en las que las mejoras pueden ejercer el impacto más significativo en el rendimiento.

Es posible que resulte difícil componer una topología de red a posteriori si no se ha participado en el proceso de diseño. Los cables de la red en los armarios de cableado desaparecen en los pisos y techos y este hecho dificulta el trazado de sus destinos. Y debido a que los dispositivos están dispersos en todo el edificio, resulta difícil saber cómo se conectan todas las piezas. Con paciencia, se puede determinar exactamente cómo se interconecta todo y luego documentar la infraestructura de la red en un diagrama de topología.

La figura muestra un diagrama simple de topología de red. Nótese cuántos switches se encuentran presentes en la red, así como también la forma en que cada switch se interconecta. El diagrama de topología identifica cada puerto del switch utilizado para las comunicaciones inter switches y rutas redundantes entre switches de capa de acceso y switches de capa de distribución. El diagrama de topología también muestra dónde se ubican las diferentes comunidades de usuarios en la red y la ubicación de los servidores y de los medios de almacenamiento de datos.



1.2.2 CARACTERÍSTICAS DE LOS SWITCHES.-

Factores de forma de los switches

¿Cuáles son las características clave de los switches que se utilizan en las redes jerárquicas? Al buscar las especificaciones para un switch, ¿Qué significan todos los acrónimos y las frases? ¿Qué significa "PoE" y qué es "tasa de reenvío"? En este tema aprenderá sobre estas características.

Al seleccionar un switch se necesita decidir entre una configuración fija o una configuración modular y entre apilable y no apilable. Otra consideración es el grosor del switch expresado en cantidad de bastidores. Por ejemplo, los Switches de configuración fija que se muestran en la figura son todos de 1 bastidor (1U). Con frecuencia estas opciones se denominan factores de forma del switch.

Switches de configuración fija

Los switches de configuración fija son sólo lo que podría esperarse: fijos en su configuración. Esto significa que no se pueden agregar características u opciones al switch más allá de las que originalmente vienen con el switch. El modelo en particular que se compra determina las características y opciones disponibles. Por ejemplo, si se adquiere un switch fijo gigabit de 24 puertos, no se pueden agregar puertos cuando se les necesite. Habitualmente, existen diferentes opciones de configuración que varían en cuanto al número y al tipo de puertos incluidos.

Switches modulares

Los switches modulares ofrecen más flexibilidad en su configuración. Habitualmente, los switches modulares vienen con chasis de diferentes tamaños que permiten la instalación de diferentes números de tarjetas de línea modulares. Las tarjetas de línea son las que contienen los puertos. La tarjeta de línea se ajusta al chasis del switch de igual manera que las tarjetas de expansión se ajustan en la PC. Cuanto más grande es el chasis, más módulos puede admitir. Como se observa en la figura, es posible elegir entre muchos tamaños de chasis diferentes. Si se compró un switch modular con una tarjeta de línea de 24 puertos, con facilidad se podría agregar una tarjeta de línea de 24 puertos para hacer que el número de puertos ascienda a 48.

Switches apilables

Los switches apilables pueden interconectarse con el uso de un cable especial del backplane que otorgarendimiento de ancho de banda entre los switches. Cisco introdujo la tecnología StackWise en una de sus líneas de productos con switches. StackWise permite interconectar hasta nueve switches con el uso de conexiones backplane totalmente redundantes. Como se observa en la figura, los switches están apilados uno sobre el otro y los cables conectan los switches en forma de cadena margarita. Los switches apilados operan con efectividad como un único switch más grande. Los switches apilables son convenientes cuando la tolerancia a fallas y la disponibilidad de ancho de banda son críticas y resulta costoso implementar un switch modular. El uso de conexiones cruzadas hace que la red pueda recuperarse rápidamente si falla un único switch. Los switches apilables utilizan un puerto especial para las interconexiones y no utilizan puertos de línea para las conexiones inter switches. Asimismo, las velocidades son habitualmente más rápidas que cuando se utilizan puertos de línea para la conexión de switches.

Rendimiento

Cuando se selecciona un switch para las capas de acceso, de distribución y núcleo, se debe considerar la capacidad del switch para admitir los requerimientos de densidad de puerto, tasas de reenvío y agregado de ancho de banda de la red.

Densidad de puerto

La densidad de puerto es el número de puertos disponibles en un switch único. Los switches de configuración fija habitualmente admiten hasta 48 puertos en un único dispositivo, con opciones de cuatro puertos adicionales para dispositivos de factor de forma pequeños enchufables (SFP), según muestra la figura. Las altas densidades de puerto permiten un mejor uso del espacio y de la energía cuando la fuente de ambos es limitada. Si tiene dos switches y cada uno contiene 24 puertos, se podrían admitir hasta 46 dispositivos porque se pierde al menos un puerto por switch para conectar cada switch al resto de la red. Además, se requieren dos tomas de alimentación eléctrica. Por otro lado, si tiene un único switch con 48 puertos, se pueden admitir 47 dispositivos con un sólo puerto utilizado para conectar el switch con el resto de la red y sólo una toma de alimentación eléctrica es necesaria para incluir el único switch.

Los switches modulares pueden admitir densidades de puerto muy altas mediante el agregado de tarjetas de línea de puerto de switch múltiples, como muestra la figura. Por ejemplo, el switch Catalyst 6500 puede admitir un exceso de 1000 puertos de switch en un único dispositivo.

Las grandes redes empresariales que admiten muchos miles de dispositivos de red requieren switches modulares de alta densidad para lograr el mejor uso del espacio y de la energía. Sin el uso de un switch modular de alta densidad, la red necesitaría muchos switches de configuración fija para incluir el número de dispositivos que necesitan acceso a la red. Este enfoque puede consumir muchas tomas de alimentación eléctrica y mucho espacio en el armario.

El usuario también debe abordar el tema de los cuellos de botella del enlace. Una serie de switches de configuración fija pueden consumir muchos puertos adicionales para el agregado de ancho de banda entre los switches con el fin de lograr el rendimiento previsto. Con un único switch modular, el agregado del ancho de banda no constituye un problema porque el backplane del chasis puede proporcionar el ancho de banda necesario para incluir los dispositivos conectados a las tarjetas de línea de puerto del switch.

Velocidades de envío

Haga clic en el botón Velocidades de envío en la figura para observar un ejemplo de tasas de reenvío en los switches con diferentes densidades de puerto.

Las tasas de reenvío definen las capacidades de procesamiento de un switch mediante la estimación de la cantidad de datos que puede procesar por segundo el switch. Las líneas de productos con switch se clasifican según las tasas de reenvío. Los switches de la capa de entrada presentan tasas de reenvío inferiores que los switches de la capa empresarial. Es importante considerar las tasas de reenvío cuando se selecciona un switch. Si la tasa de reenvío del switch es demasiado baja, no puede incluir una comunicación a velocidad de cable completa a través de todos sus puertos de switch. La velocidad de cable es la tasa de datos que cada puerto en el switch puede lograr, 100 Mb/s Fast Ethernet o 1000 Mb/s Gigabit Ethernet. Por ejemplo, un switch gigabit con 48 puertos que opera a una velocidad de cable completa genera 48 Gb/s de tráfico. Si el switch sólo admite una tasa de reenvío de 32 Gb/s, no puede ejecutar la velocidad de cable completa a través de todos los puertos de forma simultánea. Afortunadamente, es habitual que los switches de la capa de acceso no necesiten operar a velocidad de cable completa porque se encuentran físicamente limitados por sus enlaces en la capa de distribución. Esto permite utilizar switches menos costosos, de rendimiento inferior en la capa de acceso y switches más caros pero con un rendimiento superior en la capa de distribución y en la capa núcleo, en las que la tasa de reenvío es más importante.

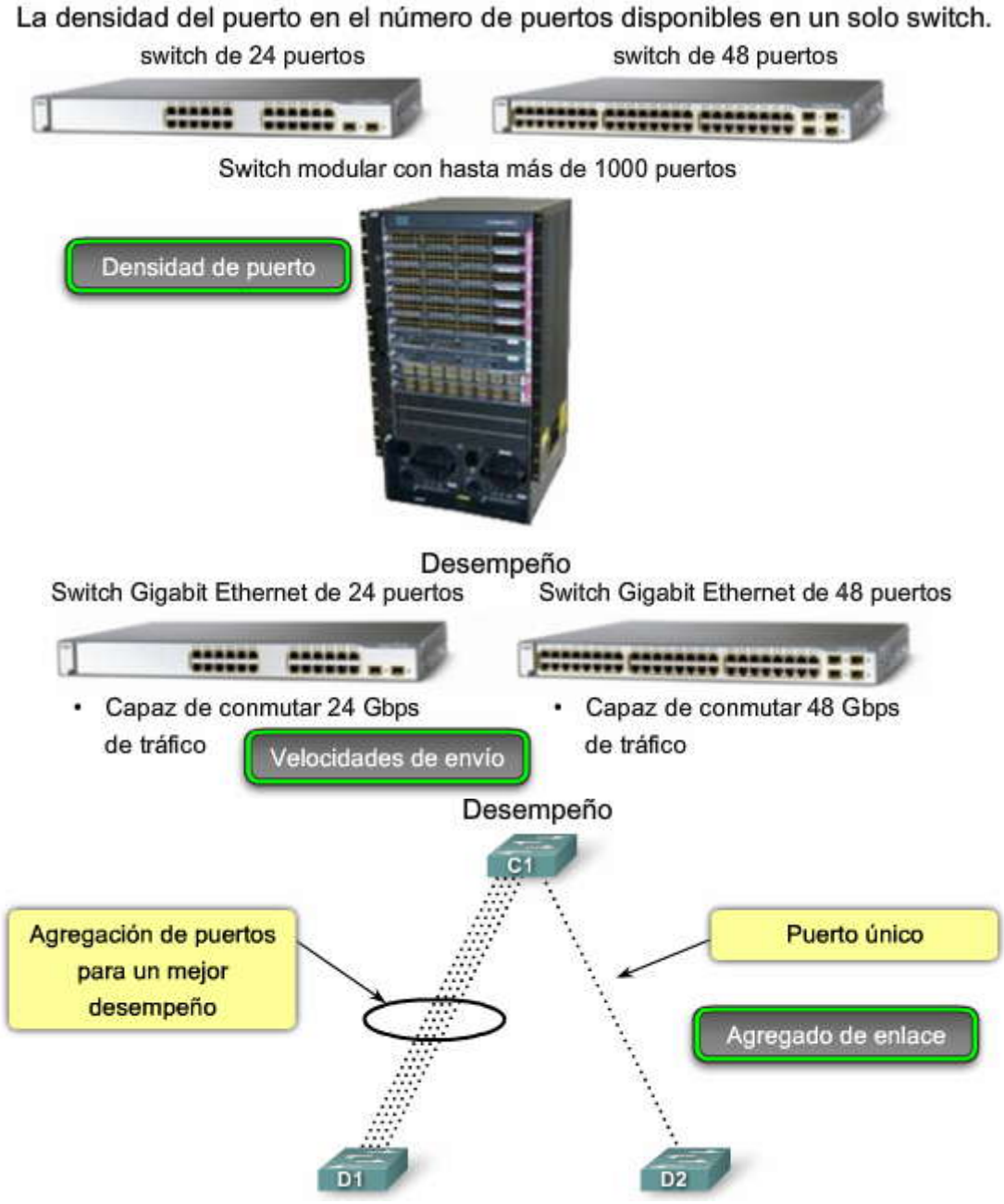
Agregado de enlaces

Haga clic en el botón Agregado de enlace en la figura.

Como parte del agregado de ancho de banda, se debe determinar si existen puertos suficientes en un switch para agregar y así admitir el ancho de banda requerido. Por ejemplo, considere un puerto Gigabit Ethernet, que transporta hasta 1 Gb/s de tráfico. Si tiene un switch con 24 puertos, con todos los puertos capaces de ejecutar a velocidades de gigabit, podría generar hasta 24 Gb/s de tráfico de red. Si el switch está conectado con el resto de la red a través de un único cable de red, puede sólo enviar 1 Gb/s de datos al resto de la red. Debido a la contención para el ancho de banda, los datos se enviarían con más lentitud. El resultado es una velocidad de cable de 1/24º disponible para cada uno de los 24 dispositivos conectados al switch. La velocidad de cable describe la tasa máxima y teórica de transmisión de datos de una conexión. Por ejemplo, la velocidad de cable de una conexión Ethernet depende de las propiedades físicas y eléctricas del cable, combinadas con la capa más baja de los protocolos de conexión.

El agregado de enlace ayuda a reducir estos cuellos de botella del tráfico al permitir la unión de hasta ocho puertos de switch para las comunicaciones de datos y al suministrar hasta 8 Gb/s de rendimiento de datos cuando se utilizan los puertos Gigabit Ethernet. Con el agregado de enlaces múltiples de 10 Gigabit Ethernet (10GbE) en algunos switches de la capa empresarial, es posible lograr tasas de rendimiento muy altas. Cisco utiliza el término EtherChannel cuando describe los puertos de switch agregados.

Como se observa en la figura, se utilizan cuatro puertos separados en los switches C1 y D1 para crear un EtherChannel de 4 puertos. La tecnología EtherChannel permite que un grupo de enlaces físicos de Ethernet cree un enlace lógico de Ethernet con el fin de proporcionar tolerancia a fallas y enlaces de alta velocidad entre switches, routers y servidores. En este ejemplo hay un rendimiento equivalente a cuatro veces el de la conexión de único puerto entre los switches C1 y D2.



Funcionalidad de la PoE y de la Capa 3

Otras dos características que se necesita considerar cuando se selecciona un switch son la funcionalidad de Power over Ethernet (PoE) y de la Capa 3.

Power over Ethernet

Power over Ethernet (PoE) permite que el switch suministre energía a un dispositivo por el cableado de Ethernet existente. Como se puede observar en la figura, esta característica puede utilizarse por medio de los teléfonos IP y algunos puntos de acceso inalámbricos. PoE permite mayor flexibilidad al instalar los puntos de acceso inalámbricos y los teléfonos IP porque

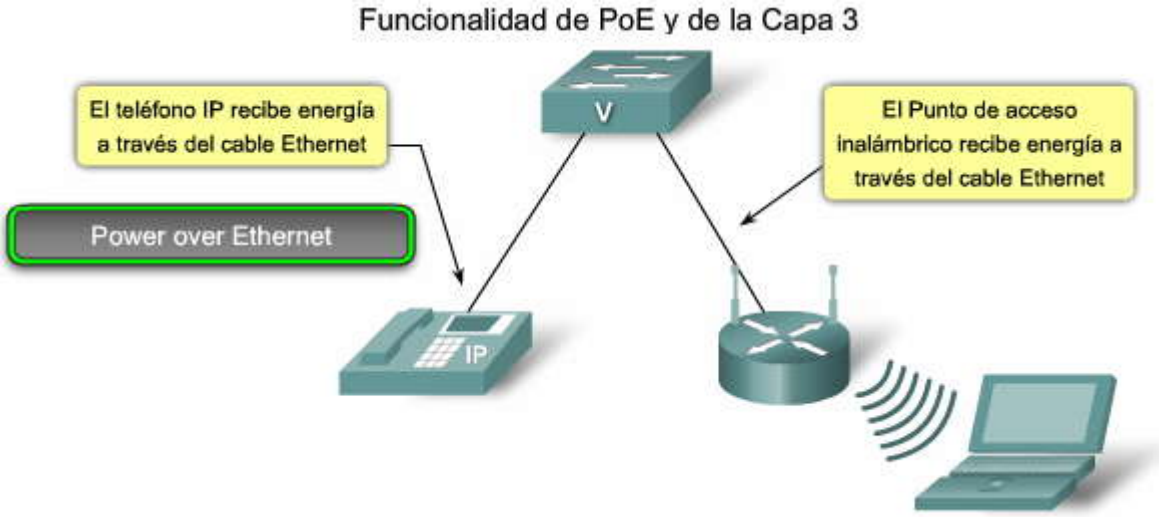
se los puede instalar en cualquier lugar donde se puede tender un cable de Ethernet. No es necesario considerar cómo suministrar energía eléctrica normal al dispositivo. Sólo se debe elegir un switch que admita PoE si realmente se va a aprovechar esa función, porque suma un costo considerable al switch.

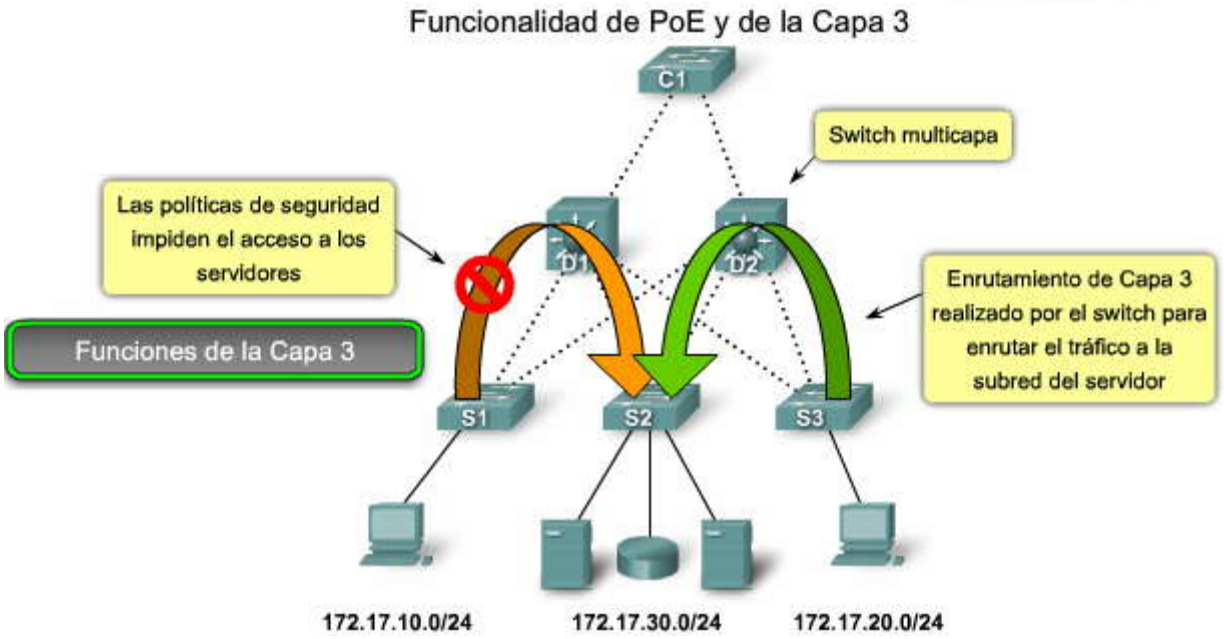
Haga clic en el ícono del switch para ver los puertos de PoE.
Haga clic en el ícono del teléfono para ver los puertos del teléfono.
Haga clic en el punto de acceso inalámbrico para observar sus puertos.

Funciones de la Capa 3

Haga clic en el botón funciones de la Capa 3 en la figura para observar algunas funciones de la Capa 3 que pueden aportar los switches en una red jerárquica.

Normalmente, los switches operan en la Capa 2 del modelo de referencia OSI, donde pueden ocuparse principalmente de las direcciones MAC de los dispositivos conectados con los puertos del switch. Los switches de la Capa 3 ofrecen una funcionalidad avanzada que se analiza en más detalle en los capítulos posteriores de este curso. Los switches de la Capa 3 también reciben el nombre de switches multicapas.





1.2.3 CARÁCTERÍSTICAS DEL SWITCH EN UNA RED JERÁRQUICA.-

Características del switch de la capa de acceso

Ahora que conoce qué factores debe considerar al elegir un switch, examinemos qué características se necesitan en cada capa en una red jerárquica. Luego, podrá relacionar la especificación del switch con su capacidad para funcionar como switch de las capas de acceso, de distribución o núcleo.

Los switches de la capa de acceso facilitan la conexión de los dispositivos de nodo final a la red. Por esta razón, necesitan admitir características como seguridad de puerto, VLAN, Fast Ethernet/Gigabit Ethernet, PoE y agregado de enlaces.

La seguridad de puerto permite que el switch decida cuántos y qué dispositivos específicos se permiten conectar al switch. Todos los switches Cisco admiten seguridad de capa de puerto. La seguridad de puerto se aplica en el acceso. En consecuencia, es una importante primera línea de defensa para una red. Aprenderá acerca de seguridad de puerto en el capítulo 2.

Las VLAN son un componente importante de una red convergente. El tráfico de voz habitualmente recibe una VLAN separada. De esta manera, el tráfico de voz puede admitirse con más ancho de banda, conexiones más redundantes y seguridad mejorada. Los switches de la capa de acceso permiten establecer las VLAN para los dispositivos de nodo final en su red.

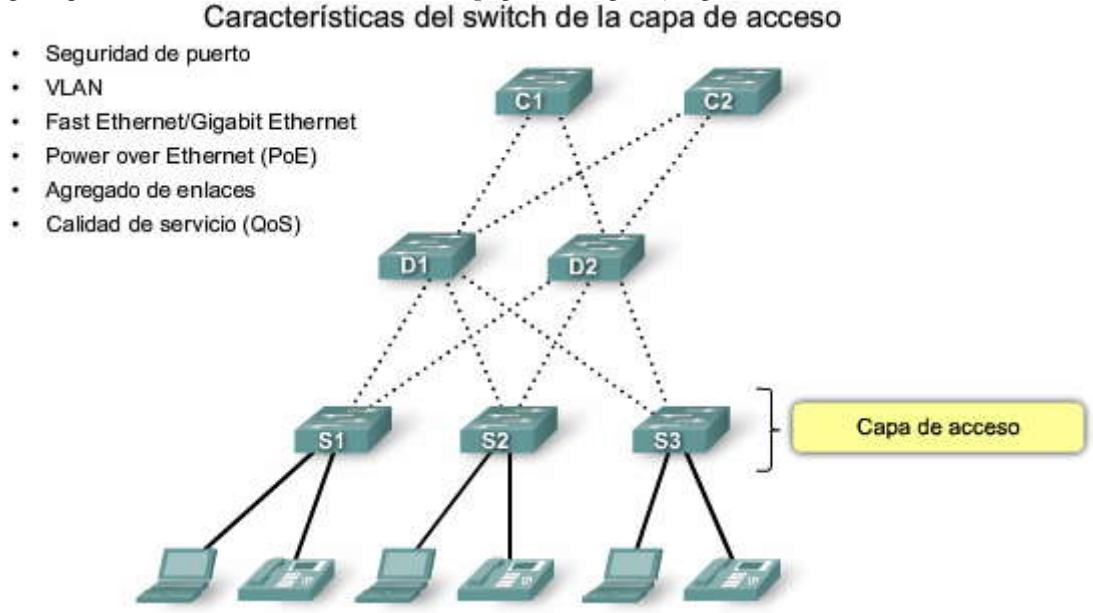
La velocidad de puerto es también una característica que se necesita considerar para los switches de la capa de acceso. Según los requerimientos de rendimiento para su red, debe elegir entre los puertos de switch Fast Ethernet Fast y Gigabit Ethernet. Fast Ethernet permite hasta 100 Mb/s de tráfico por puerto de switch. Fast Ethernet es adecuada para telefonía IP y tráfico de datos en la mayoría de las redes comerciales. Sin embargo, el rendimiento es más lento que el de los puertos Gigabit Ethernet. Gigabit Ethernet permite hasta 1000 Mb/s de tráfico por puerto de switch. La mayoría de los dispositivos modernos, como las estaciones de trabajo, computadoras portátiles y teléfonos IP, admite Gigabit Ethernet. Esto permite transferencias de datos más eficaces y permite a los usuarios ser más productivos. Gigabit Ethernet presenta una desventaja: los switches que admiten Gigabit Ethernet son más costosos.

Otro requerimiento de la característica de algunos switches de capa de acceso es PoE. PoE aumenta drásticamente el precio general del switch en todas las líneas de productos de switches Cisco Catalyst, por lo que sólo debe considerarse cuando se necesita convergencia de voz o se están implementando puntos de acceso inalámbricos y es difícil o costoso ponerlos en funcionamiento en la ubicación deseada.

El agregado de enlaces es otra característica común a la mayoría de los switches de capa de acceso. El agregado de enlaces permite que el switch utilice enlaces múltiples simultáneamente. Los switches de capa de acceso se benefician con el agregado de enlaces cuando se agrega ancho de banda hasta los switches de capa de distribución.

Debido a que la conexión de enlace entre el switch de capa de acceso y el switch de capa de distribución es en general el cuello de botella en la comunicación, la tasa interna de reenvío de los switches de capa de acceso no necesita ser tan alta como el enlace entre los switches de capa de distribución y los de capa de acceso. Las características como la tasa interna de envío no ofrecen problemas para los switches de capa de acceso porque sólo manejan el tráfico desde los dispositivos finales y lo reenvían a los switches de capa de distribución.

En una red convergente que admite tráfico de red de datos, voz y video, los switches de capa de acceso necesitan admitir QoS para mantener la prioridad del tráfico. Los teléfonos IP Cisco son tipos de equipos que se hallan en la capa de acceso. Cuando se conecta un teléfono IP Cisco a un puerto del switch de capa de acceso configurado para admitir tráfico de voz, ese puerto del switch indica al teléfono IP cómo enviar su tráfico de voz. Es necesario permitir QoS en los switches de capa de acceso para que el tráfico de voz del teléfono IP tenga prioridad, por ejemplo, sobre el tráfico de datos.



Características del switch de la capa de distribución

Los switches de la capa de distribución desempeñan una función muy importante en la red. Recopilan los datos de todos los switches de capa de acceso y los envían a los switches de capa núcleo. Aprenderá más adelante en este curso que el tráfico generado en la Capa 2 en una red conmutada necesita ser administrado o segmentado en las VLAN para no consumir ancho de banda de forma innecesaria a través de la red. Los switches de capa de distribución proporcionan funciones de enrutamiento entre las VLAN, para que una VLAN pueda comunicarse con otra en la red. Habitualmente, este enrutamiento se produce en la capa de distribución porque los switches de capa de distribución presentan capacidades de procesamiento más altas que los switches de capa de acceso. Los switches de capa de distribución reducen la necesidad de que los switches núcleo realicen la tarea, debido a que el núcleo está ocupado con el manejo del reenvío de volúmenes muy altos de tráfico. Debido a que el enrutamiento entre las VLAN se realiza en la capa de distribución, los switches en esta capa necesitan admitir las funciones de la Capa 3.

Políticas de seguridad

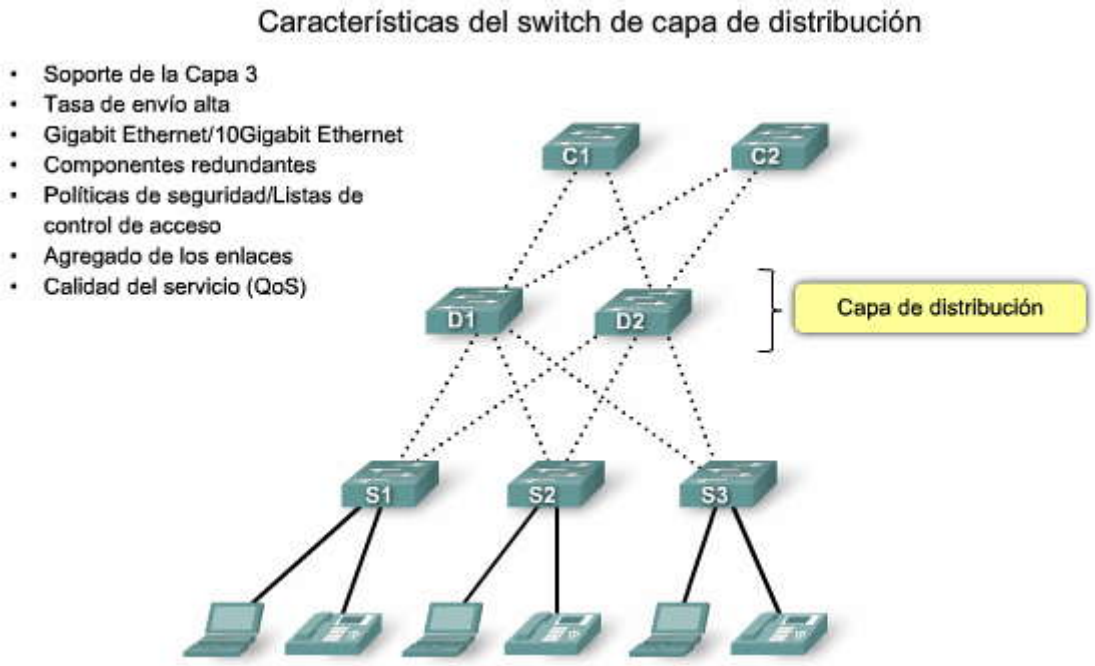
Otro motivo por el que se necesita la funcionalidad de la Capa 3 para los switches de capa de distribución obedece a las políticas de seguridad avanzada que pueden aplicarse al tráfico de red. Se utilizan listas de acceso para controlar cómo fluye el tráfico a través de la red. Una Lista de control de acceso (ACL) permite que el switch impida ciertos tipos de tráfico y autorice otros. Las ACL también permiten controlar qué dispositivos de red pueden comunicarse en la red. El uso de las ACL es un procesamiento intensivo porque el switch necesita inspeccionar cada paquete y observar si coincide con una de las reglas de la ACL definida en el switch. Se realiza la inspección en la capa de distribución porque los switches en esta capa habitualmente tienen capacidad de procesamiento como para manejar la carga adicional y también dichacapa simplifica el uso de las ACL. En vez de utilizar las ACL para cada switch de capa de acceso en la red, las mismas se definen en los switches de capa de distribución, que son menos y hacen que la administración de las ACL sea más fácil.

Calidad de servicio

Los switches de capa de distribución también necesitan admitir QoS para mantener la prioridad del tráfico que proviene de los switches de capa de acceso que implementaron QoS. Las políticas de prioridad aseguran que se garantice el ancho de banda adecuado para las comunicaciones de audio y video a fin de mantener una calidad aceptable del servicio. Para mantener la prioridad de los datos de voz a través de la red, todos los switches que envían datos de voz deben admitir QoS; si la totalidad de los dispositivos de la red no admite QoS, sus beneficios se reducen. Esto produce rendimiento y calidad deficientes en las comunicaciones de video.

Los switches de capa de distribución tienen alta demanda en la red debido a las funciones que desempeñan. Es importante que los switches de distribución admitan redundancia para una disponibilidad adecuada. La pérdida de un switch de capa de distribución podría afectar en gran medida al resto de la red porque todo el tráfico de capa de acceso pasa a través de los switches de capa de distribución. Normalmente, los switches de capa de distribución se implementan en pares para asegurar la disponibilidad. Además, se recomienda que los switches de capa de distribución admitan fuentes de energía múltiples, intercambiables en caliente. La disposición de más de una fuente de energía permite que el switch continúe operando incluso si una de las fuentes de energía falló durante el funcionamiento. Si posee fuentes de energía intercambiables en caliente, puede cambiar una fuente de energía que falla mientras el switch se está ejecutando. Esto permite reparar el componente con fallas sin afectar la funcionalidad de la red.

Finalmente, los switches de capa de distribución necesitan admitir el agregado de enlaces. Habitualmente, los switches de capa de acceso utilizan enlaces múltiples para conectarse a un switch de capa de distribución para asegurar el adecuado ancho de banda y así adaptar el tráfico generado en la capa de acceso y aportar tolerancia ante fallas en caso de que se pierda un enlace. Debido a que los switches de capa de distribución aceptan el tráfico entrante de múltiples switches de capa de acceso, necesitan enviar todo ese tráfico tan rápido como sea posible a los switches de capa núcleo. Como resultado, los switches de capa de distribución también necesitan enlaces agregados de un alto ancho de banda de regreso a los switches de capa núcleo. Los switches más nuevos de capa de distribución admiten enlaces agregados de 10 Gigabit Ethernet (10GbE) en los switches de capa núcleo.



Características del switch de capa núcleo

La capa núcleo de una topología jerárquica es una backbone de alta velocidad de la red y requiere switches que pueden manejar tasas muy altas de reenvío. La tasa de reenvío requerida depende en gran medida del número de dispositivos que participan en la red. Determine su tasa de reenvío necesaria mediante la realización y el examen de varios informes de flujo de tráfico y análisis de las comunidades de usuarios. En base a sus resultados, puede identificar un switch apropiado para admitir la red. Tome la precaución de evaluar sus necesidades para el presente y el futuro cercano. Si opta por un switch inadecuado para ejecutar el núcleo de la red, enfrentará los problemas potenciale con cuellos de botella enel núcleo y contribuirá a que todas las comunicaciones en la red se vuelvan más lentas.

Agregado de enlaces

La capa núcleo también necesita admitir el agregado de enlaces para asegurar el ancho de banda adecuado que ingresa al núcleo proveniente de los switches de capa de distribución. Los switches de capa de distribución deben tener soporte para conexiones agregadas de 10GbE, que en la actualidad es la opción de conectividad Ethernet disponible de mayor velocidad. Esto permite que los correspondientes switches de capa de distribución distribuyan el tráfico con la mayor eficiencia posible al núcleo.

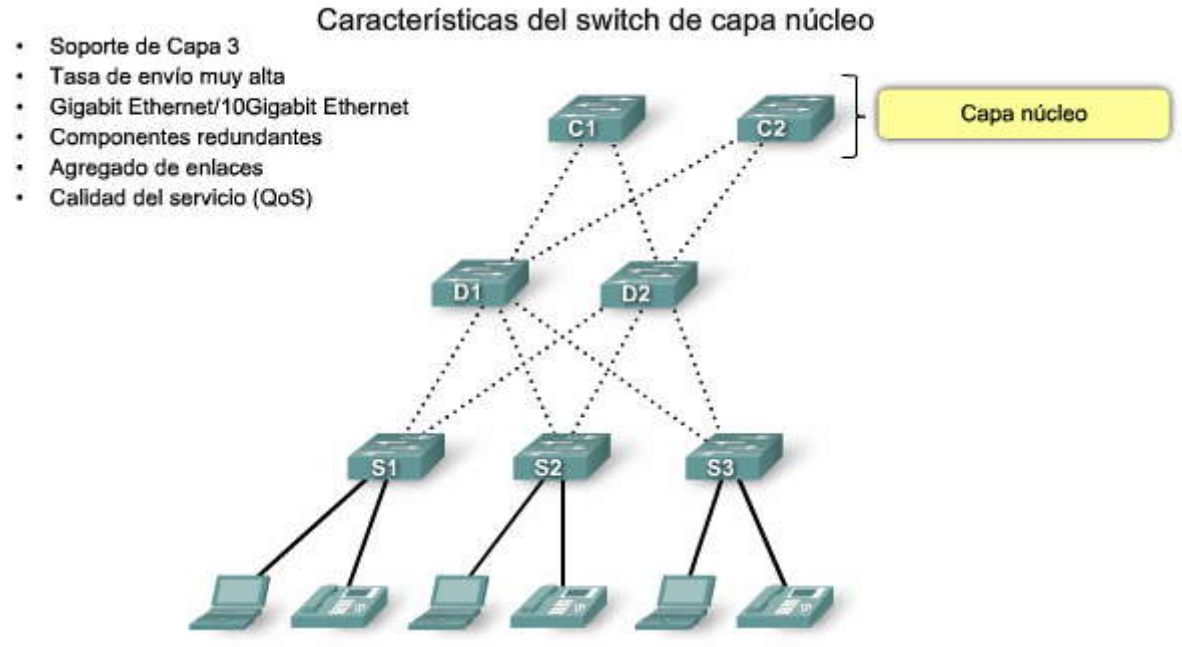
Redundancia

La disponibilidad de la capa núcleo es también esencial para crear tanta redundancia como se pueda. Normalmente, la redundancia de la Capa 3 presenta una convergencia más veloz que la redundancia de la Capa 2 en caso de falla del hardware. La convergencia en este contexto hace referencia al tiempo que le consume a la red la adaptación a un cambio y no debe confundirse con una red convergente que admite comunicaciones de datos, audio y video. Con ese concepto en mente, necesita asegurarse de que sus switches de capa núcleo admiten las funciones de la Capa 3. Un análisis completo sobre las implicaciones de la redundancia de la Capa 3 excede el alcance de este curso. La necesidad de redundancia de la Capa 2 en este contexto continúa siendo una cuestión pendiente. La redundancia de la Capa 2 se examina en el capítulo 5, donde se trata el protocolo spanning tree (STP). Además, busque los switches de capa núcleo que admiten las características de redundancia del hardware adicional como fuentes de energía redundante que pueden intercambiarse mientras el switch continúa funcionando. Debido a la alta carga de trabajo que transportan los switches de capa núcleo, tienden a funcionar con más temperatura que los switches de capa de acceso o de distribución, y entonces deben contar con opciones de refrigeración más sofisticadas. Muchos switches verdaderos con capacidad de capa núcleo presentan la habilidad de intercambiar ventiladores de refrigeración sin necesidad de apagar el switch.

Por ejemplo, sería perjudicial apagar un switch de capa núcleo para cambiar una fuente de energía o un ventilador en la mitad del día cuando el uso de la red está en su máximo punto. Para realizar un reemplazo de hardware se podría considerar una interrupción de la red de al menos 5 minutos si se es muy veloz para realizar el mantenimiento. En una situación más realista, el switch podría estar desconectado durante 30 minutos o más yes probable que esta situación no sea aceptable. Con hardware intercambiable en caliente no se realizan interrupciones durante el mantenimiento de los switches.

QoS es una parte importante de los servicios prestados por los switches de capa núcleo. Por ejemplo, los prestadores de servicios (que suministran IP, almacenamiento de datos, correo electrónico y otros servicios) y las Redes de área extensa

(WAN) de las empresas, están adicionando mayor tráfico de voz y video a una cantidad de tráfico de datos encrecimiento. En el núcleo y el extremo de la red, el tráfico fundamental y sensible a los tiempos como la voz debe recibir garantías superiores de QoS que el tráfico de menor sensibilidad a los tiempos como las transferencias de archivos o el correo electrónico. Debido a que el acceso a la WAN de alta velocidad es con frecuencia extremadamente costoso, la suma de ancho de banda en la capa núcleo no es una opción. Ya que QoS proporciona una solución basada en software para priorizar el tráfico, los switches de capa núcleo pueden suministrar una manera rentable de admitir uso óptimo y diferenciado del ancho de banda existente.



1.2.4 SWITCHES PARA PEQUEÑAS Y MEDIANAS EMPRESAS (SMB)

Características de los switches Cisco Catalyst

Ahora que conoce qué características de los switches se utilizan en qué capa en una red jerárquica, aprenderá acerca de los switches Cisco que son aplicables para cada capa en un modelo de red jerárquica. Actualmente, no se puede seleccionar un switch Cisco teniendo en cuenta sólo el tamaño de una empresa. Una empresa pequeña con 12 empleados podría estar integrada en la red de una empresa multinacional y requerir todos los servicios de LAN avanzados disponibles en la oficina central corporativa. La siguiente clasificación de los switches Cisco dentro de un modelo de redes jerárquicas representa un punto de partida para sus decisiones con respecto a qué switch es mejor para una aplicación dada. La clasificación presentada refleja cómo podría ver el rango de los switches Cisco si fuese una empresa multinacional. Por ejemplo, las densidades de los puertos del switch Cisco 6500 sólo tienen sentido como un switch de capa de acceso en el que existen muchos cientos de usuarios en un área, como el piso de una bolsa de valores. Si considera las necesidades de una empresa mediana, un switch que se muestra como un switch de capa de acceso, por ejemplo, el switch Cisco 3560, podría utilizarse como un switch de capa de distribución si cumpliese los criterios determinados por el diseñador de red para esa aplicación.

Cisco tiene siete líneas de productos de switches. Cada línea de producto ofrece diferentes características y funciones, que permiten hallar el switch correcto que cumpla con los requerimientos funcionales de su red. Las líneas de productos de switches de Cisco son:

Catalyst Express 500
Catalyst 2960
Catalyst 3560
Catalyst 3750
Catalyst 4500
Catalyst 4900
Catalyst 6500

Catalyst Express 500

Catalyst Express 500 es el switch de capa de entrada de Cisco. Ofrece lo siguiente:

Tasas de reenvío desde 8,8 Gb/s a 24 Gb/s
Seguridad de puerto de la Capa 2

Administración basada en Web
Soporte de comunicaciones de datos convergentes/IP

Esta serie de switches es apropiada para las implementaciones de la capa de acceso en las que no se requiere una densidad alta de puerto. Los switches de la serie Cisco Catalyst Express 500 son escalados para ámbitos de pequeñas empresas con un número de empleados que oscila entre 20 y 250. Los switches de la serie Catalyst Express 500 se encuentran disponibles en diferentes configuraciones fijas.

Conectividad Fast Ethernet y Gigabit Ethernet
Hasta 24 puertos de 10/100 con PoE opcional ó 12 puertos de 10/100/1000

Los switches de la serie Catalyst Express 500 no permiten administración mediante IOS CLI de Cisco. Se administran con el uso de la interfaz de administración de Web incorporada, Cisco Network Assistant o el nuevo Cisco Configuration Manager desarrollados específicamente para los switches de la serie Catalyst Express 500. Catalyst Express no admite acceso a la consola.

Para obtener más información acerca de la serie Cisco Express 500 de switches, visite http://www.cisco.com/en/US/products/ps6545/index.html.

Catalyst 2960

Los switches de la serie Catalyst 2960 habilitan a las redes de capa de entrada de empresas medianas y de sucursales para prestar servicios de LAN mejorados. Los switches de la serie Catalyst 2960 son apropiados para las implementaciones de la capa de acceso en las que el acceso a la fuente de energía y al espacio es limitado. Los laboratorios de Conmutación de LAN e Inalámbrico de CCNA Exploration 3 se basan en las características del switch Cisco 2960.

Los switches de la serie Catalyst 2960 ofrecen lo siguiente:

Tasas de reenvío de 16 Gb/s a 32 Gb/s
Switching de capas múltiples
Características de QoS para admitir comunicaciones IP
Listas de control del acceso (ACL)
Conectividad Fast Ethernet y Gigabit Ethernet
Hasta 48 puertos de 10/100 o puertos de 10/100/1000 con enlaces gigabit adicionales de doble propósito

La serie Catalyst 2960 de switches no admite PoE.

La serie Catalyst 2960 admite Cisco IOS CLI, interfaz de administración de Web integrada y Cisco Network Assistant. La serie de switches admite acceso de consola y auxiliar al switch.

Para obtener más información acerca de la serie Catalyst 2960 de switches, visite http://www.cisco.com/en/US/products/ps6406/index.html.

Catalyst 3560

La serie Cisco Catalyst 3560 es una línea de switches de clase empresarial que incluyen soporte para PoE, QoS y características de seguridad avanzada como ACL. Estos switches son los switches de capa de acceso ideales para acceso a la LAN de pequeñas empresas o ámbitos de redes convergentes de sucursales.

La serie Cisco Catalyst 3560 admite tasas de reenvío de 32 Gb/s a 128 Gb/s (serie de switches Catalyst 3560-E).

Los switches de la serie Catalyst 3560 se encuentran disponibles en diferentes configuraciones fijas:

Conectividad Fast Ethernet y Gigabit Ethernet
Hasta 48 puertos de 10/100/1000, más cuatro puertos pequeños de factor de forma enchufables (SFP)
Conectividad opcional de 10 Gigabit Ethernet en los modelos Catalyst 3560-E
PoE integrada opcional (Cisco pre estándar y IEEE 802.3af); hasta 24 puertos con 15,4 vatios o 48 puertos con 7,3 vatios

Para obtener más información acerca de la serie de switches Catalyst 3560, visite http://www.cisco.com/en/US/products/hw/switches/ps5528/index.html.

Catalyst 3750

La serie de switches Cisco Catalyst 3750 es ideal para los switches de capa de acceso en organizaciones medianas y en sucursales empresariales. Esta serie ofrece tasas de reenvío de 32 Gb/s a 128 Gb/s (serie de switches Catalyst 3750-E). La serie Catalyst 3750 admite la tecnología StackWise de Cisco. La tecnología StackWise permite interconectar hasta nueve switches físicos Catalyst 3750 en un switch lógico con el uso de una conexión backplane, redundante, de alto rendimiento (32 Gb/s).

Los switches de la serie Catalyst 3750 se encuentran disponibles en diferentes configuraciones fijas apilables:

Conectividad Fast Ethernet y Gigabit Ethernet
Hasta 48 puertos de 10/100/1000, más cuatro puertos SFP
Conectividad opcional de 10 Gigabit Ethernet en los modelos Catalyst 3750-E
PoE integrada opcional (Cisco preestándar y IEEE 802.3af); hasta 24 puertos con 15,4 vatios o 48 puertos con 7,3 vatios

Para obtener más información acerca de la serie de switches Catalyst 3750, visite
http://www.cisco.com/en/US/products/hw/switches/ps5023/index.html.

Catalyst 4500

Catalyst 4500 es la primera plataforma de switching modular de rango mediano que ofrece switching de multicapas para empresas, pequeñas o medianas compañías y prestadores de servicios.

Con tasas de reenvío de hasta 136 Gb/s, la serie Catalyst 4500 puede administrar el tráfico a la capa de distribución. La capacidad modular de la serie Catalyst 4500 permite densidades de puerto muy altas mediante el agregado de tarjetas de líneas del puerto de switches a su chasis modular. La serie Catalyst 4500 ofrece QoS de multicapas y funciones de enrutamiento sofisticadas.

Los switches de la serie Catalyst 4500 se encuentran disponibles en diferentes configuraciones modulares:

El chasis modular de 3, 6, 7 y 10 ranuras ofrece diferentes capas de escalabilidad
Alta densidad de puerto: hasta 384 puertos Fast Ethernet o Gigabit Ethernet disponibles en cobre o fibracon 10 enlaces Gigabit
PoE (Cisco preestándar y IEEE 802.3af)
suministros de energía AC o DC interna, dual, intercambiable en caliente
Capacidades de enrutamiento IP avanzadas asistidas por hardware

Para obtener más información acerca de la serie de switches Catalyst 4500, visite
http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html.

Catalyst 4900

Los switches de la serie Catalyst 4900 están diseñados y optimizados para el switching del servidor al permitir tasas de reenvío muy altas. Cisco Catalyst 4900 no es un switch típico de la capa de acceso. Es un switch especial de la capa de acceso diseñado para implementaciones del centro de datos en donde es posible que haya muchos servidores cercanos. La serie de switches admite suministros de energía redundante y dual además de ventiladores que se pueden intercambiar mientras el switch se está ejecutando. Esto permite que los switches logren una disponibilidad superior, que es esencial en las implementaciones de centros de datos.

Los switches de la serie Catalyst 4900 admiten características avanzadas de QoS y se convierten en los candidatos ideales para el hardware de telefonía IP de extremo posterior. Los switches de la serie Catalyst 4900 no admiten la característica StackWise de la serie Catalyst 3750 ni admiten PoE.

Los switches de la serie Catalyst 4900 se encuentran disponibles en diferentes configuraciones fijas:

Hasta 48 puertos de 10/100/1000 con cuatro puertos SFP ó 48 puertos de 10/100/1000 con dos puertos de 10GbE
Suministros de energía AC o DC dual, intercambiable en caliente
Bandejas de ventiladores intercambiables en caliente

Para obtener más información acerca de la serie de switches Catalyst 4900, visite http://www.cisco.com/en/US/products/ps6021/index.html.

Catalyst 6500

El switch modular de la serie Catalyst 6500 se optimiza para redes seguras, convergentes de voz, video y datos. Catalyst 6500 puede administrar el tráfico en las capas de distribución y núcleo. La serie Catalyst 6500 es el switch de Cisco de más alto rendimiento, que admite tasas de reenvío de hasta 720 Gb/s. Catalyst 6500 es ideal para ámbitos de redes muy grandes hallados en empresas, compañías medianas y prestadores de servicios.

Los switches de la serie Catalyst 6500 se encuentran disponibles en diferentes configuraciones modulares:

Chasis modular de 3, 4, 6, 9 y 13 ranuras
Módulos de servicio de LAN/WAN
Dispositivos PoE hasta 420 IEEE 802.3af de Clase 3 (15,4W)
Hasta 1152 puertos de 10/100, 577 puertos de 10/100/1000, 410 puertos SFP Gigabit Ethernet ó 64 puertos de 10 Gigabit Ethernet
Suministros de energía AC o DC internos, duales, intercambiables en caliente
Capacidades de enrutamiento IP avanzadas, asistidas por hardware

Para obtener más información acerca de la serie de switches Catalyst 6500, visite http://www.cisco.com/en/US/products/hw/switches/ps708/index.html

La siguiente herramienta puede ayudarlo a identificar el switch correcto para una implementación: http://www.cisco.com/en/US/products/hw/switches/products_promotion0900aecd8050364f.html

La siguiente guía aporta una comparación detallada de las ofertas actuales de switches de Cisco: http://www.cisco.com/en/US/prod/switches/ps5718/ps708/networking_solutions_products_genericcontent0900aecd805f0955.pdf.

Características de las capas del modelo jerárquico

	Acceso	Distribución	Núcleo
Agregado de ancho de banda	✓	✓	✓
Fast Ethernet/Gigabit Ethernet	✓		
Gigabit Ethernet/10Gigabit Ethernet		✓	✓
Tasa alta de envío		✓	
Soporte de la capa 3		✓	✓
Seguridad del puerto	✓		
Power over Ethernet(PoE)	✓		
Calidad del servicio (QoS)	✓	✓	✓
Componentes redundantes		✓	✓
Políticas de seguridad/listas de control de acceso		✓	
Tasa muy alta de envío			✓
VLAN	✓		

CAPITULO II – "CONFIGURACIÓN Y CONCEPTOS BÁSICOS DEL SWITCH"

2.0 INTRODUCCIÓN DEL CAPITULO.-

2.0.1 INTRODUCCIÓN DEL CAPITULO.-

En este capítulo, el estudiante se basará en los conocimientos adquiridos en CCNA Exploration 4.0: Aspectos básicos de redes, para repasar y reforzar dichos conocimientos mediante actividades de práctica exhaustiva. Adquirirá conocimientos sobre ciertas amenazas malintencionadas para los switches y aprenderá a activar un switch con una configuración inicial segura.

En este capítulo aprenderá a:

- Resumir el funcionamiento de Ethernet como se definió para las LAN de 100/1 000 Mbps en el estándar IEEE 802.3.
- Explicar las funciones que permiten que un switch envíe tramas de Ethernet en una LAN.
- Configurar un switch para que funcione en una red diseñada para admitir transmisiones de voz, video y datos.
- Configurar la seguridad básica de un switch que funciona en una red diseñada para admitir transmisiones de voz, video y datos.

2.1 INTRODUCCION A LAS LAN 802.3/ETHERNET.-

2.1.1 ELEMENTOS CLAVE DE LAS REDES 802.3/ETHERNET.-

En este tema, se describirán los componentes clave del estándar Ethernet que desempeñan un importante papel en el diseño y en la implementación de las redes de conmutación. Se analizará cómo funcionan las comunicaciones Ethernet y el papel que desempeñan los switches en el proceso de comunicación.

CSMA/CD

Las señales de Ethernet se transmiten a todos los hosts que están conectados a la LAN mediante un conjunto de normas especiales que determinan cuál es la estación que puede tener acceso a la red. El conjunto de normas que utiliza Ethernet está basado en la tecnología de acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) IEEE. Seguramente recordará de CCNA Exploration: Aspectos básicos de networking, que CSMA/CD se utiliza solamente con la comunicación half-duplex que suele encontrarse en los hubs. Los switches full-duplex no utilizan CSMA/CD.

Detección de portadora

En el método de acceso CSMA/CD Método de acceso, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir.

Si un dispositivo detecta una señal de otro dispositivo, espera un período determinado antes de intentar transmitirla.

Cuando no se detecta tráfico alguno, el dispositivo transmite su mensaje. Mientras se produce dicha transmisión, el dispositivo continúa atento al tráfico o a posibles colisiones en la LAN. Una vez enviado el mensaje, el dispositivo vuelve al modo de escucha predeterminado.

Acceso múltiple

Si la distancia entre los dispositivos es tal que la latencia de las señales de un dispositivo supone la no detección de éstas por parte de un segundo dispositivo, éste también podría comenzar a transmitirlas. De este modo, los medios contarían con dos dispositivos transmitiendo señales al mismo tiempo. Los mensajes se propagan en todos los medios hasta que se encuentran. En ese momento, las señales se mezclan y los mensajes se destruyen: se ha producido una colisión. Aunque los mensajes se dañan, la mezcla de señales continúa propagándose en todos los medios.

Detección de colisiones

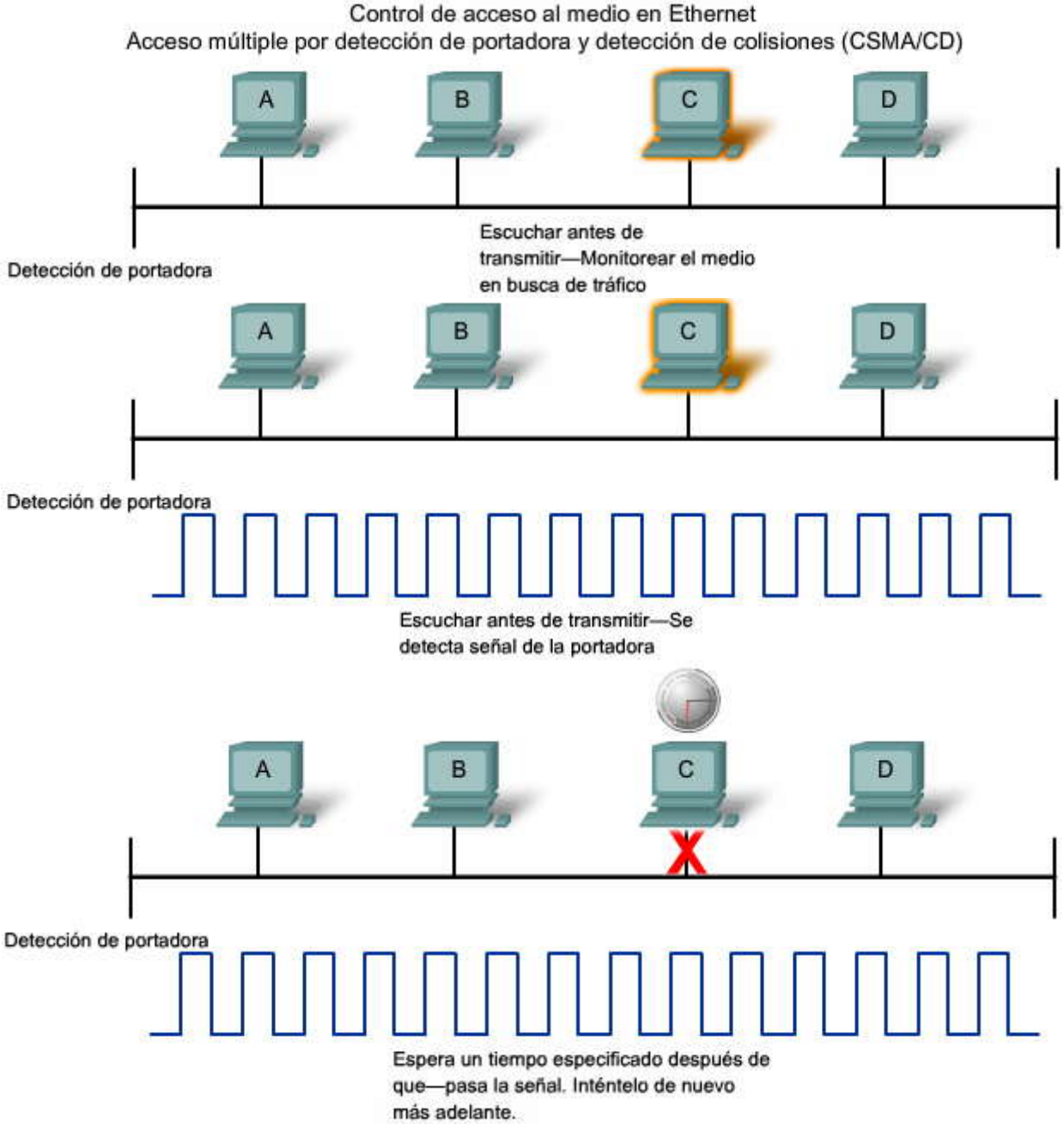
Cuando un dispositivo está en el modo de escucha, puede detectar cuando se produce una colisión en los medios compartidos, ya que todos los dispositivos pueden detectar un aumento en la amplitud de la señal que esté por encima del nivel normal.

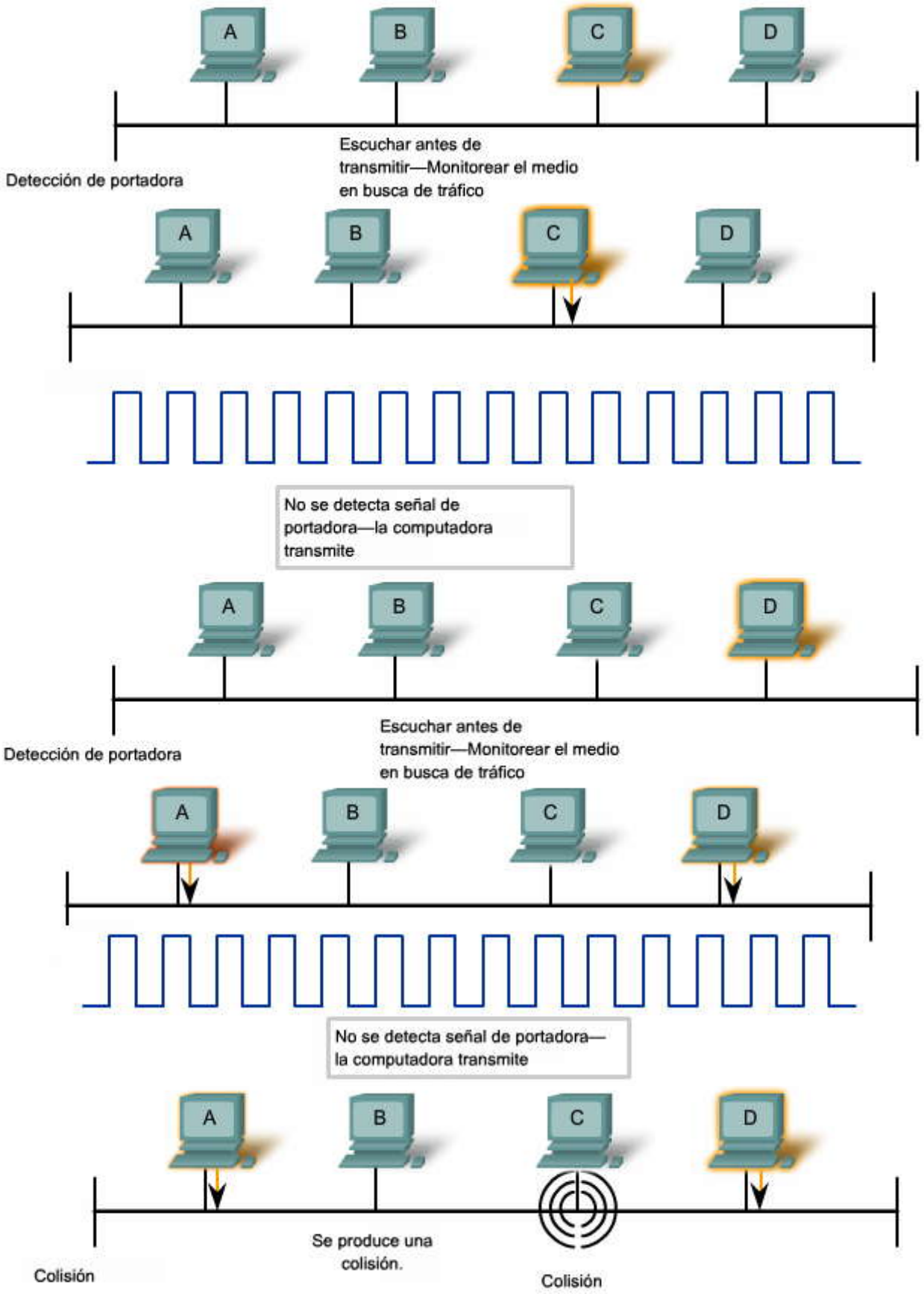
Cuando se produce una colisión, los demás dispositivos que están en el modo de escucha, además de todos los dispositivos de transmisión, detectan el aumento de amplitud de la señal. Todos los dispositivos que estén transmitiendo en ese momento lo seguirán haciendo, para garantizar que todos los dispositivos en la red puedan detectar la colisión.

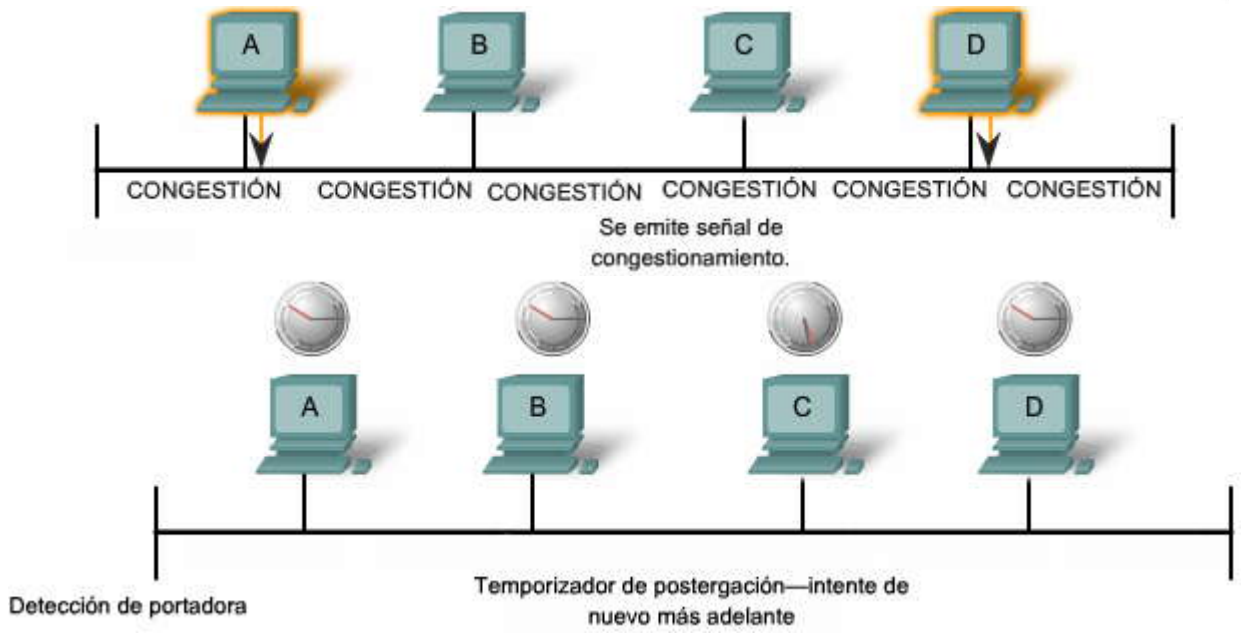
Señal de congestión y postergación aleatoria

Cuando se detecta una colisión, los dispositivos de transmisión envían una señal de congestionamiento. La señal de congestionamiento avisa a los demás dispositivos acerca de la colisión para que éstos invoquen un algoritmo de postergación. La función de éste es hacer que todos los dispositivos detengan su transmisión durante un período aleatorio, con lo cual se reducen las señales de colisión.

Una vez que finaliza el retraso asignado a un dispositivo, dicho dispositivo regresa al modo "escuchar antes de transmitir". Un período de postergación aleatorio garantiza que los dispositivos involucrados en la colisión no intenten enviar tráfico nuevamente al mismo tiempo, lo que provocaría que se repita todo el proceso. Sin embargo, durante el período de postergación es posible que un tercer dispositivo transmita antes de que cualquiera de los dos involucrados en la colisión tengan oportunidad de volver a transmitir.




A
B
C
D
Escuchar antes de transmitir—Monitorear el medio en busca de tráfico
Detección de portadora
A
B
C
D
No se detecta señal de portadora—la computadora transmite
A
B
C
D
Escuchar antes de transmitir—Monitorear el medio en busca de tráfico
Detección de portadora
A
B
C
D
No se detecta señal de portadora—la computadora transmite
A
B
C
D
Se produce una colisión.
Colisión
Colisión



Comunicaciones Ethernet

Consulte el área de Comunicaciones Ethernet seleccionada en la figura.

Las comunicaciones en una red LAN conmutada se producen de tres maneras: unicast, broadcast y multicast:

Unicast: Comunicación en la que un host envía una trama a un destino específico. En la transmisión unicast sólo existen un emisor y un receptor. La transmisión unicast es el modo de transmisión predominante en las LAN y en Internet. Algunos ejemplos de transmisiones unicast son: HTTP, SMTP, FTP y Telnet.

Broadcast: Comunicación en la que se envía una trama desde una dirección hacia todas las demás direcciones. En este caso, existe sólo un emisor pero se envía la información a todos los receptores conectados. La transmisión broadcast es fundamental cuando se envía el mismo mensaje a todos los dispositivos de la LAN. Un ejemplo de transmisión broadcast es la consulta de resolución de direcciones que envía el protocolo de resolución de direcciones (ARP) a todas las computadoras en una LAN.

Multicast: Comunicación en la que se envía una trama a un grupo específico de dispositivos o clientes. Los clientes de la transmisión multicast deben ser miembros de un grupo multicast lógico para poder recibir la información. Un ejemplo de transmisión multicast son las transmisiones de voz y video relacionadas con las reuniones de negocios en conferencia basadas en la red.

Trama de Ethernet

Haga clic en el botón Trama de Ethernet que se muestra en la figura.

El primer curso de la serie, CCNA Exploration: Aspectos básicos de networking, describe la estructura de la trama de Ethernet en forma detallada. Para realizar un breve resumen, la estructura de la trama de Ethernet agrega encabezados y tráilers alrededor de la Capa 3 PDU para encapsular el mensaje que debe enviarse. Tanto el tráiler como el encabezado de Ethernet cuentan con varias secciones (o campos) que el protocolo Ethernet utiliza. Lafigura muestra la estructura del estándar de la trama actual de Ethernet, versión revisada IEEE 802.3 (Ethernet).

Desplace el mouse sobre los nombres de los campos para ver las descripciones.

Campos Preámbulo y Delimitador de inicio de trama

Loa campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD) (1 byte) se utilizan para la sincronización entre los dispositivos emisores y receptores. Estos primeros 8 bytes de la trama se emplean para captar la atención de los nodos receptores. Básicamente, los primeros bytes sirven para que los receptores se preparen para recibir una nueva trama.

Campo Dirección MAC de destino

El campo Dirección MAC de destino (6 bytes) es el identificador del receptor deseado. La Capa 2 utiliza esta dirección para ayudar a que un dispositivo determine si la trama está dirigida a él. Se compara la dirección de la trama con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.

Campo Dirección MAC origen

El campo Dirección MAC de origen (6 bytes) identifica la NIC o interfaz que origina la trama. Los switches utilizan esta dirección para agregar dicha interfaz a sus tablas de búsqueda.

Campo Longitud/tipo

El campo Longitud/Tipo (2 bytes) define la longitud exacta del campo Datos de la trama. Este campo se utiliza más adelante como parte de la Secuencia de verificación de trama (FCS) con el objeto de asegurar que se haya recibido el mensaje de manera adecuada. Aquí se puede ingresar solamente el tipo o la longitud de una trama. Si el objetivo deun campo es designar un tipo, el campo Tipo describe cuál es el protocolo que se implementa. Cuando un nodo recibe una trama y el campo Tipo/Longitud designa un tipo, el nodo determina qué protocolo de capa superior está presente. Si el valor de los dos octetos es igual o mayor que el hexadecimal de 0x0600 o decimal de 1536, el contenido del campo Datos se descifra según el protocolo indicado. Si el valor de dos bytes es menor que 0x0600, entonces el valor representa la longitud de los datos de la trama.

Campos Datos y Relleno

Los campos Datos y Relleno (de 46 a 1500 bytes) contienen la información encapsulada de una capa superior, que es una PDU de Capa 3 genérica, o, más comúnmente, un paquete de IPv4. Todas las tramas deben tener una longitud mínima de 64 bytes (longitud mínima que colabora en la detección de colisiones). Si se encapsula un paquete menor, el campo Relleno se utiliza para incrementar el tamaño de la trama hasta alcanzar el tamaño mínimo.

Campo Secuencia de verificación de trama

El campo FCS (4 bytes) detecta errores en una trama. Utiliza una comprobación de redundancia cíclica (CRC). El dispositivo emisor incluye los resultados de la CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para buscar errores. Si los cálculos coinciden, no se ha producido ningún error. Si los cálculos no coinciden, la trama se descarta.

Dirección MAC

Haga clic en el botón Dirección MAC que se muestra en la figura.

En CCNA Exploration: Aspectos básicos de networking, aprendió sobre la dirección MAC. Una dirección Ethernet MAC es un valor binario de 48 bits que se compone de dos partes y se expresa como 12 dígitos hexadecimales. Los formatos de las direcciones pueden ser similares a 00-05-9A-3C-78-00, 00:05:9A:3C:78:00 ó 0005.9A3C.7800.

Todos los dispositivos conectados a una LAN Ethernet tienen interfaces con direcciones MAC. La NIC utiliza la dirección MAC para determinar si deben pasarse los mensajes a las capas superiores para su procesamiento. La dirección MAC está codificada de manera permanente dentro de un chip ROM en una NIC. Este tipo de dirección MAC se denomina dirección grabada (BIA, Burned In Address). Algunos fabricantes permiten que se modifiquen las direcciones MAC de manera local. La dirección MAC se compone del identificador exclusivo de organización (OUI) y del número de asignación del fabricante.

Desplace el mouse sobre los nombres de los campos para ver las descripciones.

Identificador Exclusivo de Organización

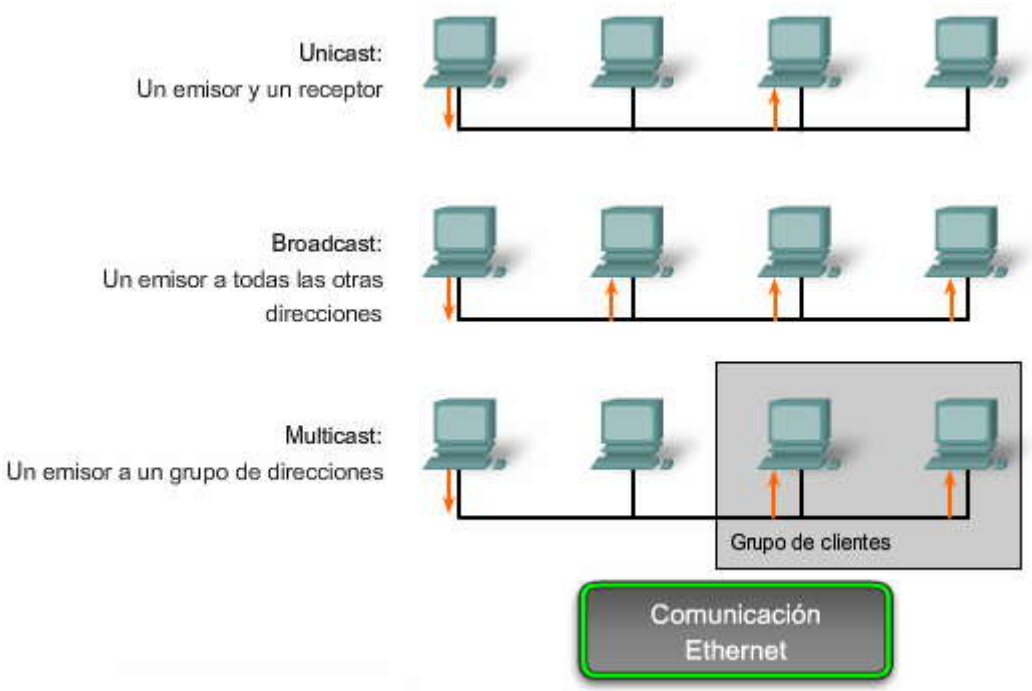
El OUI es la primera parte de una dirección MAC. Tiene una longitud de 24 bits e identifica al fabricante de la tarjeta NIC. El estándar IEEE regula la asignación de los números de OUI. Dentro del OUI, existen 2 bits que sólo tienen significado cuando se utilizan en la dirección de destino, como se describe a continuación:

Bit multicast o broadcast: Indica a la interfaz receptora que la trama está destinada a un grupo o a todas las estaciones finales del segmento de la LAN.

Bit de direcciones administrado de manera local: Si la dirección MAC asignada por el fabricante puede modificarse en forma local, éste es el bit que debe configurarse.

Número de asignación del fabricante

La parte de la dirección MAC asignada por el fabricante es de 24 bits de longitud e identifica exclusivamente el hardware de Ethernet. Puede ser una BIA o bien con el bit modificado en forma local mediante software.



Desplace el mouse sobre cada nombre de campo para ver la descripción.

Desplace el mouse sobre cada nombre de campo para ver la descripción.

Configuración de Duplex

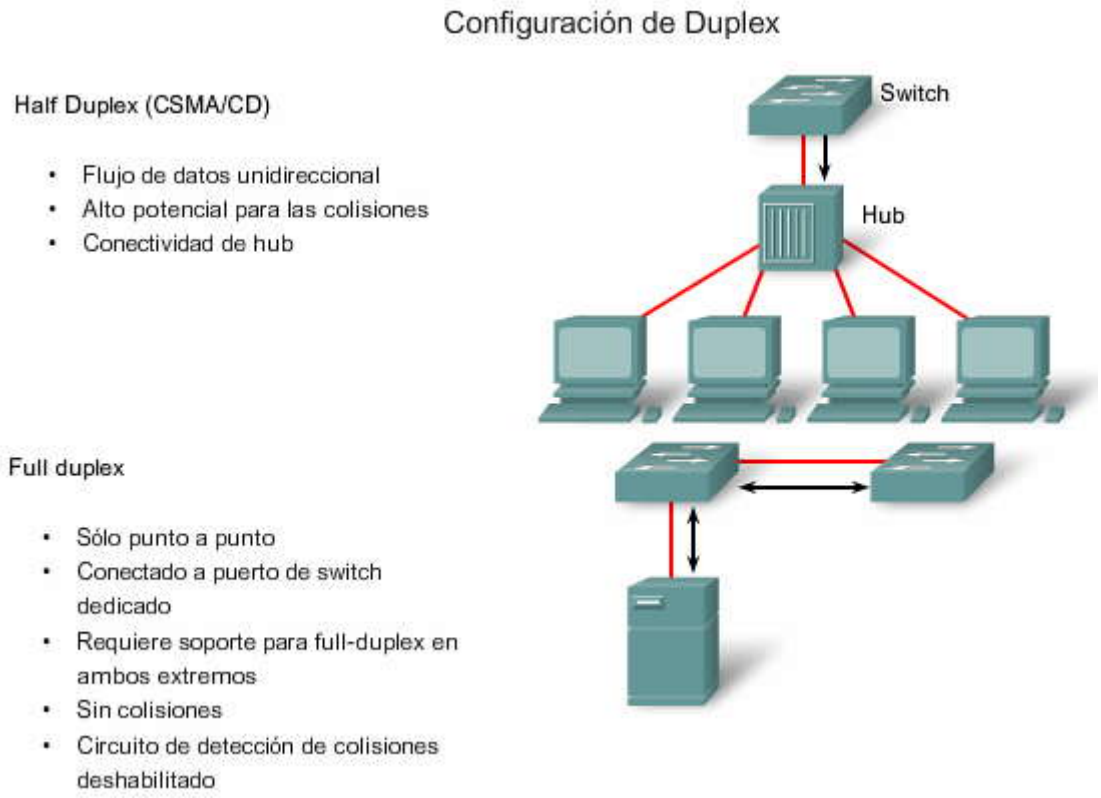
Se utilizan dos tipos de parámetros duplex para las comunicaciones en una red Ethernet: half duplex y full duplex. La figura muestra los dos parámetros dúplex que están disponibles en los equipos de red modernos.

Half Duplex: La comunicación half-duplex se basa en un flujo de datos unidireccional en el que el envío y la recepción de datos no se producen al mismo tiempo. Esto es similar a la función de las radios de dos vías o dos walki-talkies en donde una sola persona puede hablar a la vez. Si una persona habla mientras lo hace la otra, se produce una colisión. Por ello, la comunicación half-duplex implementa el CSMA/CD con el objeto de reducir las posibilidades de que se produzcan colisiones y detectarlas en caso de que se presenten. Las comunicaciones half-duplex presentan problemas de funcionamiento debido a la constante espera, ya que el flujo de datos sólo se produce en una dirección a la vez. Las conexiones half-duplex suelen verse en los dispositivos de hardware más antiguos, como los hubs. Los nodos que están conectados a los hubs y que comparten su conexión con un puerto de un switch deben funcionar en el modo half-duplex porque las computadoras finales tienen que tener la capacidad de detectar las colisiones. Los nodos pueden funcionar en el

modo half-duplex si la tarjeta NIC no puede configurarse para hacerlo en full duplex. En este caso, el puerto del switch también adopta el modo half-duplex predeterminado. Debido a estas limitaciones, la comunicación full-duplex ha reemplazado a la half duplex en los elementos de hardware más modernos.

Full duplex: En las comunicaciones full-duplex el flujo de datos es bidireccional, por lo tanto la información puede enviarse y recibirse al mismo tiempo. La capacidad bidireccional mejora el rendimiento, dado que reduce el tiempo de espera entre las transmisiones. Actualmente, la mayoría de las tarjetas NIC Ethernet, Fast Ethernet y Gigabit Ethernet disponibles en el mercado proporciona capacidad full-duplex. En el modo full-duplex, el circuito de detección de colisiones se encuentra desactivado. Las tramas enviadas por los dos nodos finales conectados no pueden colisionar, dado que éstos utilizan dos circuitos independientes en el cable de la red. Cada conexión full-duplex utiliza un solo puerto. Las conexiones full-duplex requieren un switch que admita esta modalidad o bien una conexión directa entre dos nodos compatibles con el modo full duplex. Los nodos que se conecten directamente al puerto de un switch dedicado con tarjetas NIC capaces de admitir full duplex deben conectarse a puertos de switches que estén configurados para funcionar en el modo full-duplex.

El rendimiento de una configuración de red compartida Ethernet estándar basada en hubs es generalmente del 50% al 60% del ancho de banda de 10 Mb/s. Una red Fast Ethernet full-duplex, en comparación con un ancho de banda de 10 Mb/s, ofrece un rendimiento del 100% en ambas direcciones (transmisión de 100 Mb/s y recepción de 100 Mb/s).



Configuración del puerto de switch

El puerto de un switch debe configurarse con parámetros duplex que coincidan con el tipo de medio. Más adelante en este capítulo se configurarán los parámetros de duplex. Los switches Cisco Catalyst cuentan con tres parámetros:

La opción auto establece el modo autonegociación de duplex. Cuando este modo se encuentra habilitado, los dos puertos se comunican para decidir el mejor modo de funcionamiento.
La opción full establece el modo full-duplex.
La opción half establece el modo half-duplex.

Para los puertos 10/100/1000 y Fast Ethernet, la opción predeterminada es auto. Para los puertos 100BASE-FX, la opción predeterminada es full. Los puertos 10/100/1000 funcionan tanto en el modo half-duplex como en el full-duplex cuando se establecen en 10 ó 100 Mb/s, pero sólo funcionan en el modo full-duplex cuando se establecen en 1000 Mb/s.

Nota: El modo autonegociación puede producir resultados impredecibles. De manera predeterminada, cuando la autonegociación falla, el switch Catalyst establece el correspondiente puerto del switch en el modo half-duplex. Este tipo de falla se produce cuando un dispositivo conectado no admite el modo autonegociación. Al configurar eldispositivo en forma manual para que funcione en el modo half-duplex, coincidirá con el modo predeterminado del switch. Sin embargo, pueden producirse errores de autonegociación si se configura el dispositivo en forma manual para que funcione en el modo full-

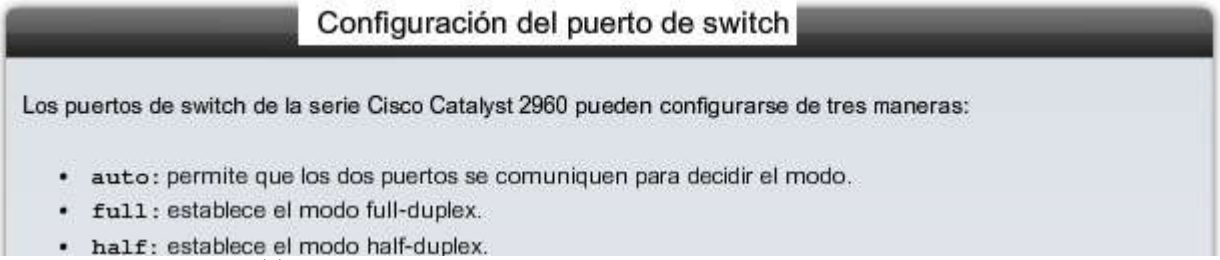
duplex. Al tener half-duplex en un extremo y full-duplex en el otro, pueden producirse colisiones tardías en el extremo de half-duplex. A fin de evitar tal situación, ajuste manualmente los parámetros de duplex del switch para que coincidan con el dispositivo conectado. Si el puerto del switch está en el modo full-duplex y el dispositivo conectado, en el modo half-duplex, verifique si existen errores de FCS en el puerto full-duplex del switch.

auto-MDIX

Las conexiones entre dispositivos específicos, por ejemplo entre switches o entre un switch y un router, solían requerir la utilización de ciertos tipos de cables (de conexión cruzada o conexión directa). Ahora, en cambio, se puede utilizar el comando de configuración de interfaz **mdix auto** de la CLI para habilitar la función automática de conexión cruzada de interfaz dependiente del medio (auto-MDIX).

Al habilitar la función auto-MDIX, el switch detecta el tipo de cable que se requiere para las conexiones Ethernet de cobre y, conforme a ello, configura las interfaces. Por lo tanto, se puede utilizar un cable de conexión directa o cruzada para realizar la conexión con un puerto 10/100/1000 de cobre situado en el switch, independientemente del tipo de dispositivo que se encuentre en el otro extremo de la conexión.

La función auto-MDIX se habilita de manera predeterminada en los switches que ejecutan el software Cisco IOS, versión 12.2(18)SE o posterior. En el caso de las versiones existentes entre Cisco IOS, versión 12.1(14)EA1 y 12.2(18)SE, la función auto-MDIX está deshabilitada de manera predeterminada.



Direccionamiento MAC y Tablas de direcciones MAC de los switches

Los switches emplean direcciones MAC para dirigir las comunicaciones de red a través de su estructura al puerto correspondiente hasta el nodo de destino. La estructura del switch son los circuitos integrados y la programación de máquina adjunta que permite controlar las rutas de datos a través del switch. El switch debe primero saber qué nodos existen en cada uno de sus puertos para poder definir cuál será el puerto que utilizará para transmitir una trama unicast.

El switch determina cómo manejar las tramas de datos entrantes mediante una tabla de direcciones MAC. El switch genera su tabla de direcciones MAC grabando las direcciones MAC de los nodos que se encuentran conectados en cada uno de sus puertos. Una vez que la dirección MAC de un nodo específico en un puerto determinado queda registrada en la tabla de direcciones, el switch ya sabe enviar el tráfico destinado a ese nodo específico desde el puerto asignado a dicho nodo para posteriores transmisiones.

Cuando un switch recibe una trama de datos entrantes y la dirección MAC de destino no figura en la tabla, éste reenvía la trama a todos los puertos excepto al que la recibió en primer lugar. Cuando el nodo de destino responde, el switch registra la dirección MAC de éste en la tabla de direcciones del campo dirección de origen de la trama. En las redes que cuentan con varios switches interconectados, las tablas de direcciones MAC registran varias direcciones MAC para los puertos que conectan los switches que reflejan los nodos de destino. Generalmente, los puertos de los switches que se utilizan para interconectar dos switches cuentan con varias direcciones MAC registradas en la tabla de direcciones.

Para ver cómo funciona lo descrito anteriormente, haga clic en los pasos de la figura.

A continuación se describe este proceso:

Paso 1. El switch recibe una trama de broadcast de la PC 1 en el Puerto 1.

Paso 2. El switch ingresa la dirección MAC de origen y el puerto del switch que recibió la trama en la tabla de direcciones.

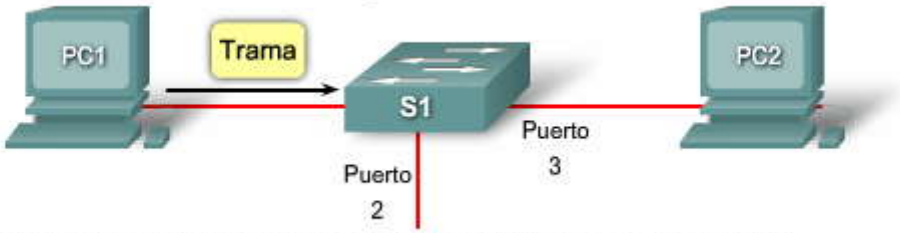
Paso 3. Dado que la dirección de destino es broadcast, el switch genera flooding en todos los puertos enviando la trama, excepto el puerto que la recibió.

Paso 4. El dispositivo de destino responde al broadcast con una trama de unicast dirigida a la PC 1.

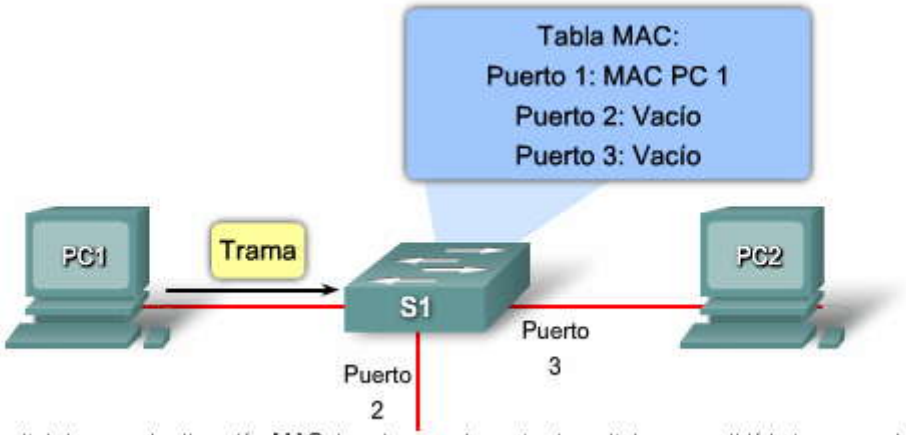
Paso 5. El switch ingresa la dirección MAC de origen de la PC2 y el número de puerto del switch que recibió la trama en la tabla de direcciones. La dirección de destino de la trama y el puerto relacionado a ella se encuentran en la tabla de direcciones MAC.

Paso 6. Ahora el switch puede enviar tramas entre los dispositivos de origen y destino sin saturar el tráfico, ya que cuenta con entradas en la tabla de direcciones que identifican a los puertos asociados.

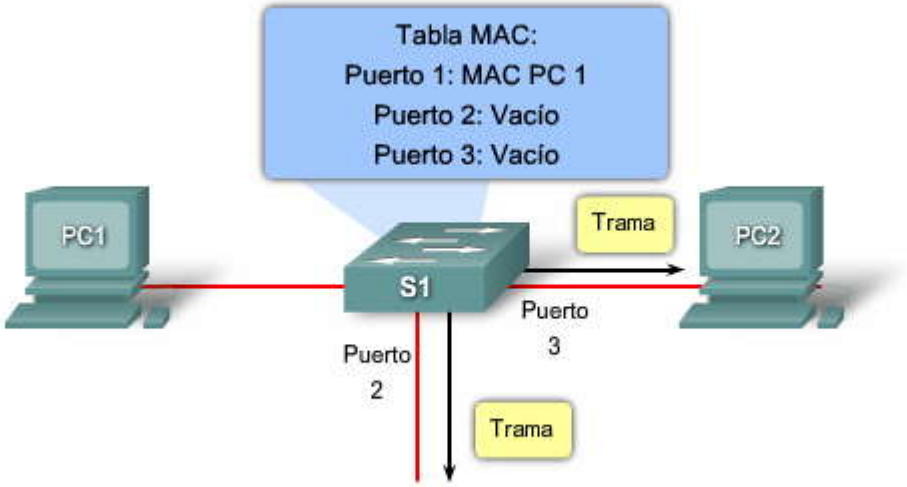
Direcciones MAC y Tablas MAC de los switches



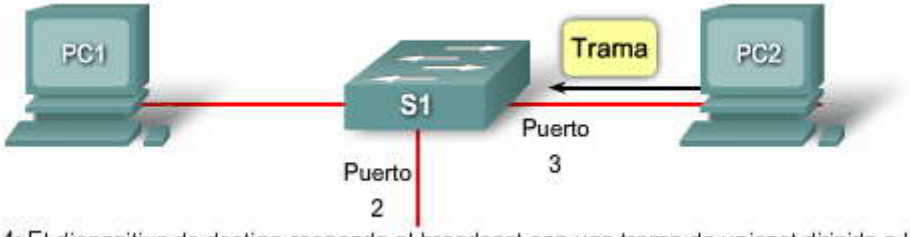
Paso 1: El switch recibe una trama con destino a la PC2 en el puerto 1 de la PC1.



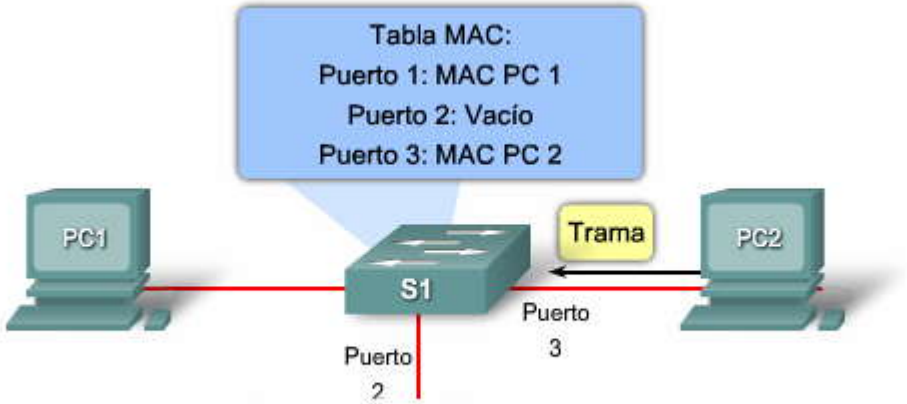
Paso 2: El switch ingresa la dirección MAC de origen y el puerto de switch que recibió la trama en la tabla MAC.



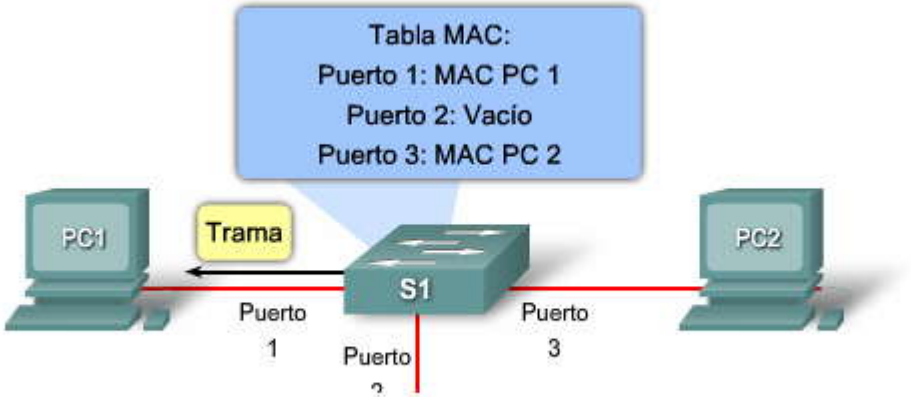
Paso 3: Debido a que la dirección de destino es un broadcast, el switch envía la trama a todos los puertos, excepto al puerto en el cual se recibió la trama.



Paso 4: El dispositivo de destino responde al broadcast con una trama de unicast dirigida a la PC 1.



Paso 5: El switch ingresa la dirección MAC de origen de la PC 2 y el número de puerto del puerto de switch que recibió la trama en la tabla MAC. En la tabla MAC pueden encontrarse la dirección de destino de la trama y su puerto asociado.



Paso 6: Ahora el switch puede enviar tramas entre los dispositivos de origen y destino sin flooding, ya que cuenta con entradas en la tabla MAC que identifican a los puertos asociados.

2.1.2 ASPECTOS QUE SE DEBEN TENER EN CUENTA PARA LAS REDES 802.3/ETHERNET

En este tema, se describirán las pautas de diseño de Ethernet que se necesitan para interpretar los diseños jerárquicos de las redes para las empresas pequeñas y medianas. Este tema se centra en los dominios de colisiónes y de broadcast, y en el modo en que éstos afectan el diseño de las LAN.

Ancho de banda y rendimiento

Una importante desventaja de las redes Ethernet 802.3 son las colisiones. Las colisiones se producen cuando dos hosts transmiten tramas de forma simultánea. Cuando se produce una colisión, las tramas transmitidas se dañan o se destruyen. Los hosts transmisores detienen la transmisión por un período aleatorio, conforme a las reglas de Ethernet 802.3 de CSMA/CD.

Dado que Ethernet no tiene forma de controlar cuál será el nodo que transmitirá en determinado momento, sabemos que cuando más de un nodo intente obtener acceso a la red, se producirán colisiones. La solución de Ethernet para las colisiones no tiene lugar de manera instantánea. Además, los nodos que estén involucrados en la colisión no podrán dar comienzo a la transmisión hasta que se resuelva el problema. Cuanto mayor sea la cantidad de nodos que se agreguen a los medios compartidos, mayor será la posibilidad de que se produzcan colisiones. Por ello, es importante comprender que al establecer el ancho de banda de la red Ethernet en 10 Mb/s, el ancho de banda completo para la transmisión estará disponible sólo una vez que se hayan resuelto las colisiones. El rendimiento neto del puerto (la cantidad promedio de datos eficazmente transmitidos) disminuirá de manera significativa según la cantidad de nodos adicionales que se utilicen en la red. Los hubs no ofrecen mecanismo alguno que sirva para eliminar o reducir estas colisiones y el ancho de banda disponible que cualquier nodo tenga que transmitir se verá reducido en consecuencia. Por lo tanto, la cantidad de nodos que comparta la red Ethernet influirá en el rendimiento o la productividad de dicha red.

Dominios de colisión

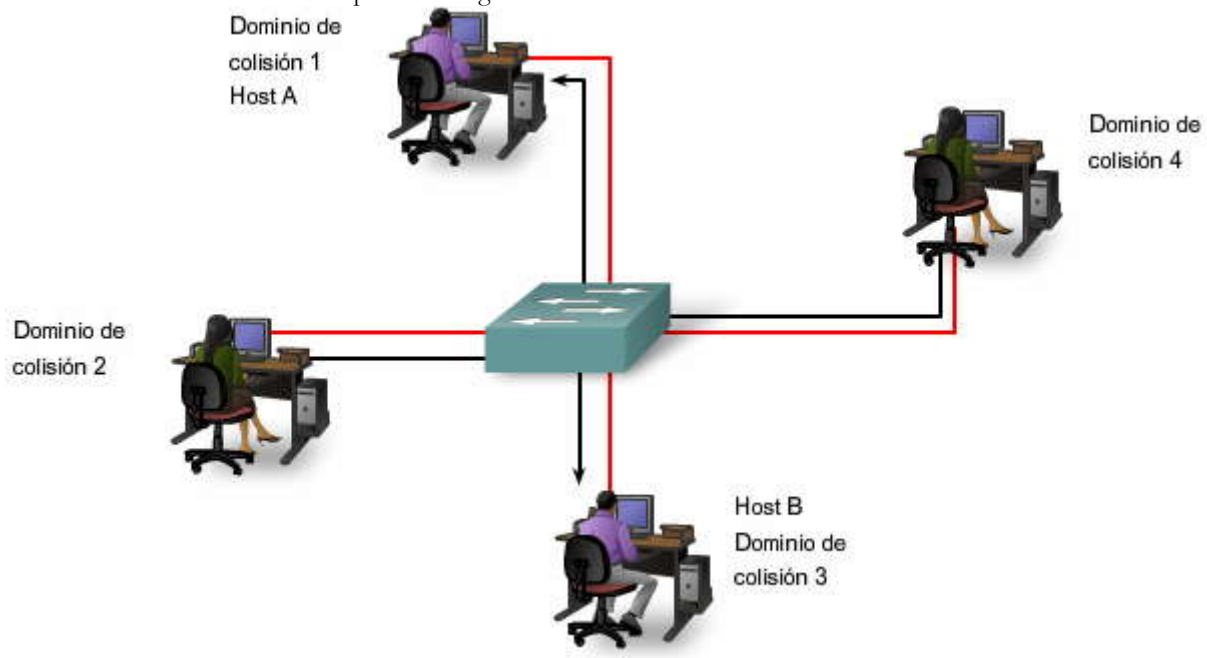
Al expandir una LAN Ethernet para alojar más usuarios con mayores requisitos de ancho de banda, aumenta la posibilidad de que se produzcan colisiones. Para reducir el número de nodos en un determinado segmento de red, se pueden crear segmentos físicos de red individuales, llamados dominios de colisión.

El área de red donde se originan las tramas y se producen las colisiones se denomina dominio de colisiones. Todos los entornos de los medios compartidos, como aquellos creados mediante el uso de hubs, son dominios de colisión. Cuando un

host se conecta a un puerto de switch, el switch crea una conexión dedicada. Esta conexión se considera como un dominio de colisiones individual, dado que el tráfico se mantiene separado de cualquier otro y, por consiguiente, se eliminan las posibilidades de colisión. La figura muestra dominios de colisión exclusivos en un entorno conmutado. Por ejemplo: si un switch de 12 puertos tiene un dispositivo conectado a cada puerto, se crean 12 dominios de colisión.

Como se mencionó anteriormente, un switch crea una tabla de direcciones MAC mediante el registro de direcciones MAC de los hosts que están conectados a cada puerto de switch. Cuando dos hosts conectados desean comunicarse entre sí, el switch utiliza la tabla de conmutación para establecer la conexión entre los puertos. El circuito se mantiene hasta que finaliza la sesión. En la figura, el Host A y el Host B desean comunicarse entre sí. El switch crea la conexión a la que se denomina microsegmento. El microsegmento se comporta como una red de sólo dos hosts, un host que envía y otro que recibe, y se utiliza el máximo ancho de banda disponible.

Los switches reducen las colisiones y permiten una mejor utilización del ancho de banda en los segmentos de red, ya que ofrecen un ancho de banda dedicado para cada segmento de red.



Dominios de broadcast

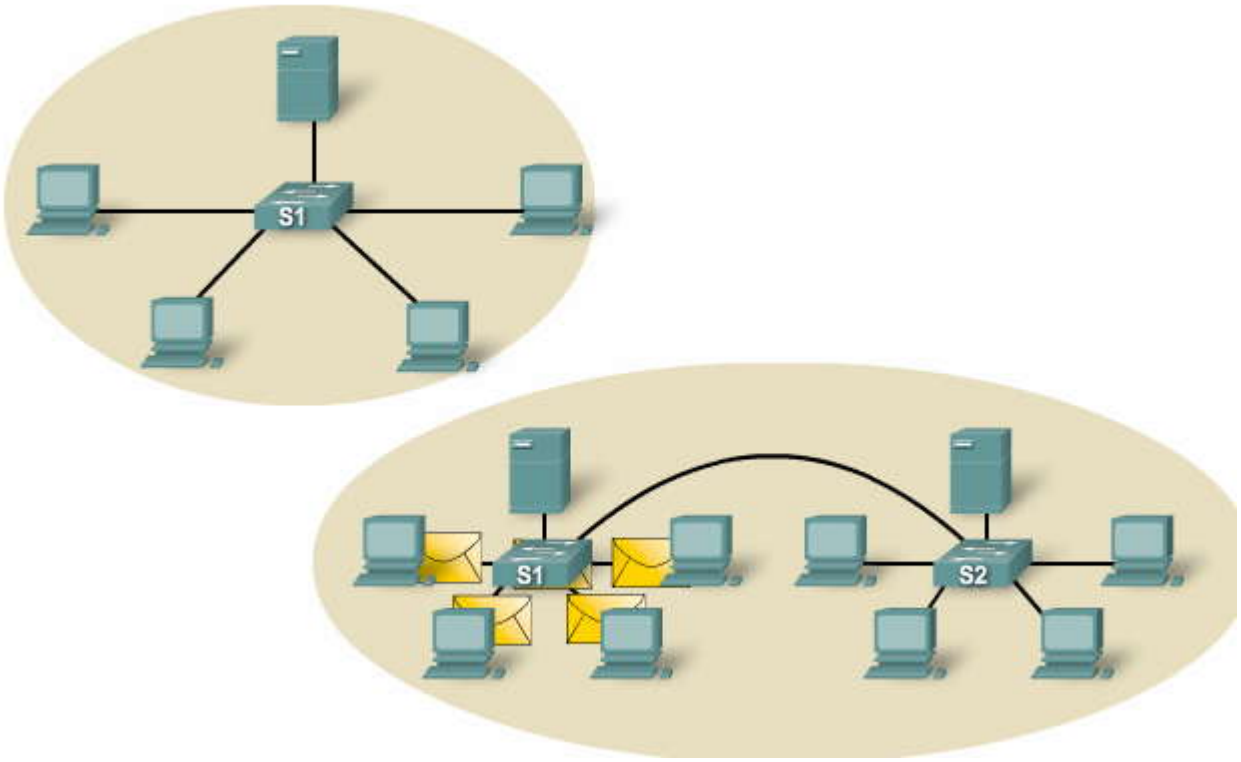
Si bien los switches filtran la mayoría de las tramas según las direcciones MAC, no hacen lo mismo con las tramas de broadcast. Para que otros switches de la LAN obtengan tramas de broadcast, éstas deben ser reenviadas por switches. Una serie de switches interconectados forma un dominio de broadcast simple. Sólo una entidad de Capa 3, como un router o una LAN virtual (VLAN), puede detener un dominio de broadcast de Capa 3. Los routers y las VLAN se utilizan para segmentar los dominios de colisión y de broadcast. El uso de las VLAN para segmentar los dominios de broadcast se analiza en el próximo capítulo.

Cuando un dispositivo desea enviar un broadcast de Capa 2, la dirección MAC destino en la trama se establece en sólo unos. Al configurar el destino en este valor, todos los dispositivos aceptarán y procesarán la trama de broadcast.

El dominio de broadcast de la Capa 2 se conoce como dominio de broadcast MAC. El dominio de broadcast MAC incluye todos los dispositivos de la LAN que reciben broadcasts de tramas a través de un host a todas las demás máquinas en la LAN. Esto se muestra en la primera mitad de la animación.

Cuando un switch recibe una trama de broadcast la reenvía a cada uno de sus puertos excepto al puerto entrante en el que el switch recibió esa trama. Cada dispositivo conectado reconoce la trama de broadcast y la procesa. Esto provoca una disminución en la eficacia de la red dado que el ancho de banda se utiliza para propagar el tráfico de broadcast.

Cuando se conectan dos switches, el dominio de broadcast aumenta. En este ejemplo, se reenvía una trama de broadcast a todos los puertos conectados en el switch S1. El switch S1 está conectado al switch S2. La trama se propaga a todos los dispositivos conectados al switch S2. Esto se muestra en la segunda mitad de la animación.



Latencia de red

La latencia es el tiempo que una trama o paquete tarda en hacer el recorrido desde la estación origen hasta su destino final. Los usuarios de las aplicaciones basadas en redes experimentan la latencia cuando tienen que esperar varios minutos para obtener acceso a la información almacenada en un centro de datos o cuando un sitio Web tarda varios minutos en cargar el explorador. La latencia consiste en por lo menos tres componentes.

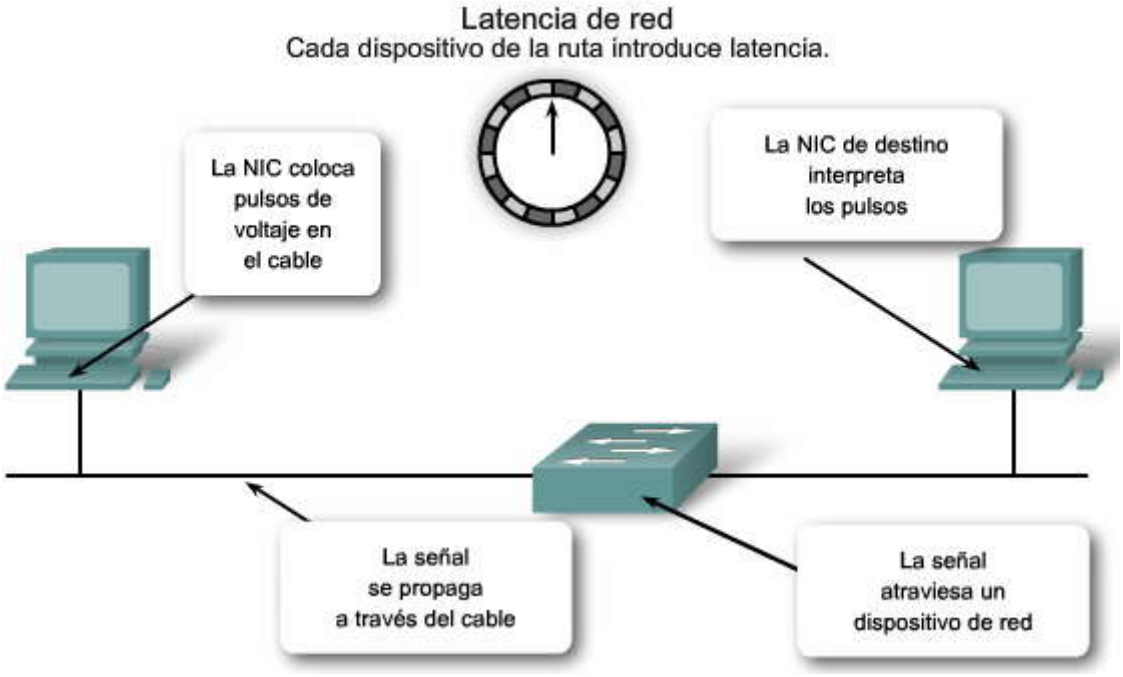
En primer lugar, el tiempo que toma la NIC origen en colocar pulsos de voltaje en el cable y el tiempo que tarda la NIC destino en interpretar estos pulsos. Esto se denomina a veces retraso de la NIC (por lo general, es de 1 microsegundo para una NIC 10BASE-T).

En segundo lugar, el retardo de propagación real, ya que la señal tarda un tiempo en recorrer el cable. Normalmente, éste es de unos 0,556 microsegundos por 100 m para Cat 5 UTP. Si la longitud del cable es mayor y la velocidad nominal de propagación (NVP, Nominal Velocity of Propagation) es menor, el retraso de propagación será mayor.

En tercer lugar, la latencia aumenta según los dispositivos de red que se encuentren en la ruta entre dos dispositivos. Estos pueden ser dispositivos de Capa 1, Capa 2 o Capa 3. Estos tres factores que contribuyen a la latencia pueden distinguirse en la animación a medida que la trama atraviesa la red.

La latencia no depende únicamente de la distancia y de la cantidad de dispositivos. Por ejemplo: si dos computadoras están separadas por tres switches correctamente configurados, es probable que éstas experimenten una latencia menor que la que se produciría si estuvieran separadas por dos routers correctamente configurados. Esto se debe a que los routers ejecutan funciones más complejas y que llevan más tiempo. Por ejemplo: un router debe analizar datos de Capa 3 mientras que los switches sólo analizan los datos de Capa 2. Dado que los datos de la Capa 2 se presentan antes que los de la Capa 3 en la estructura de la trama, los switches pueden procesarla con mayor velocidad. Los switches también admiten alta velocidad de transmisión de voz, video y redes de datos mediante circuitos integrados de aplicaciones específicas (ASIC, Application Specific Integrated Circuits) que proporcionan soporte de hardware para muchas tareas de networking. Otras características de los switches, como por ejemplo búfer de memoria basado en puerto, calidad de servicio (QoS) de nivel de puertos y administración de congestión, también ayudan a reducir la latencia en la red.

La latencia basada en switches puede también deberse a un exceso de demanda en la estructura de éste. Muchos switches de nivel de entrada no cuentan con el rendimiento interno suficiente como para administrar las capacidades del ancho de banda completo en todos los puertos de manera simultánea. El switch debe tener la capacidad de administrar la cantidad máxima de datos que se espera en la red. Dado que la tecnología de los switches es cada vez mejor, la latencia a través de ellos ya no es un problema. La causa predominante de latencia de red en una LAN conmutada está más relacionada con los medios que se transmiten, los protocolos de enrutamiento utilizados y los tipos de aplicaciones que se ejecutan en la red.

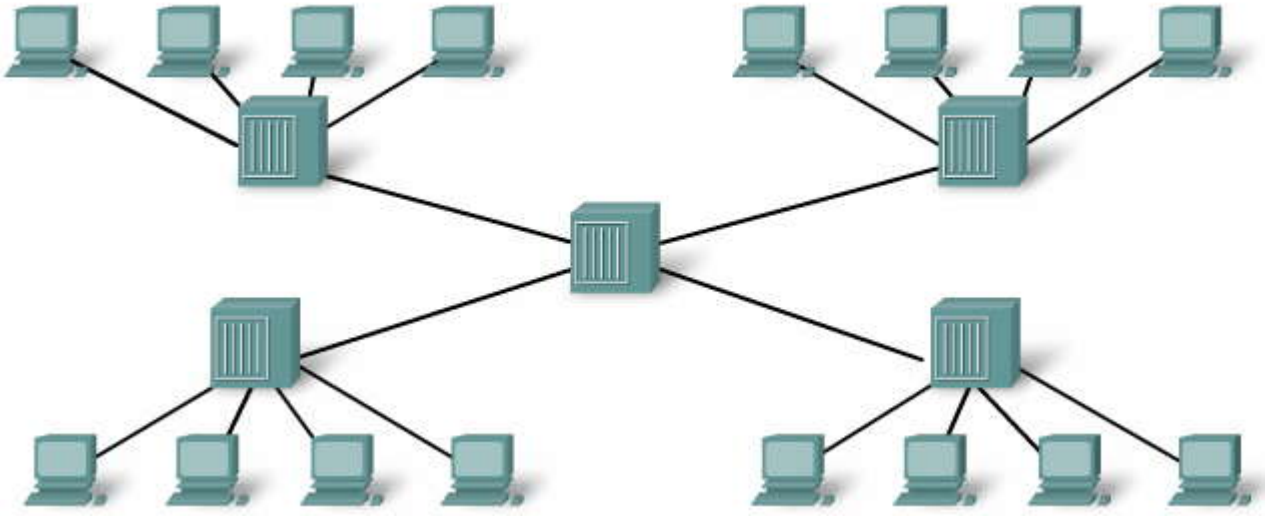


Congestión de red

El primer motivo por el cual segmentar una LAN en partes más pequeñas es el de aislar el tráfico y lograr una mejor utilización del ancho de banda por usuario. Al no segmentarla, la LAN se obstruye rápidamente debido al tráfico y a las colisiones. La figura muestra una red que está sujeta a congestión debido a varios dispositivos de nodos en una red basada en hubs.

A continuación se mencionan las causas más comunes de congestión de red:

- Tecnología de redes y computadoras cada vez más potentes. Hoy en día, las CPU, los buses y los dispositivos periféricos son mucho más rápidos y potentes que aquellos utilizados en las LAN anteriores. Porlo tanto, éstos pueden enviar una mayor cantidad de datos a través de la red y también procesarlos a una mayor velocidad.
- Volumen de tráfico de la red cada vez mayor. En la actualidad el tráfico de la red es más habitual, ya que se necesitan recursos remotos para llevar a cabo tareas básicas. Además, los mensajes de broadcast, como las consultas de resolución de direcciones que envía el ARP, pueden afectar de manera negativa el rendimiento de la red y de las estaciones de trabajo.
- Aplicaciones con alta demanda de ancho de banda. Las aplicaciones de software son cada vez más ricas en cuanto a funcionalidad y requieren un ancho de banda superior. Por ejemplo: las aplicaciones de edición, diseño de ingeniería, video a pedido (VoD), aprendizaje electrónico (e-learning) y streaming video requieren una considerable capacidad y velocidad de procesamiento.



Segmentación LAN

Las LAN se segmentan en varios dominios de broadcast y de colisión más pequeños mediante el uso de routers y switches. Anteriormente se utilizaban los puentes pero no suele verse este tipo de equipos de red en una moderna LAN conmutada. La figura muestra los routers y switches que segmentan una LAN.

En la figura, la red está segmentada en dos dominios de colisión mediante el switch.

Desplace el mouse por el Dominio de colisiones para ver el tamaño de cada uno de ellos.

Sin embargo, en la figura, el dominio de broadcast abarca toda la red.

Desplace el mouse por el Dominio de broadcast para ver el tamaño de éste.

Puentes y switches

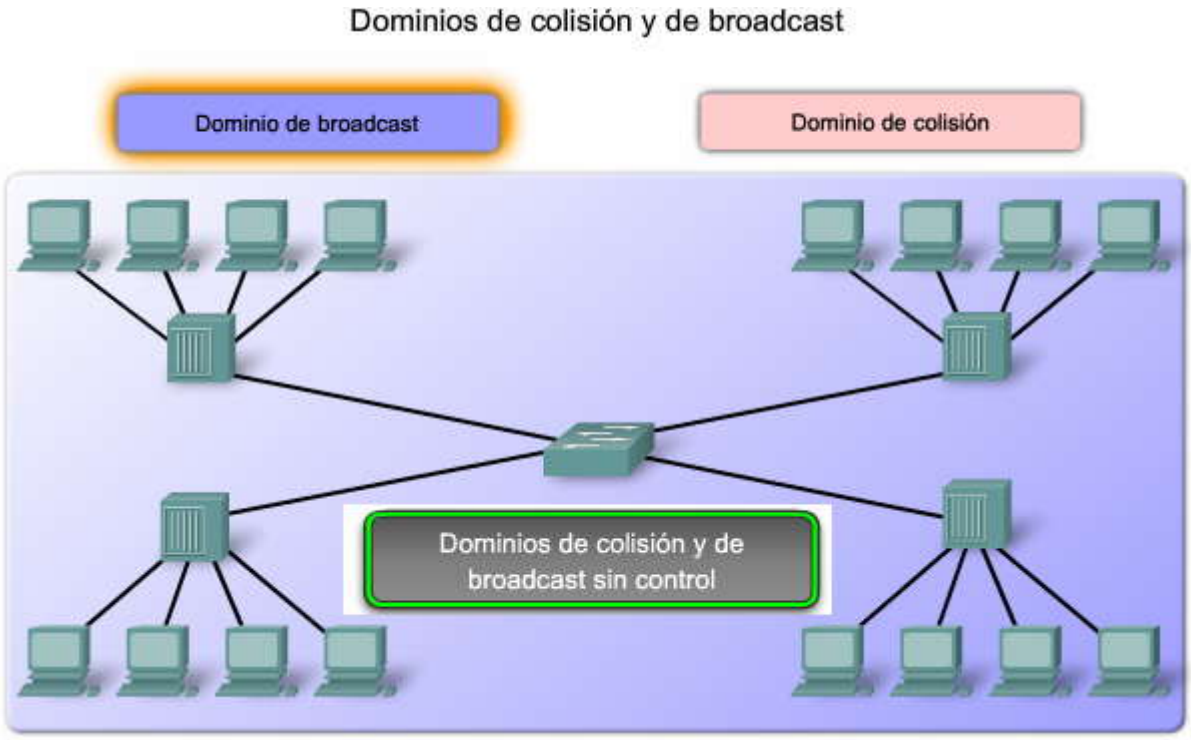
Si bien los puentes y los switches tienen muchos atributos en común, su tecnología presenta varias diferencias. Los puentes se utilizan generalmente para dividir una LAN en un par de segmentos más pequeños. En cambio los switches se utilizan, por lo general, para dividir una gran LAN en varios segmentos más pequeños. Los puentes tienen sólo un par de puertos para la conectividad de la LAN, mientras que los switches cuentan con varios.

Routers

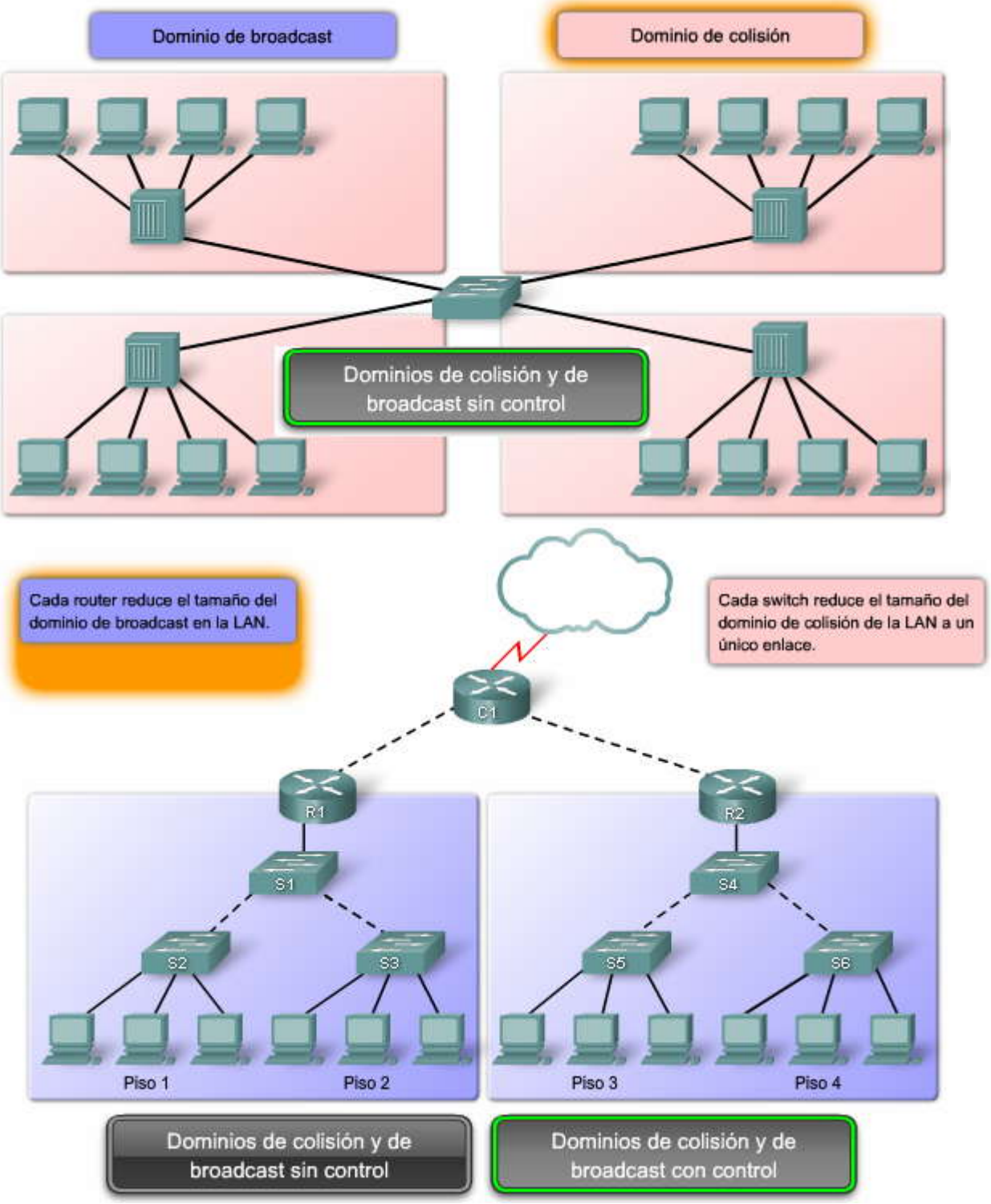
Aunque el switch LAN reduce el tamaño de los dominios de colisión, todos los hosts conectados al switch pertenecen al mismo dominio de broadcast. Los routers pueden utilizarse para crear dominios de broadcast, ya que no reenvían tráfico de broadcast predeterminado. Si se crean pequeños dominios de broadcast adicionales con unrouter, se reducirá el tráfico de broadcast y se proporcionará mayor disponibilidad de ancho de banda para las comunicaciones unicast. Cada interfaz del router se conecta a una red individual que contiene tráfico de broadcast dentro del segmento de la LANen el que se originó.

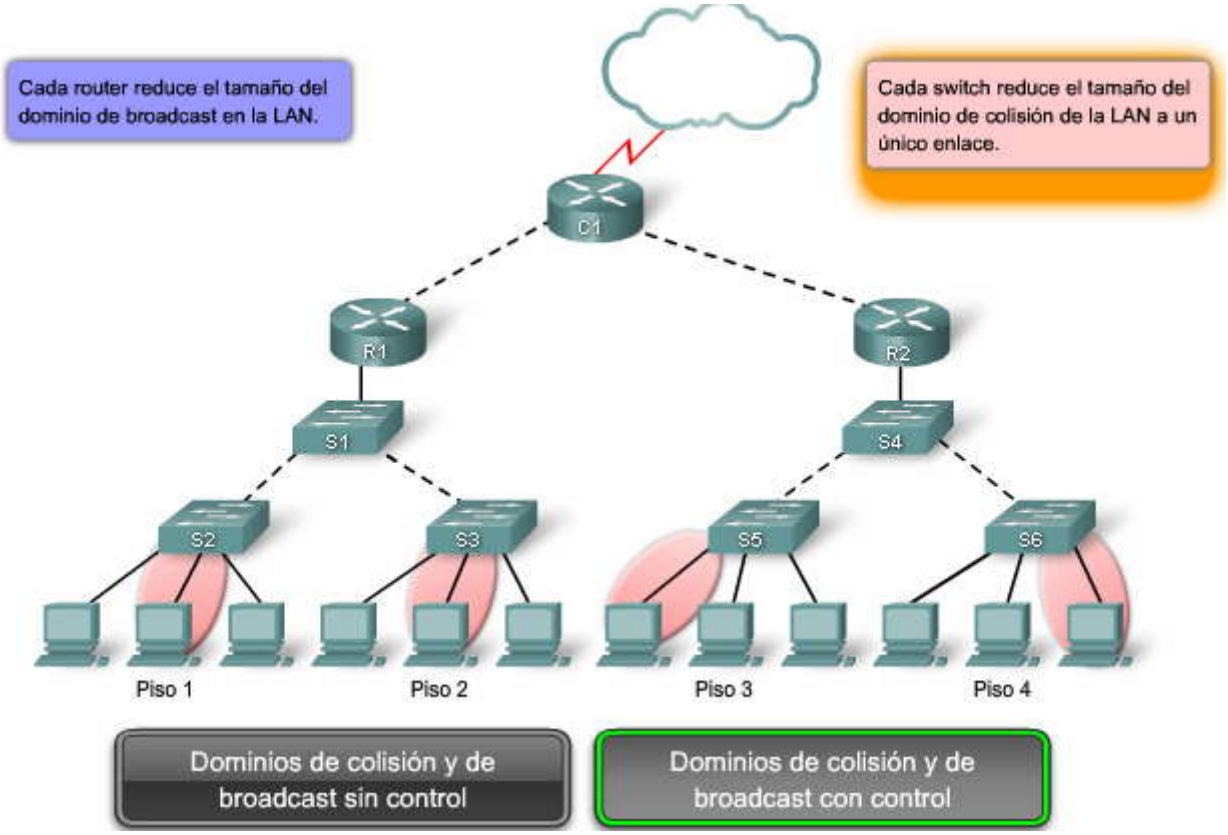
Haga clic en los botones Dominios de colisión y de broadcast con control para ver las consecuencias al introducir routers y más switches en la red.

Desplace el mouse sobre las dos áreas de texto para identificar los distintos dominios de colisión y de broadcast.



Dominios broadcast





2.1.3 CONSIDERACIONES DEL DISEÑO DE LA LAN.-

Control de la latencia de la red

Al diseñar una red para reducir la latencia, se necesita tener en cuenta la latencia originada por cada dispositivo de la red. Los switches pueden provocar latencia cuando se saturan en una red ocupada. Por ejemplo: si un switch central tiene que brindar soporte a 48 puertos, siendo cada uno capaz de funcionar a 1000 Mb/s full duplex, el switch tendría que admitir aproximadamente 96 Gb/s de rendimiento interno para mantener la velocidad plena del cable en todos los puertos al mismo tiempo. En este ejemplo, los requisitos de rendimiento mencionados son típicos de los switches de nivel central y no de los switches de nivel de acceso.

El empleo de dispositivos de capas superiores también puede aumentar la latencia en la red. Cuando un dispositivo de Capa 3, como un router, debe examinar la información de direccionamiento que contiene la trama, debe realizar una lectura más profunda de la trama que un dispositivo de Capa 2, lo cual se traduce en mayor cantidad de tiempo de procesamiento. Al limitar el uso de dispositivos de capas superiores, se reducirá el nivel de latencia de la red. No obstante, la correcta utilización de los dispositivos de Capa 3 ayuda a evitar la contención del tráfico de broadcast en un dominio amplio de broadcast o el alto índice de colisiones en un dominio de colisiones de gran tamaño.

Eliminación de los cuellos de botellas

Los cuellos de botella son lugares donde la alta congestión de la red provoca un bajo rendimiento.

Haga clic en el botón Eliminación de los cuellos de botella de la red que se encuentra en la figura.

En esta figura, que muestra seis computadoras conectadas a un switch, un único servidor se encuentra conectado también al mismo switch. Todas las estaciones de trabajo y el servidor están conectados mediante una tarjeta NIC de 1000 Mb/s. ¿Qué sucede cuando las seis computadoras intentan tener acceso al servidor al mismo tiempo? ¿Cada una de las estaciones de trabajo obtiene un acceso dedicado al servidor de 1000 Mb/s? No, todas las computadoras tienen que compartir la conexión de 1000 Mb/s que el servidor tiene con el switch. De manera acumulativa, las computadoras cuentan con una capacidad de 6000 Mb/s con el switch. Si cada conexión se utilizara a plena capacidad, cada computadora podría emplear sólo 167 Mb/s, un sexto del ancho de banda de 1000 Mb/s. Para reducir el cuello de botella en el servidor, es posible instalar más tarjetas de red, y de este modo incrementar el total de ancho de banda que el servidor es capaz de recibir. La figura muestra cinco tarjetas NIC en el servidor y un ancho de banda aproximadamente cinco veces mayor. La misma lógica se aplica a las tipologías de redes. Cuando los switches de varios nodos están interconectados por una única conexión de 1000 Mb/s, se crea un cuello de botella en esa única interconexión.

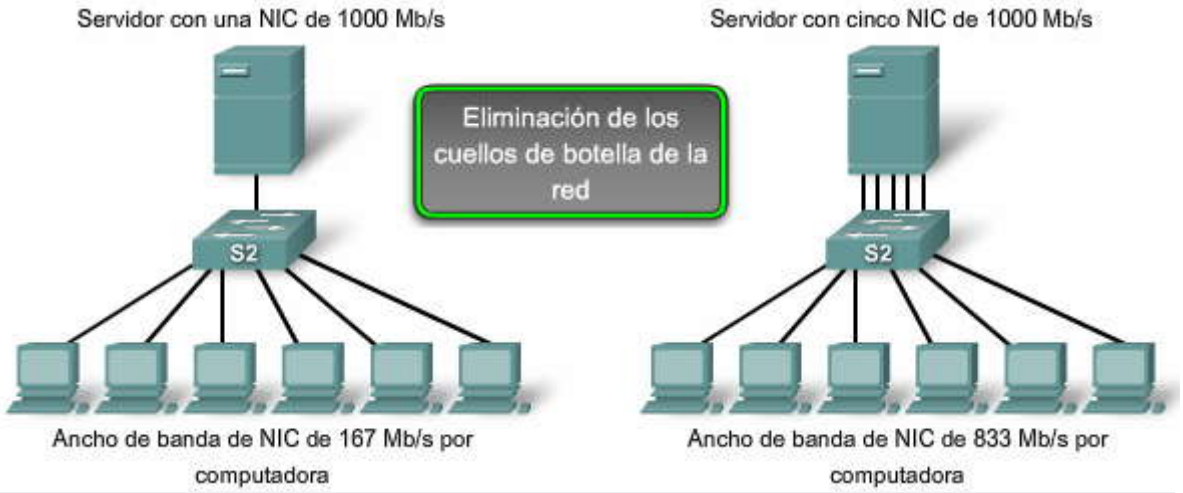
Si se utilizan enlaces de mayor capacidad (por ejemplo: ampliar una conexión de 100 Mb/s hasta 1000 Mb/s) y se emplean varios enlaces promoviendo una tecnología de unificación de enlaces (por ejemplo, combinar dos enlaces como si fueran uno para duplicar la capacidad de la conexión) pueden reducirse los cuellos de botella creados por los enlaces de switches interconectados y de routers. Si bien este curso no abarca el modo de configurar la unificación de enlaces, es importante tener en cuenta las capacidades de un determinado dispositivo al evaluar las necesidades de una red. ¿Con cuántos puertos cuenta y qué capacidad de velocidad tiene el dispositivo? ¿Cuál es el rendimiento interno del dispositivo? ¿Es capaz de administrar las cargas de tráfico que se esperan considerando su ubicación en la red?

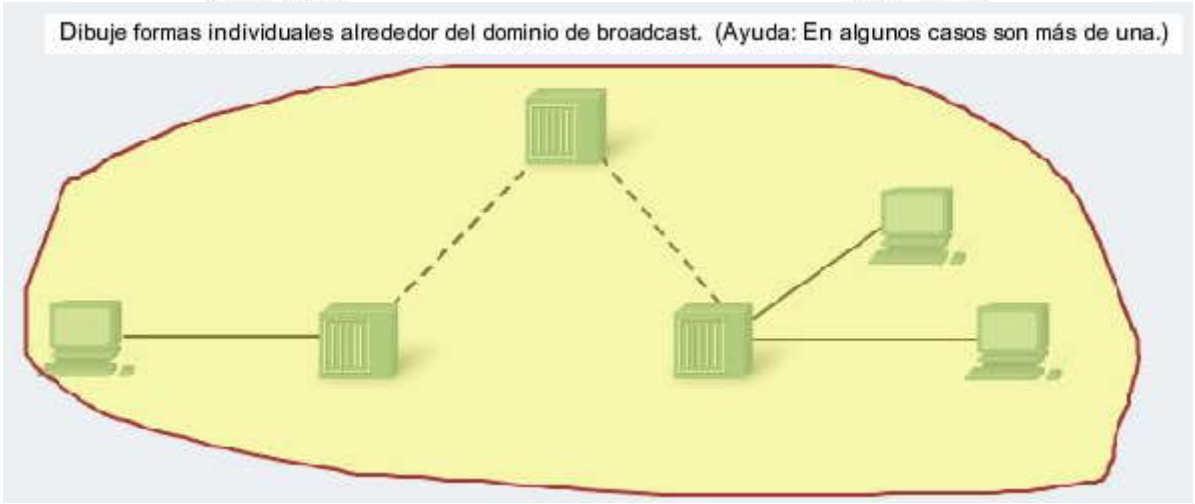
Control de la latencia de la red

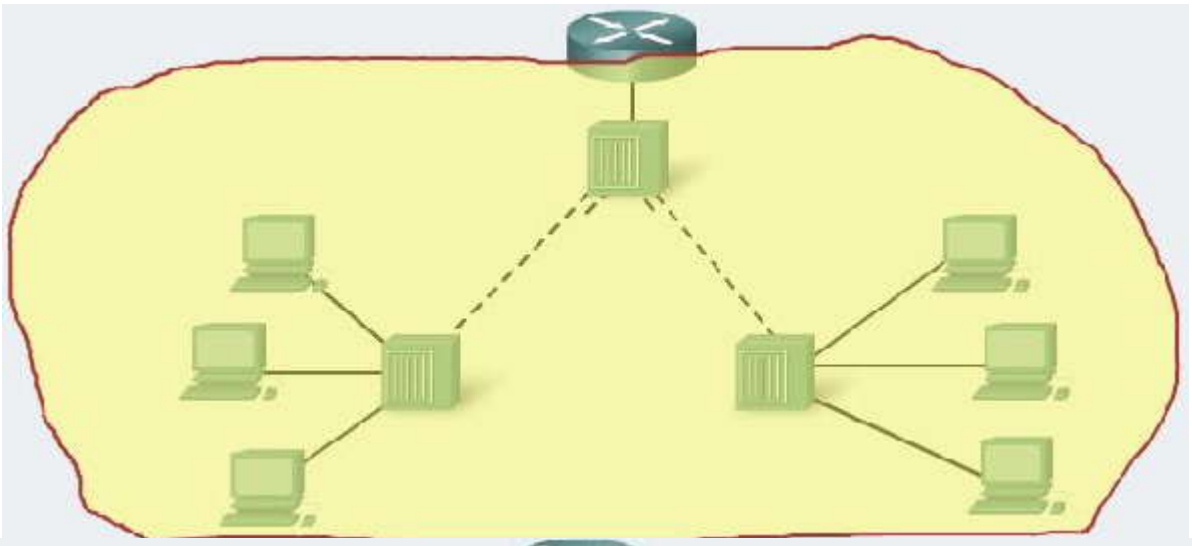
- **Considere la latencia producida por cada dispositivo de la red.**
  - Un switch de nivel de núcleo que mantiene 48 puertos, ejecutándose a 1000 Mb/s full duplex, requiere un rendimiento interno de 96 Gb/s para mantener la velocidad de cable total en todos los puertos al mismo tiempo.

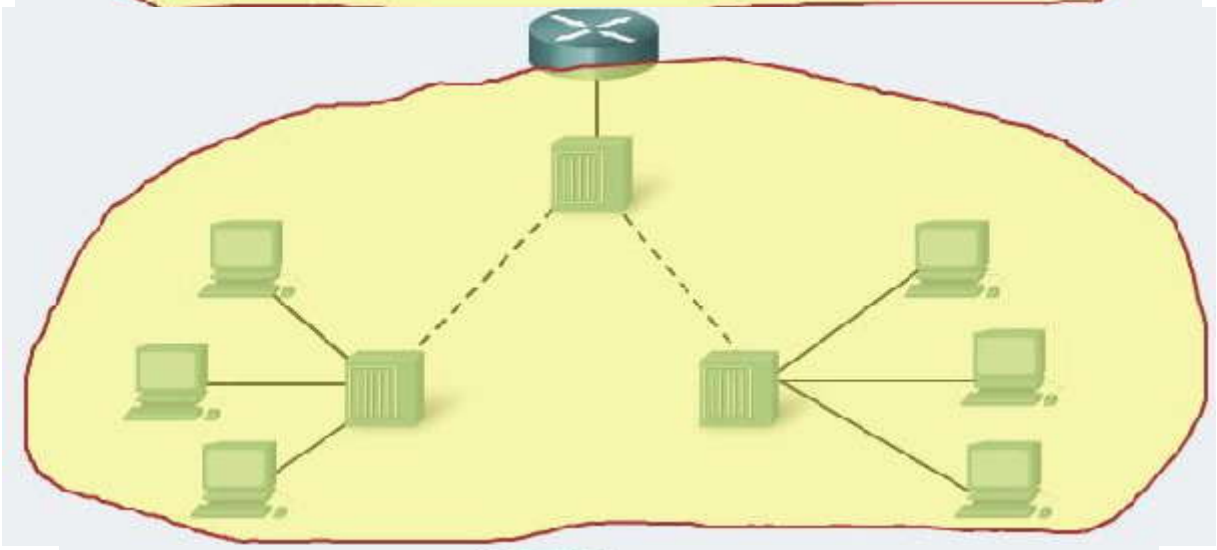
- **Los dispositivos de las capas OSI más altas también pueden aumentar la latencia de la red.**
  - El router debe quitar los campos de la Capa 2 de la trama para poder interpretar la información de direccionamiento de la Capa 3. El tiempo de procesamiento adicional provoca latencia.
  - Se balancea el uso de dispositivos de capas superiores para deducir la latencia de la red con la necesidad de evitar la contención del tráfico de broadcast o las altas tasas de colisiones.

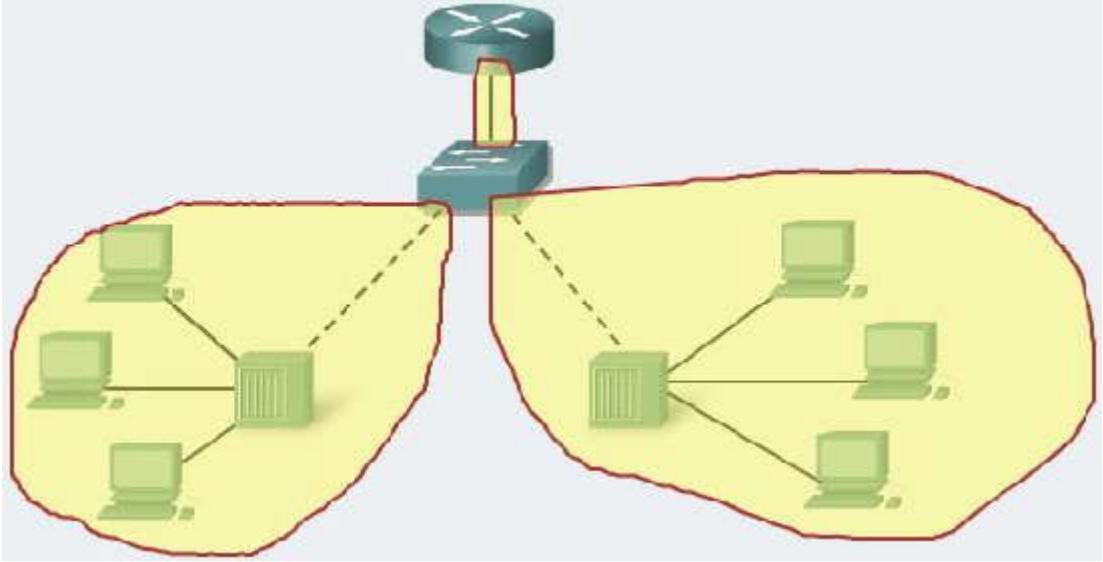
Control de la latencia de la red

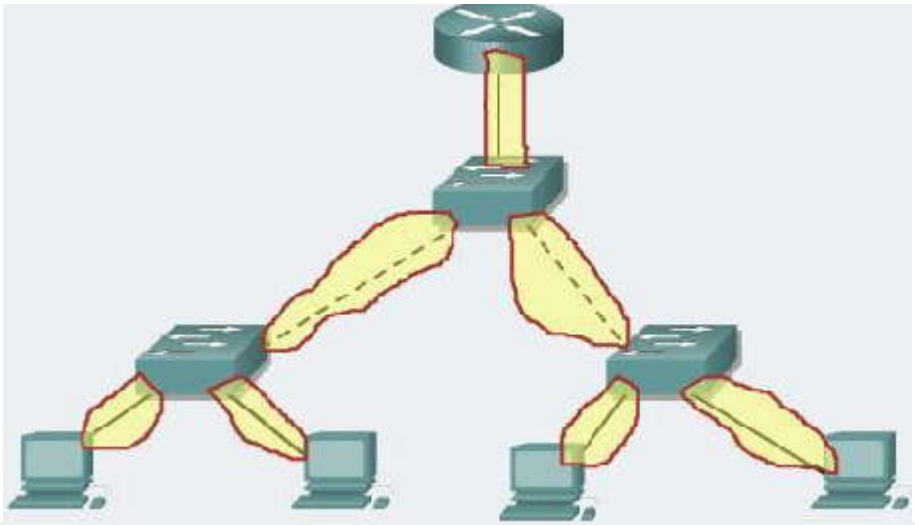


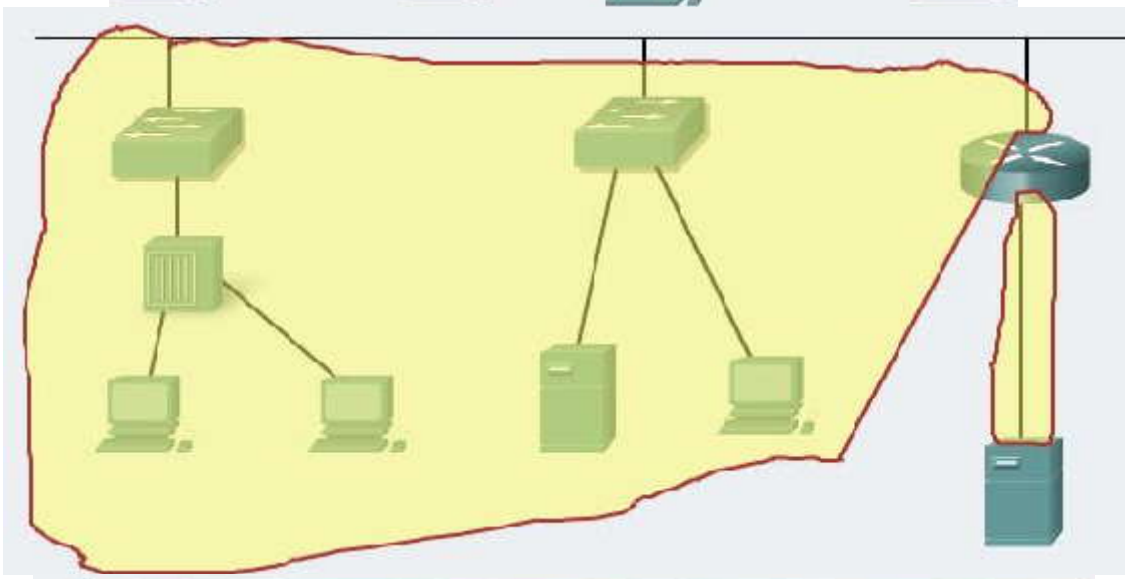


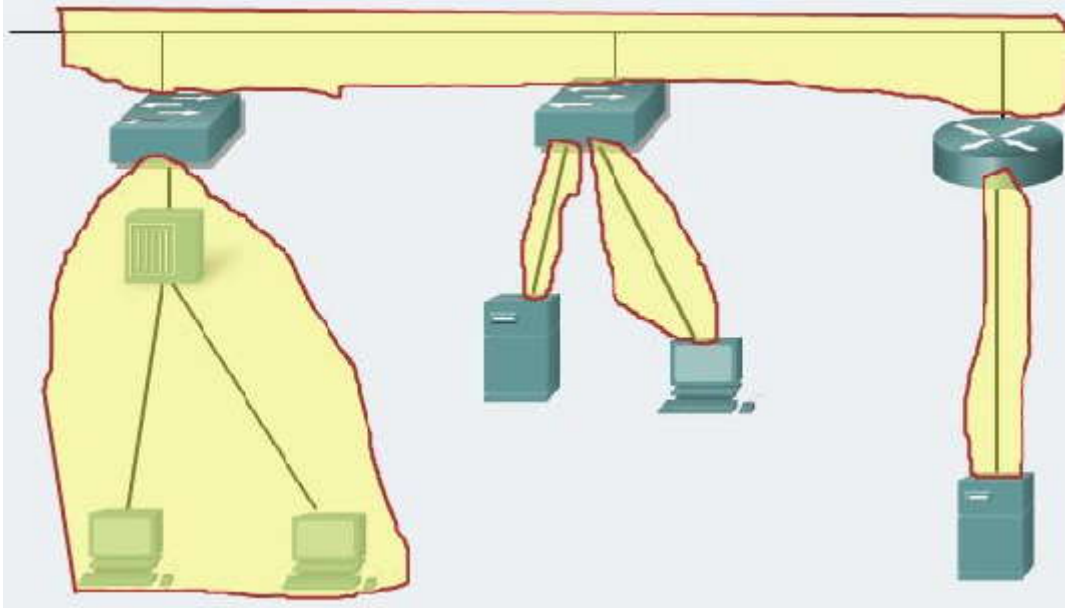


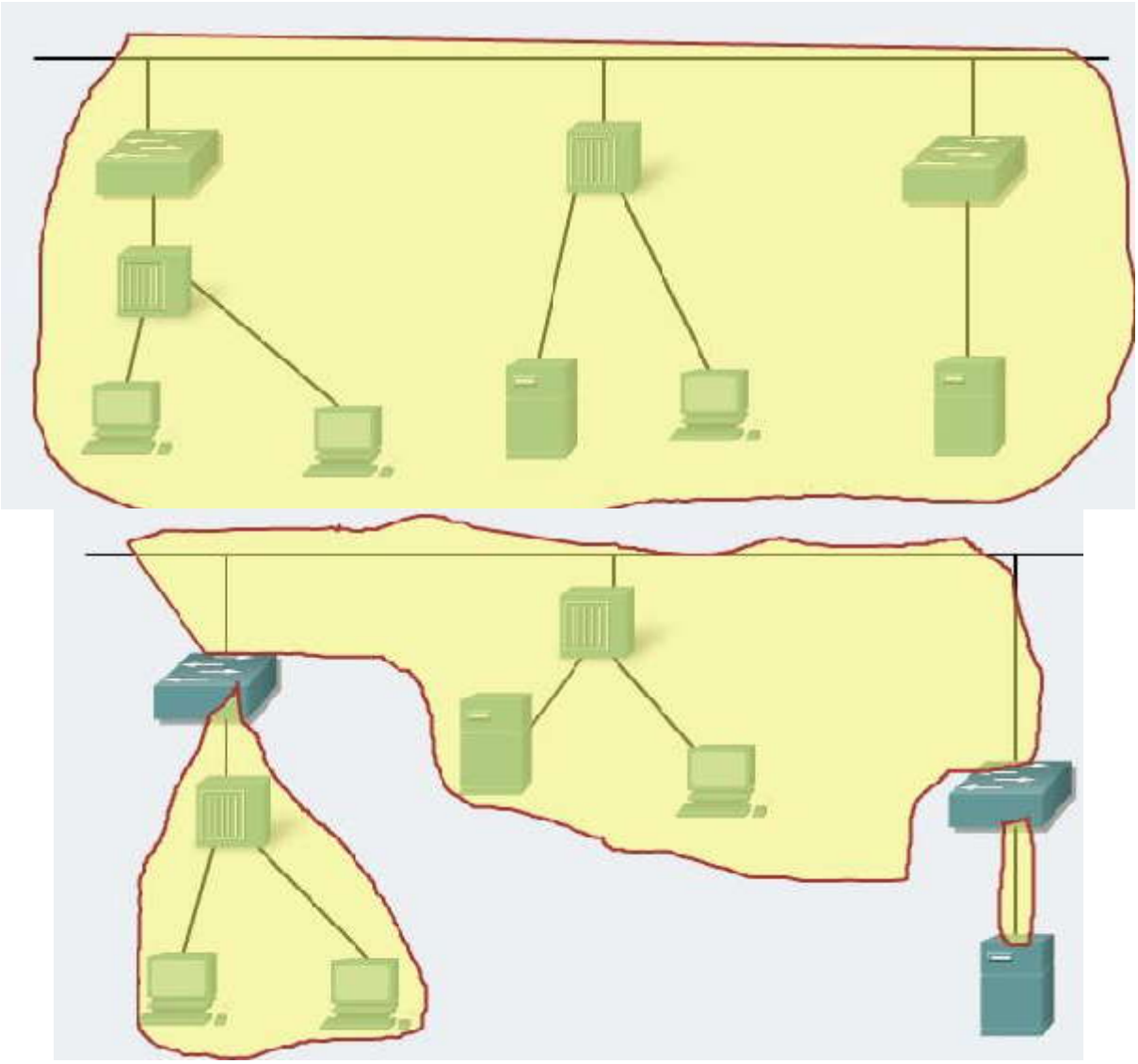












2.2 REENVÍO DE TRAMAS MEDIANTE UN SWITCH

2.2.1 METODOS DE REEVÍO DEL SWITCH.-

Métodos de reenvío de paquetes del switch

En este tema, se describirá cómo los switches reenvían tramas Ethernet en una red. Los switches pueden funcionar de distintos modos y éstos pueden tener tanto efectos positivos como negativos.

Anteriormente, los switches solían utilizar uno de los siguientes métodos de reenvío para conmutar datos entre los puertos de la red: conmutación por método de corte o almacenamiento y envío. El botón Métodos de reenvío del switch muestra estos dos métodos. Sin embargo, almacenamiento y envío es el único método de reenvío que se utiliza en los modelos actuales de los switches Cisco Catalyst.

Conmutación de almacenamiento y envío

En este tipo de conmutación, cuando el switch recibe la trama, la almacena en los buffers de datos hasta recibir la trama en su totalidad. Durante el proceso de almacenamiento, el switch analiza la trama para buscar información acerca de su destino. En este proceso, el switch también lleva a cabo una verificación de errores utilizando la porción del tráiler de comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check) de la trama de Ethernet.

La CRC utiliza una fórmula matemática, basada en la cantidad de bits (1) de la trama, para determinar si ésta tiene algún error. Después de confirmar la integridad de la trama, ésta se envía desde el puerto correspondiente hasta su destino. Cuando se detecta un error en la trama, el switch la descarta. El proceso de descarte de las tramas con errores reduce la cantidad de ancho de banda consumido por datos dañados. La conmutación por almacenamiento y envío se requiere para el análisis de calidad de servicio (QoS) en las redes convergentes, en donde se necesita una clasificación de la trama para decidir el orden de prioridad del tráfico. Por ejemplo: los flujos de datos de voz sobre IP deben tener prioridad sobre el tráfico de exploración Web.

Haga clic en el botón Conmutación por almacenamiento y envío para reproducir la animación y obtener una demostración del proceso de almacenamiento y envío.

Conmutación por método de corte

En este tipo de conmutación, el switch actúa sobre los datos apenas los recibe, incluso si la transmisión aún no se ha completado. El switch recopila en el búfer sólo la información suficiente de la trama como para leer la dirección MAC de destino y así determinar a qué puerto debe reenviar los datos. La dirección MAC de destino se encuentra en los primeros 6 bytes de la trama después del preámbulo. El switch busca la dirección MAC de destino en su tabla de conmutación, determina el puerto de la interfaz de salida y reenvía la trama a su destino mediante el puerto de switch designado. El switch no lleva a cabo ninguna verificación de errores en la trama. Dado que el switch no tiene que esperar que la trama se almacene de manera completa en el búfer y que no realiza ninguna verificación de errores, la conmutación por método de corte es más rápida que la de almacenamiento y envío. No obstante, al no llevar a cabo ninguna verificación de errores, el switch reenvía tramas dañadas a través de la red. Las tramas dañadas consumen ancho de banda mientras se reenvían. Al final, la NIC de destino descarta las tramas dañadas.

Haga clic en el botón Conmutación por método de corte para reproducir la animación y obtener una demostracióndel proceso de conmutación por método de corte.

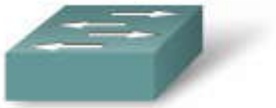
A continuación, se presentan dos variantes de la conmutación por método de corte:

- Conmutación por envío rápido: La conmutación por envío rápido ofrece el más bajo nivel de latencia. La conmutación por envío rápido reenvía el paquete inmediatamente después de leer la dirección de destino. Como la conmutación por envío rápido comienza a reenviar el paquete antes de haberlo recibido en forma completa, es probable que a veces los paquetes se entreguen con errores. Esto ocurre con poca frecuencia y el adaptador de red de destino descarta los paquetes defectuosos en el momento de su recepción. En el modo de envío rápido, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido. La conmutación por envío rápido es el típico método de corte.
- Conmutación Libre de fragmentos: En la conmutación libre de fragmentos, el switch almacena los primeros 64 bytes de la trama antes de reenviarla. Este tipo de conmutación puede ser vista como un acuerdo entre la conmutación por almacenamiento y envío y la conmutación por método de corte. El motivo por el cual la conmutación libre de fragmentos almacena sólo los primeros 64 bytes de la trama es que la mayoría de los errores y las colisiones de la red se producen en esos primeros 64 bytes. El modo libre de fragmentos intenta mejorar la conmutación por método de corte llevando a cabo una pequeña verificación de errores en los primeros 64 bytes de la trama a fin de asegurar que no se han producido colisiones antes de reenviar la trama. La conmutación libre de fragmentos supone un equilibrio entre el alto nivel de latencia y la gran integridad que ofrece la conmutación por almacenamiento y envío, y el bajo nivel de latencia y la reducida integridad que brinda la conmutación por método de corte.

Algunos switches se configuran para realizar una conmutación por método de corte por puerto hasta llegar a un umbral de error definido por el usuario y, luego, cambian la conmutación al modo de almacenamiento y envío. Si elíndice de error está por debajo del umbral, el puerto vuelve automáticamente a la conmutación por método de corte.

Métodos de reenvío de paquetes del switch

Almacenamiento y envío



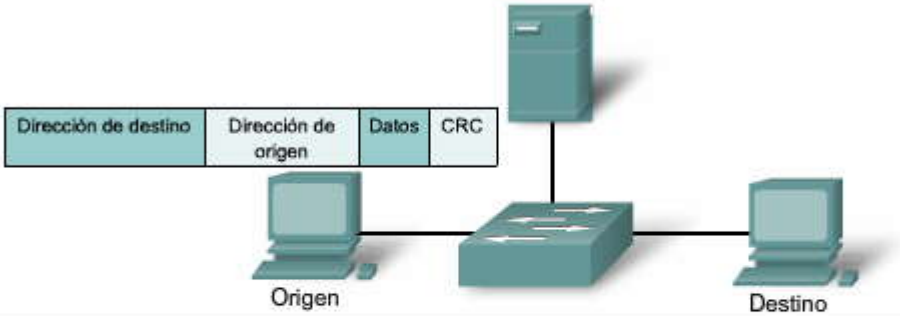
Método de corte

Un switch de almacenamiento y envío recibe toda la trama, calcula la CRC y verifica la longitud de la trama. Si la CRC y la longitud de la trama son válidas, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

El switch que utiliza el método de corte envía la trama antes de recibirla en su totalidad. Como mínimo, la dirección de destino de la trama debe leerse antes de que la trama pueda enviarse.

Métodos de reenvío del switch

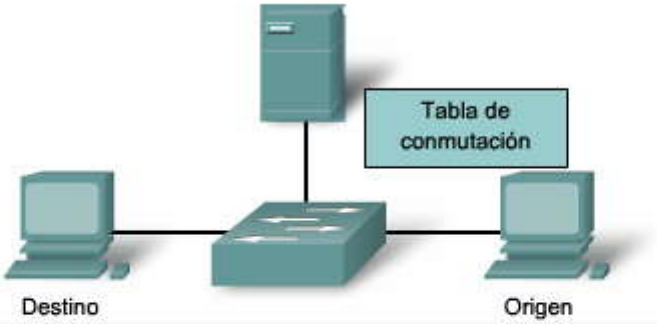
Métodos de reenvío de paquetes del switch



Un switch de almacenamiento y envío recibe toda la trama, calcula la CRC y verifica la longitud de la trama. Si la CRC y la longitud de la trama son válidas, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Conmutación por almacenamiento y envío

Métodos de reenvío de paquetes del switch



El switch que utiliza el método de corte envía la trama antes de recibirla en su totalidad. Como mínimo, la dirección de destino de la trama debe leerse antes de que la trama pueda enviarse.

Conmutación por método de corte

2.2.2 CONMUTACIÓN SIMÉTRICA Y ASIMÉTRICA.-

Conmutación simétrica y asimétrica

En este tema, se estudiarán las diferencias entre la conmutación simétrica y asimétrica en una red. La conmutación LAN se puede clasificar como simétrica o asimétrica según la forma en que el ancho de banda se asigna a los puertos de conmutación.

La conmutación simétrica proporciona conexiones conmutadas entre puertos con el mismo ancho de banda; por ejemplo, todos los puertos de 100 Mb/s o todos los puertos de 1000 Mb/s. Un switch LAN asimétrica proporciona conexiones conmutadas entre puertos con distinto ancho de banda; por ejemplo, una combinación de puertos de 10 Mb/s, 100 Mb/s y 1000 Mb/s. La figura muestra las diferencias entre la conmutación simétrica y la asimétrica.

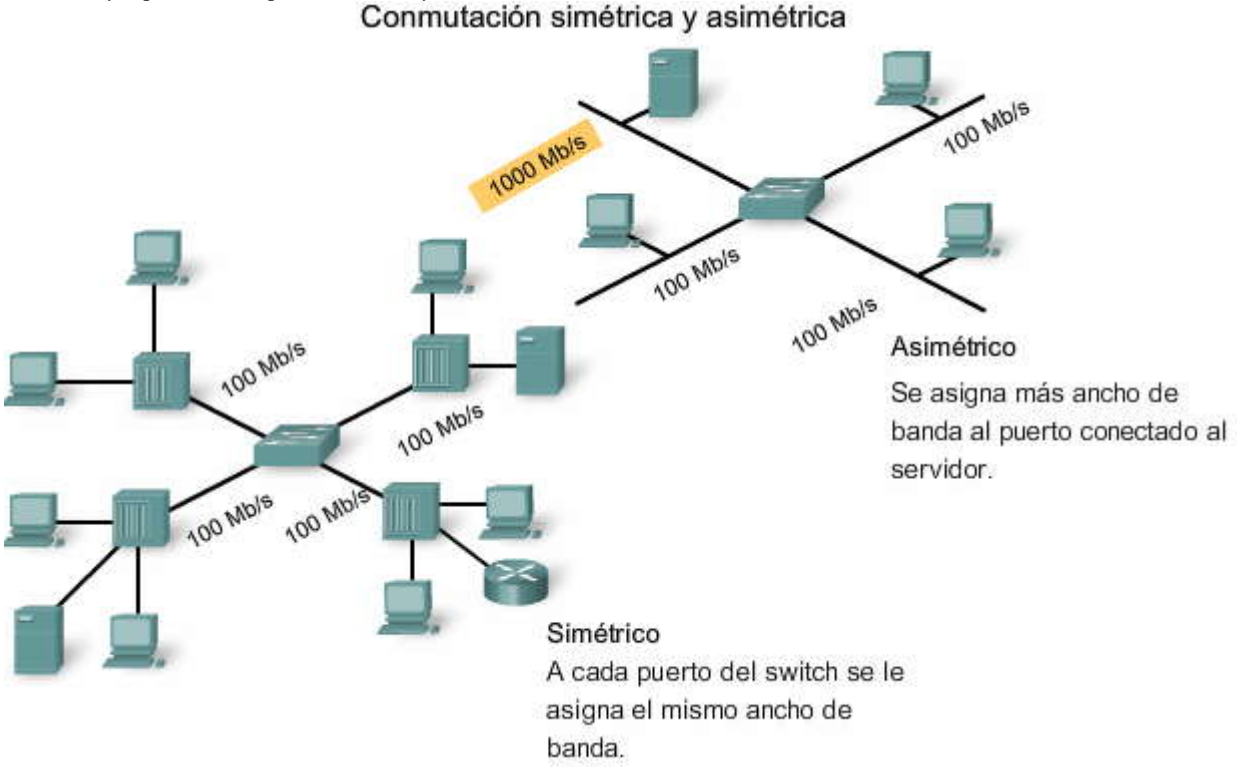
Asimétrica

La conmutación asimétrica permite un mayor ancho de banda dedicado al puerto de conmutación del servidor para evitar que se produzca un cuello de botella. Esto brinda una mejor calidad en el flujo de tráfico, donde varios clientes se comunican con un servidor al mismo tiempo. Se requieren buffers de memoria en un switch asimétrico. Para que el switch coincida con las distintas velocidades de datos en los distintos puertos, se almacenan tramas enteras en los buffers de memoria y se envían al puerto una después de la otra según se requiera.

Simétrico

En un switch simétrico, todos los puertos cuentan con el mismo ancho de banda. La conmutación simétrica se ve optimizada por una carga de tráfico distribuida de manera uniforme, como en un entorno de escritorio entre pares.

El administrador de la red debe evaluar la cantidad de ancho de banda que se necesita para las conexiones entre dispositivos a fin de que pueda adaptarse al flujo de datos de las aplicaciones basadas en redes. La mayoría de los switches actuales son asimétricos, ya que son los que ofrecen mayor flexibilidad.



2.2.3 BÚFER DE MEMORIA.-

Búfer de memoria basado en puerto y búfer de memoria compartida

Como se describió en el tema anterior, el switch analiza parte del paquete, o su totalidad, antes de reenviarlo al host de destino mediante el método de reenvío. El switch almacena el paquete en un búfer de memoria durante un breve período. En este tema, se estudiará cómo se utilizan dos tipos de buffers de memoria durante el reenvío.

Un switch Ethernet puede usar una técnica de buffers para almacenar tramas antes de enviarlas. El almacenamiento en buffers también puede utilizarse cuando el puerto destino está ocupado debido a una congestión. El switch almacena la trama hasta el momento en que pueda transmitirse. El empleo de memoria para almacenar datos se denomina

almacenamiento en buffers de memoria. El búfer de memoria está integrado al hardware del switch y, además de aumentar la cantidad de memoria disponible, no puede configurarse.

Existen dos tipos de almacenamiento en buffers de memoria: memoria compartida y memoria basada en puerto.

Búfer de memoria basada en puerto

En el búfer de memoria basado en puerto, las tramas se almacenan en colas conectadas a puertos de entrada específicos. Una trama se transmite al puerto de salida una vez que todas las tramas que están delante de ella en la cola se hayan transmitido con éxito. Es posible que una sola trama retarde la transmisión de todas las tramas almacenadas en la memoria debido al tráfico del puerto de destino. Este retardo se produce aunque las demás tramas se puedan transmitir a puertos destino abiertos.

Búfer de memoria compartida

El búfer de memoria compartida deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch. La cantidad de memoria de búfer que requiere un puerto se asigna de forma dinámica. Las tramas en el búfer se vinculan de forma dinámica al puerto de destino. Esto permite la recepción del paquete por un puerto y la transmisión por otro puerto, sin tener que colocarlo en otra cola.

El switch conserva un mapa de enlaces de trama a puerto que indica por dónde un paquete debe transmitirse. El enlace del mapa se elimina una vez que la trama se ha transmitido con éxito. La cantidad de tramas almacenadas en el búfer se encuentra limitada por el tamaño del búfer de memoria en su totalidad y no se limita a un solo búfer de puerto. Esto permite la transmisión de tramas más amplias y que se descarte una menor cantidad de ellas. Esto es importante para la conmutación asimétrica, donde las tramas se intercambian entre puertos de distintas velocidades.

Búfer de memoria basado en puerto y búfer de memoria compartida

Memoria basada en puerto	En el búfer de memoria basado en puerto, las tramas se almacenan en colas conectadas a puertos de entrada específicos.
Memoria compartida	El búfer de memoria compartida deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch.

2.2.4 CONMUTACION DE CAPA 2 Y CAPA 3.-

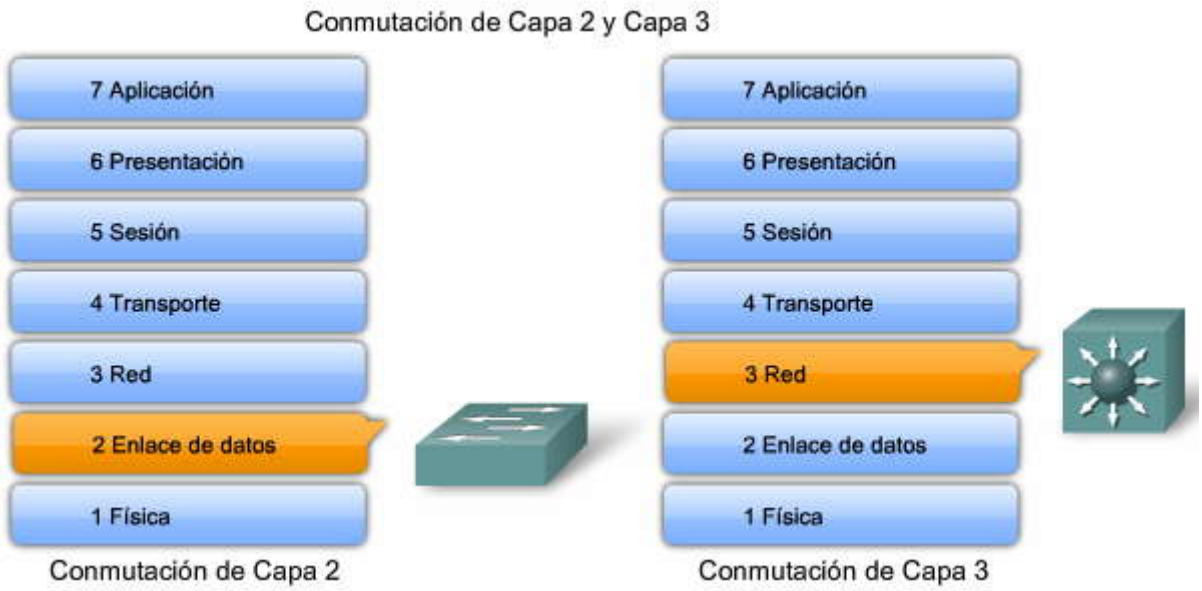
Conmutación de Capa 2 y Capa 3

En este tema, se revisará el concepto de conmutación de Capa 2 y se introducirá la conmutación de Capa 3.

Un switch LAN de Capa 2 lleva a cabo los procesos de conmutación y filtrado basándose solamente en la dirección MAC de la Capa de enlace de datos (Capa 2) del modelo OSI. El switch de Capa 2 es completamente transparente para los protocolos de la red y las aplicaciones del usuario. Recuerde que un switch de Capa 2 crea una tabla de direcciones MAC que utiliza para determinar los envíos.

Un switch de Capa 3, como el Catalyst 3560, funciona de modo similar a un switch de Capa 2, como el Catalyst 2960, pero en lugar de utilizar sólo la información de las direcciones MAC para determinar los envíos, el switch de Capa 3 puede también emplear la información de la dirección IP. En lugar de aprender qué direcciones MAC están vinculadas con cada uno de sus puertos, el switch de Capa 3 puede también conocer qué direcciones IP están relacionadas con sus interfaces. Esto permite que el switch de Capa 3 pueda dirigir el tráfico a través de la red en base a la información de las direcciones IP.

Los switches de Capa 3 son también capaces de llevar a cabo funciones de enrutamiento de Capa 3, con lo cual se reduce la necesidad de colocar routers dedicados en una LAN. Dado que los switches de Capa 3 cuentan con un hardware de conmutación especializado, normalmente, pueden enviar datos con la misma rapidez con la que pueden conmutar.



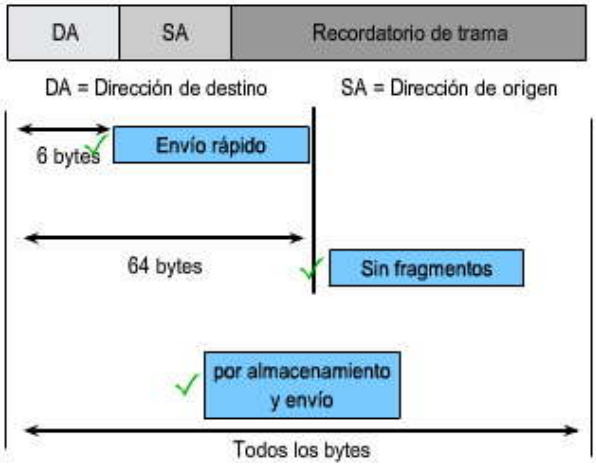
Comparación entre el switch y el router de Capa 3

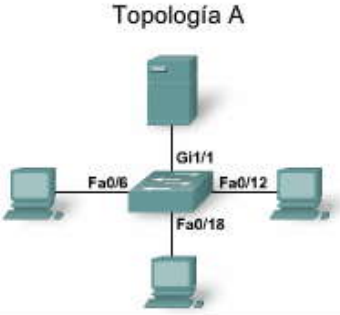
En el tema anterior, se explicó que los switches de Capa 3 examinan la información de Capa 3 de un paquete Ethernet para determinar los envíos. Los switches de Capa 3 pueden enviar paquetes entre distintos segmentos de una LAN de modo similar que los routers dedicados. Sin embargo, los switches de Capa 3 no reemplazan completamente la necesidad de utilizar routers en una red.

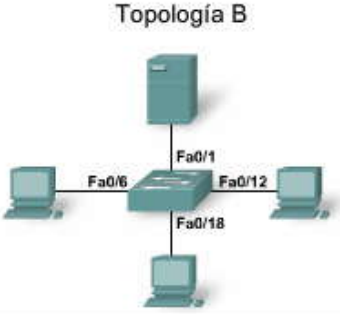
Los routers proporcionan servicios adicionales de Capa 3 que los switches de Capa 3 no pueden realizar. Los routers también pueden llevar a cabo tareas de reenvío de paquetes que no realizan los switches de Capa 3, como establecer conexiones de acceso remoto con dispositivos y redes remotas. Los routers dedicados son más flexibles en cuanto a la admisión de tarjetas de interfaz WAN (WIC, WAN Interface Cards). Por ello, son la opción preferida, y a veces incluso la única, para conectar a una WAN. Los switches de Capa 3 ofrecen funciones básicas de enrutamiento en una LAN y reducen la necesidad de utilizar routers dedicados.

Comparación entre el router y el switch de Capa 3

Característica	Switch de Capa 3	Router
Enrutamiento de Capa 3	Con soporte	Con soporte
Administración del tráfico	Con soporte	Con soporte
Soporte de WIC		Con soporte
Protocolos de enrutamiento avanzados		Con soporte
Enrutamiento por velocidad de cable	Con soporte	







_____ es un ejemplo de switch _____ que proporciona conexiones entre puertos con el mismo ancho de banda. _____ es un switch de LAN _____, que brinda conexiones conmutadas entre puertos de distinto ancho de banda.

- ✓ Topología B
- ✓ simétrica
- ✓ Topología A
- ✓ asimétrica

Completar la oración

Debido a la baja latencia de la mayoría de los switches de módem, _____ está mejor adaptado para la mayor parte de los entornos de switches.	por almacenamiento y envío
Un administrador de red debe evaluar la cantidad necesaria de ancho de banda para conexiones entre dispositivos para ajustar el flujo de datos de aplicaciones basadas en red a la hora de decidir el tipo de switch a elegir. Sin embargo, la mayoría de los switches actuales son _____ debido a que ofrecen la mayor flexibilidad.	asimétrica
En búfer de memoria _____, las tramas se almacenan en colas conectadas a interfaces de entrada específicas.	basada en puerto
En búfer de memoria _____, todas las tramas se depositan en un búfer de memoria común que comparten todos los puertos del switch.	compartido
Un switch de LAN de la Capa 2 realiza la conmutación y el filtrado en base a la dirección _____ de la capa _____.	enlace de datos MAC
Un switch de la capa 3 funciona en la capa _____ y utiliza información de la dirección _____ para tomar decisiones de envío del switch.	red IP

2.3 CONFIGURACION DE ADMINISTRACION DE SWTCHES.-

2.3.1 NAVEGACION POR LOS MODOS DE LA INTERFAZ DE LINEA DE COMANDOS.-

Modos de interfaz de línea de comando

En este tema, se revisará lo aprendido en CCNA Exploration: Aspectos básicos de redes acerca de cómo navegarpor los distintos modos de la interfaz de línea de comandos (CLI).

Como característica de seguridad, el software IOS de Cisco divide las sesiones de EXEC en los siguientes niveles de acceso:

EXEC usuario: Permite que una persona tenga acceso solamente a una cantidad limitada de comandos básicos de monitoreo. El modo EXEC del usuario es el modo predeterminado al que se ingresa después de iniciar sesión en un switch de Cisco desde la CLI. El modo EXEC del usuario se identifica con la indicación >.
EXEC privilegiado: Permite que una persona tenga acceso a todos los comandos del dispositivo, como aquellos que se utilizan para la configuración y administración, y es posible protegerlo por contraseña para que tengan acceso al dispositivo sólo los usuarios autorizados. El modo EXEC privilegiado se identifica con la indicación #.

Para pasar del modo EXEC del usuario al modo EXEC privilegiado, ingrese el comando **enable**. Para pasar del modo EXEC privilegiado al modo EXEC del usuario, ingrese el comando **disable**. En una red verdadera, el switch solicita la contraseña. Ingrese la contraseña correcta. De manera predeterminada, la contraseña no se configura. La figura muestra los comandos del IOS de Cisco que se utilizan para pasar del modo EXEC del usuario al modo EXEC privilegiado y viceversa.

Haga clic en el botón modo EXEC usuario y modo EXEC privilegiado en la figura.

Exploración de los modos de configuración

Una vez que ha ingresado el modo EXEC privilegiado en el switch de Cisco, puede tener acceso a otros modos de configuración. El software IOS de Cisco emplea una jerarquía de comandos en su estructura de modos de comandos. Cada modo de comandos admite comandos de Cisco IOS específicos que se relacionan con un tipo de operación en el dispositivo.

Existen muchos modos de configuración. Por ahora, se analizará cómo navegar por dos modos comunes de configuración: modo de configuración global y modo de configuración de interfaz.

Haga clic en el botón modos de configuración de Navegación en la figura.

Modo de configuración global

El ejemplo comienza con el switch en el modo EXEC privilegiado. Para configurar los parámetros globales del switch, como el nombre de host o la dirección IP del switch, que se emplean para la administración de switches, utilice el modo de configuración global. Para tener acceso al modo de configuración global, ingrese el comando **configure terminal** en el modo EXEC privilegiado. La indicación cambia a (config)#.

Modo de configuración de interfaz

Configurar los parámetros específicos de la interfaz es una tarea común. Para obtener acceso al modo de configuración de interfaz desde el modo de configuración global, ingrese el comando **interface**<nombre de interfaz>. La indicación cambia a (config-if)#. Para salir del modo de configuración de interfaz, utilice el comando **exit.** La indicación vuelve a cambiar a (config)#, haciéndole saber que se encuentra en el modo de configuración global. Para salir del modo de configuración global, ingrese nuevamente el comando **exit.** La indicación cambia a #, que representa al modo EXEC privilegiado.

Los modos Interfaz de la línea de comando

Sintaxis de comando de la CLI del IOS de Cisco	
Cambia de modo EXEC usuario a modo EXEC privilegiado.	switch>**enable**
Si una contraseña ha sido configurada para modo EXEC privilegiado, se le solicitará que la ingrese ahora.	password:**Contraseña**
La petición de entrada # significa modo EXEC privilegiado.	switch#
Cambia de modo EXEC privilegiado a modo EXEC usuario.	switch#**disable**
La petición de entrada > significa modo EXEC usuario.	switch>

modo EXEC usuario y modo EXEC privilegiado

Los modos Interfaz de la línea de comando

Sintaxis de comando de la CLI del IOS de Cisco	
Cambia de modo EXEC privilegiado a modo de configuración global.	switch#**configure terminal**
La petición de entrada (config)# significa que el switch está en modo de configuración global.	switch(config)#
Cambia de modo de configuración global a modo de configuración de interfaz para la interfaz 0/1 fast ethernet.	switch(config)#**interface fastethernet 0/1**
La petición de entrada (config)# significa que el switch está en modo de configuración de interfaz.	switch(config-if)#
Cambia de modo de configuración de interfaz a modo de configuración global.	switch(config-if)#**exit**
La petición de entrada (config)# significa que el switch está en modo de configuración global.	switch(config)#
Cambia de modo de configuración global a modo EXEC privilegiado.	switch(config)#**exit**
La petición de entrada # significa que el switch está en modo EXEC privilegiado.	switch#

Modos de configuración de navegación

Alternativas a la CLI basadas en la GUI

Existe una cantidad de alternativas de administración gráfica para administrar un switch de Cisco. El uso de una GUI ofrece facilidad de administración y configuración de switches, y no requiere tener amplio conocimiento sobre la CLI de Cisco.

Haga clic en el botón Asistente de red Cisco que se muestra en la figura.

Asistente de red Cisco

El asistente de red Cisco es una aplicación de la GUI basada en PC para la administración de redes y optimizada para las LAN pequeñas y medianas. Puede configurar y administrar grupos de switches o switches independientes. La figura muestra la interfaz de administración del asistente de red. El asistente de red Cisco está disponible sin costo alguno y puede descargarse desde Cisco (se requiere contraseña/nombre de usuario CCO):

http://www.cisco.com/go/networkassistant .

Haga clic en el botón Aplicación CiscoView de la figura.

Aplicación CiscoView

La aplicación de administración de dispositivos CiscoView proporciona una vista física del switch que se puede utilizar para establecer parámetros de configuración y para ver la información de funcionamiento y el estado del switch. La aplicación CiscoView, que se compra por separado, puede ser una aplicación independiente o bien formar parte de una plataforma de Protocolo de administración de red simple (SNMP) La figura muestra la interfaz de administración del Administrador de dispositivos CiscoView. Para obtener más información sobre el Administrador de dispositivos CiscoView, consulte el sitio:

http://www.cisco.com/en/US/products/sw/cscowork/ps4565/prod_bulletin0900aecd802948b0.html

Haga clic en el botón Administrador de dispositivos Cisco que se muestra en la figura.

Administrador de dispositivos Cisco

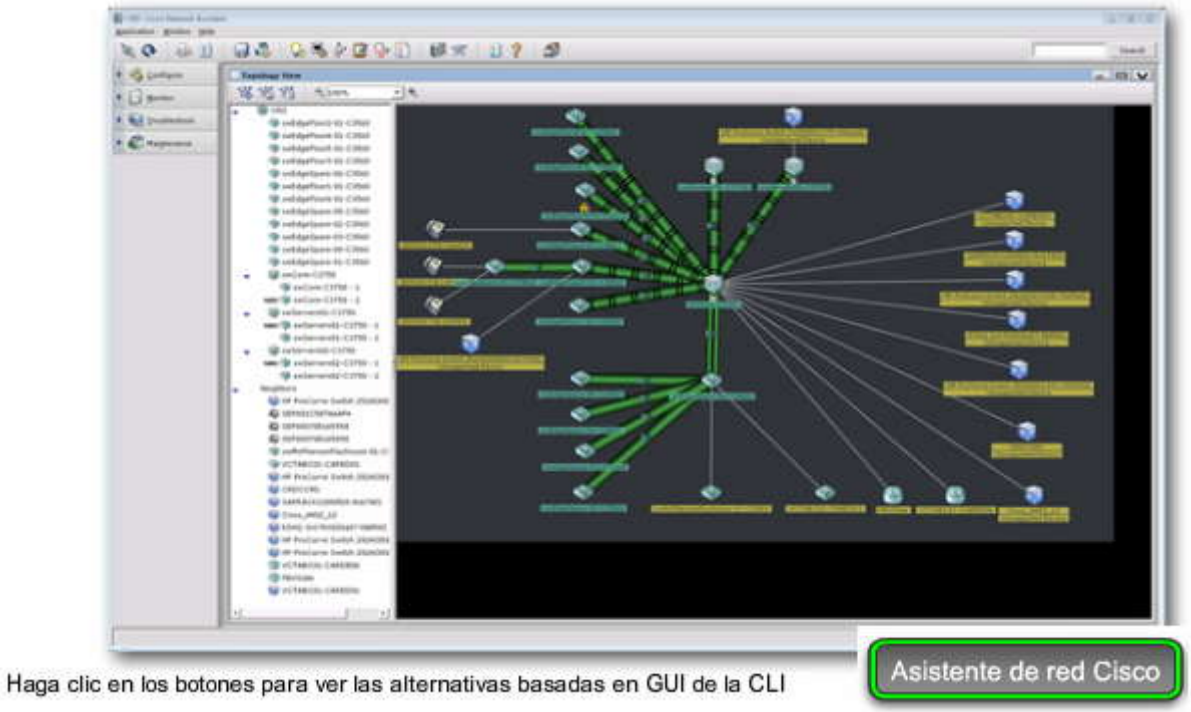
El administrador de dispositivos Cisco es un software basado en Web que se encuentra almacenado en la memoria del switch. Puede utilizar el Administrador de dispositivos y administrar los switches. Se puede obtener acceso al administrador de dispositivos desde cualquier sitio de la red a través del explorador Web. La figura muestra la interfaz de administración.

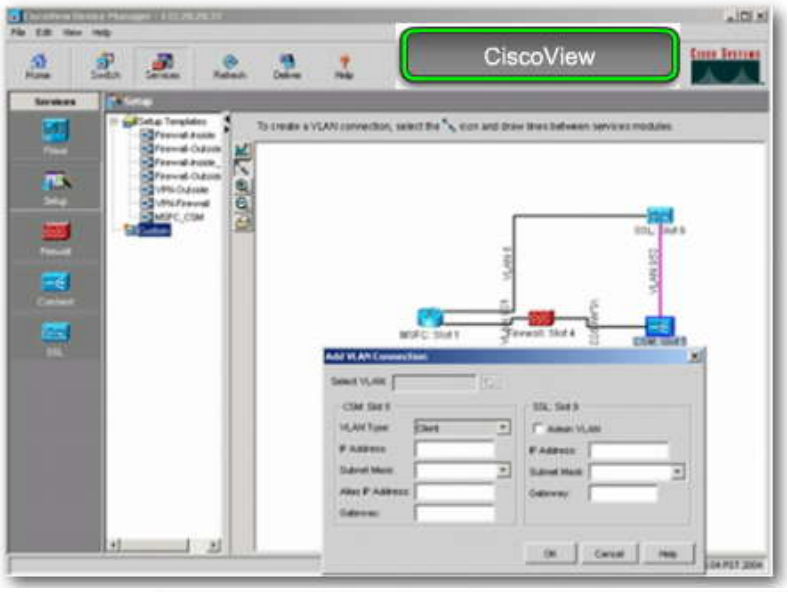
Haga clic en el botón Administración de red SNMP que se muestra en la figura.

Administración de red SNMP

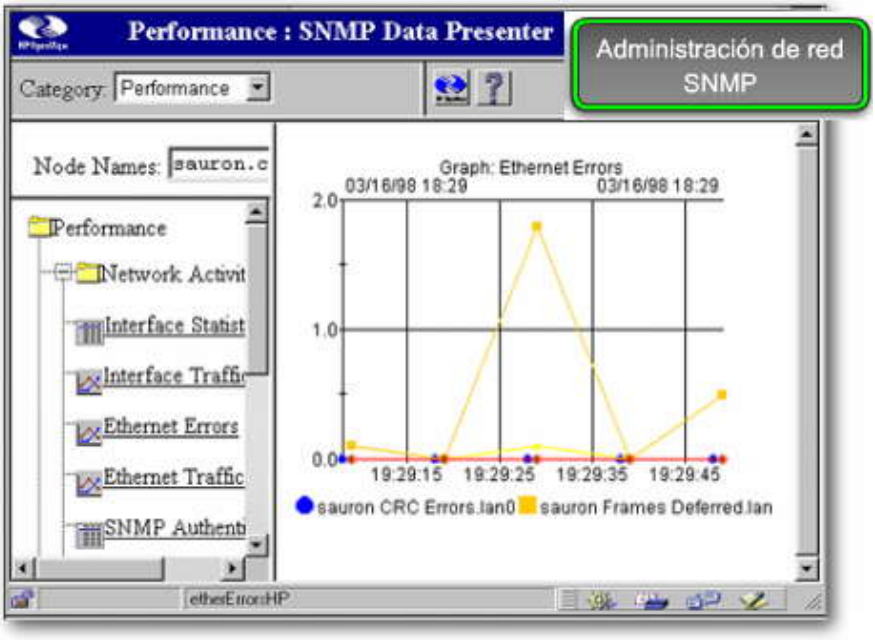
Se pueden administrar switches desde una estación de administración compatible con SNMP, como HP OpenView. El switch es capaz de proporcionar amplia información de administración y ofrece cuatro grupos de Monitoreo remoto (RMON) La administración de red SNMP es más frecuente en las redes de grandes empresas. Puede obtener más información sobre HP OpenView en el sitio:

http://h20229.www2.hp.com/news/about/index.html.




CiscoView


Catalyst 2960 Series Device Manager - switch
Administrador de dispositivos Cisco


Performance : SNMP Data Presenter
Administración de red SNMP
Category: Performance
Node Names: sauron.c
Performance
Network Activit
Interface Statist
Interface Traffic
Ethernet Errors
Ethernet Traffic
SNMP Authenti
Graph: Ethernet Errors
03/16/98 18:29
03/16/98 18:29
2.0
1.0
0.0
19:29:15
19:29:25
19:29:35
19:29:45
sauron CRC Errors.lan0
sauron Frames Deferred.lan
etherErrorHP

2.3.2 CÓMO UTILIZAR EL SEVICIO DE AYUDA.-

Ayuda sensible al contexto

La CLI del IOS de Cisco ofrece dos tipos de ayuda:

- **Ayuda de palabra:** Si no recuerda un comando completo pero sí recuerda los primeros caracteres, ingrese la secuencia de caracteres seguidos de un signo de interrogación (?). No introduzca ningún espacio antes del signo de interrogación.

Se mostrará una lista de comandos que comienzan con los caracteres que se han ingresado. Por ejemplo: si ingresa sh?, se mostrará una lista de todos los comandos que comiencen con esa secuencia de caracteres.

- **Ayuda de sintaxis de comando:** Si no sabe cuáles son los comandos disponibles en su contexto actual en la CLI del IOS de Cisco o si no conoce los parámetros que se requieren o están disponibles para completar un comando determinado, ingrese el comando ?.

Cuando sólo se ingresa ?, se muestra una lista de todos los comandos disponibles en el contexto. Si se ingresa el signo ? después de un comando específico, se mostrarán los argumentos de dicho comando. Si se muestra <cr>, significa que no se necesita ningún otro argumento para hacer funcionar el comando. Asegúrese de dejar un espacio antes del signo de interrogación para evitar que la CLI del IOS de Cisco lleve a cabo una ayuda de palabra en lugar de una ayuda de sintaxis de comando. Por ejemplo: ingrese **show ?** para obtener una lista de las opciones de comandos que admite el comando **show**.

La figura muestra las funciones de la ayuda de Cisco.

Se describirá cómo funciona la ayuda de la CLI utilizando como ejemplo el ajuste del reloj del dispositivo. Si se necesita ajustar el reloj del dispositivo pero no se conoce la sintaxis del comando **clock,** la ayuda contextual proporciona un modo de verificar dicha sintaxis.

La ayuda contextual provee el comando completo incluso si se ha ingresado sólo la primera parte del comando, por ejemplo, **cl?.**

Si ingresa el comando **clock** seguido de la tecla Enter, un mensaje de error indicará que el comando está incompleto. Para obtener los parámetros que se requieren para el comando **clock**, ingrese **?** precedido por un espacio. En el ejemplo de **clock** ?, el resultado de la ayuda muestra que se requiere la palabra clave set después de **clock**.

Si ahora ingresa el comando **clock set**, aparecerá otro mensaje de error indicando que el comando sigue estando incompleto. Agregue un espacio e ingrese el comando ? para que se muestre una lista de los argumentos de comandos que están disponibles en ese momento para el comando ingresado.

Se mostrarán los argumentos adicionales que se necesitan para ajustar el reloj en el dispositivo: la hora actual en horas, minutos y segundos. Para obtener valiosa información sobre el uso de la CLI del IOS de Cisco, visite:

Ayuda sensible al contexto

Sintaxis del comando de switch de Cisco	
Ejemplo de indicador de comando. En este ejemplo, la función de ayuda proporciona una lista de comandos disponibles en el modo actual que comienzan con cl.	switch**#cl?** clear clock
Ejemplo de comando incompleto.	switch**#clock** % Incomplete command.
Ejemplo de traducción simbólica.	switch**#colck** % Unknown command or computer name, or unable to find computer address
Ejemplo de indicador de comando. ¿Observa el espacio? En este ejemplo, la función de ayuda proporciona una lista de comandos asociados con el comando clock.	switch**#clock ?** set Establece la hora y fecha
En este ejemplo, la función de ayuda proporciona una lista de argumentos de comandos para el comando clock set.	switch**#clock set ?** hh:mm:ss Hora actual

Mensajes de error de consola

Los mensajes de error de la consola ayudan a identificar problemas cuando se ha ingresado un comando incorrecto. La figura proporciona ejemplos de mensajes de error, qué significan y cómo obtener ayuda cuando éstos se muestran

Mensajes de error de la consola

Ejemplo de mensaje de error	Significado	Cómo obtener ayuda
`switch#cl` `% Ambiguous command: "cl"`	No ingresó la cantidad suficiente de caracteres para que el dispositivo reconozca al comando.	Vuelva a ingresar el comando seguido de un signo de interrogación (?), sin espacio entre el comando y dicho signo. Se muestran las posibles palabras clave que puede ingresar con el comando.
`switch#clock` `% Incomplete command.`	No ingresó todas las palabras clave o valores requeridos por este comando.	Vuelva a ingresar el comando seguido de un signo de interrogación (?), con un espacio entre el comando y dicho signo.

`switch#clock set aa:12:23`
`^`
`% Invalid input detected at '^' marker.`
	Ingresó el comando de manera incorrecta. El símbolo del acento circunflejo (^) marca el lugar del error.	Ingrese un signo de interrogación (?) para mostrar todos los comandos o parámetros disponibles.

2.3.3 ACCESO AL HISTORIAL DE COMANDO.-

Búfer de historial de comandos

Al configurar varias interfaces en un switch, se puede ahorrar tiempo y evitar escribir los comandos nuevamente mediante el búfer del historial de comandos del IOS de Cisco. En este tema se explicará de qué manera configurar el búfer del historial de comandos para respaldar sus tareas de configuración.

La CLI de Cisco proporciona un historial o registro de los comandos que se han ingresado. Esta característica, llamada historial de comandos, es especialmente útil para ayudar a recordar entradas o comandos largos o complejos.

El historial de comandos permite llevar a cabo las siguientes tareas:

- Mostrar los contenidos del búfer de comandos.
- Establecer el tamaño del búfer del historial de comandos.
- Recordar comandos previamente ingresados y almacenados en el búfer del historial. Cada modo de configuración cuenta con un búfer exclusivo.

De manera predeterminada, el historial de comandos se activa y el sistema registra las últimas 10 líneas de comandos en el búfer de historial. Puede utilizar el comando **show history** para que se muestren los últimos comandos EXEC ingresados.

Búfer del historial de comandos

```
switch#show history
  enable
  show history
  enable
  config
  t
  confi
  t
  show history
switch#
```

Utilice el comando **show history** para ver los comandos EXEC ingresados recientemente.

Configurar el búfer de historial de comandos

En los productos de redes Cisco que admiten el software IOS de Cisco, el historial de comandos se activa de manera predeterminada y se registran las últimas 10 líneas de comandos en el búfer de historial.

El historial de comandos puede desactivarse para una determinada sesión de terminal mediante el comando **terminal no history** en el modo EXEC del usuario o privilegiado. Cuando se desactiva el historial de comandos, el dispositivo deja de retener las líneas de comandos que se ingresen.

Para revertir el tamaño del historial de terminal y establecerlo nuevamente al valor predeterminado de 10 líneas, ingrese el comando **terminal no history size** command in privileged EXEC mode. La figura proporciona una explicación y ejemplos de estos comandos del IOS de Cisco.

Configure el buffer de historial de comandos

Sintaxis de comando de la CLI del IOS de Cisco	
Habilite el historial del terminal. Este comando se puede ejecutar desde el modo EXEC privilegiado o usuario.	`switch#terminal history`
Configura el tamaño del historial del terminal. El historial del terminal puede mantener de 0 a 256 líneas de comando.	`switch#terminal history size 50`
Restablece el tamaño del historial del terminal al valor predeterminado de 10 líneas de comando.	`switch#terminal no history size`
Inhabilita el historial del terminal.	`switch#terminal no history`

2.3.4 SECUENCIA DE ARRANQUE DEL SWITCH.-

Describir la secuencia de arranque

En este tema, se explicará la secuencia de comandos del IOS de Cisco que ejecuta un switch desde el estado de apagado hasta que muestra la indicación para iniciar sesión. Una vez que el switch de Cisco se enciende, atraviesa la siguiente secuencia.

El switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa que se encuentra almacenado en la NVRAM y que se ejecuta cuando el switch se enciende por primera vez.

El cargador de arranque:

- Lleva a cabo la inicialización de bajo nivel de la CPU. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.
- Realiza el autodiagnóstico al encender (POST) para el subsistema de la CPU. Comprueba la DRAM de la CPU y la parte del dispositivo flash que integra el sistema de archivos flash.
- Inicializa el sistema de archivos flash en la tarjeta del sistema.
- Carga una imagen predeterminada del software del sistema operativo en la memoria y hace arrancar al switch. El cargador de arranque intenta encontrar la imagen del IOS de Cisco en el switch buscando primero en un directorio que tiene el mismo nombre que el archivo de imagen (sin incluir la extensión .bin). Si no la encuentra allí, el cargador de arranque busca en cada subdirectorio antes de continuar la búsqueda en el directorio original.

Luego, el sistema operativo inicializa las interfaces mediante los comandos del IOS de Cisco que se encuentran en el archivo de configuración del sistema operativo, config.text, y almacenados en la memoria flash del switch.

Recuperación tras un colapso del sistema

El cargador de arranque también proporciona acceso al switch en caso de que el sistema operativo no pueda utilizarse. El cargador de arranque cuenta con un dispositivo de línea de comandos que permite obtener acceso a los archivos almacenados en la memoria flash antes de que se cargue el sistema operativo. Desde la línea de comandos del cargador de arranque es posible ingresar comandos para formatear el sistema de archivos flash, volver a instalar la imagen de software del sistema operativo o recuperar una contraseña perdida u olvidada.

Descripción de la secuencia de arranque

Secuencia de arranque de un switch de Cisco:

-El switch carga el software cargador de arranque de NVRAM.

-El cargador de arranque:

- Realiza la inicialización de la CPU a bajo nivel.
- Realiza el POST para el subsistema de la CPU.
- Inicializa el sistema de archivos flash en la placa del sistema.
- Carga una imagen predeterminada de software de sistema operativo en la memoria y arranca el switch.

-El sistema operativo se ejecuta utilizando el archivo config.text, guardado en el almacenamiento flash del switch.

El cargador de arranque puede ser de utilidad en la recuperación en caso de un colapso del sistema operativo:

-Proporciona acceso al switch si el sistema operativo tiene problemas lo suficientemente graves como para quedar inutilizable.

-Proporciona acceso a los archivos almacenados en flash antes de que se cargue el sistema operativo.

-Utilice la línea de comandos del cargador de arranque para las operaciones de recuperación.

2.3.5 PREPARACIÓN PARA LA CONFIGURACION DEL SWITCH.-

Preparación para la configuración del switch

El inicio de un switch Catalyst requiere la ejecución de los siguientes pasos:

Paso 1. Antes de poner en funcionamiento el switch, verifique que:

Todos los cables de red estén correctamente conectados.

La PC o el terminal estén conectados al puerto de consola.

La aplicación del emulador de terminal, como HyperTerminal, esté funcionando y esté correctamente configurada.

La figura muestra una PC conectada a un switch mediante el puerto de consola.

Haga clic en el botón Configurar Hyperterminal de la figura.

La figura muestra la correcta configuración de HyperTerminal, que puede utilizarse para ver la consola de un dispositivo Cisco.

Paso 2. Conecte el cable de energía eléctrica al socket de la fuente de energía. El switch se pondrá en funcionamiento. Algunos switches Catalyst, incluida la serie Cisco Catalyst 2960, no cuentan con un botón de encendido.

Paso 3. Observe que la secuencia de arranque transcurra de la siguiente manera:

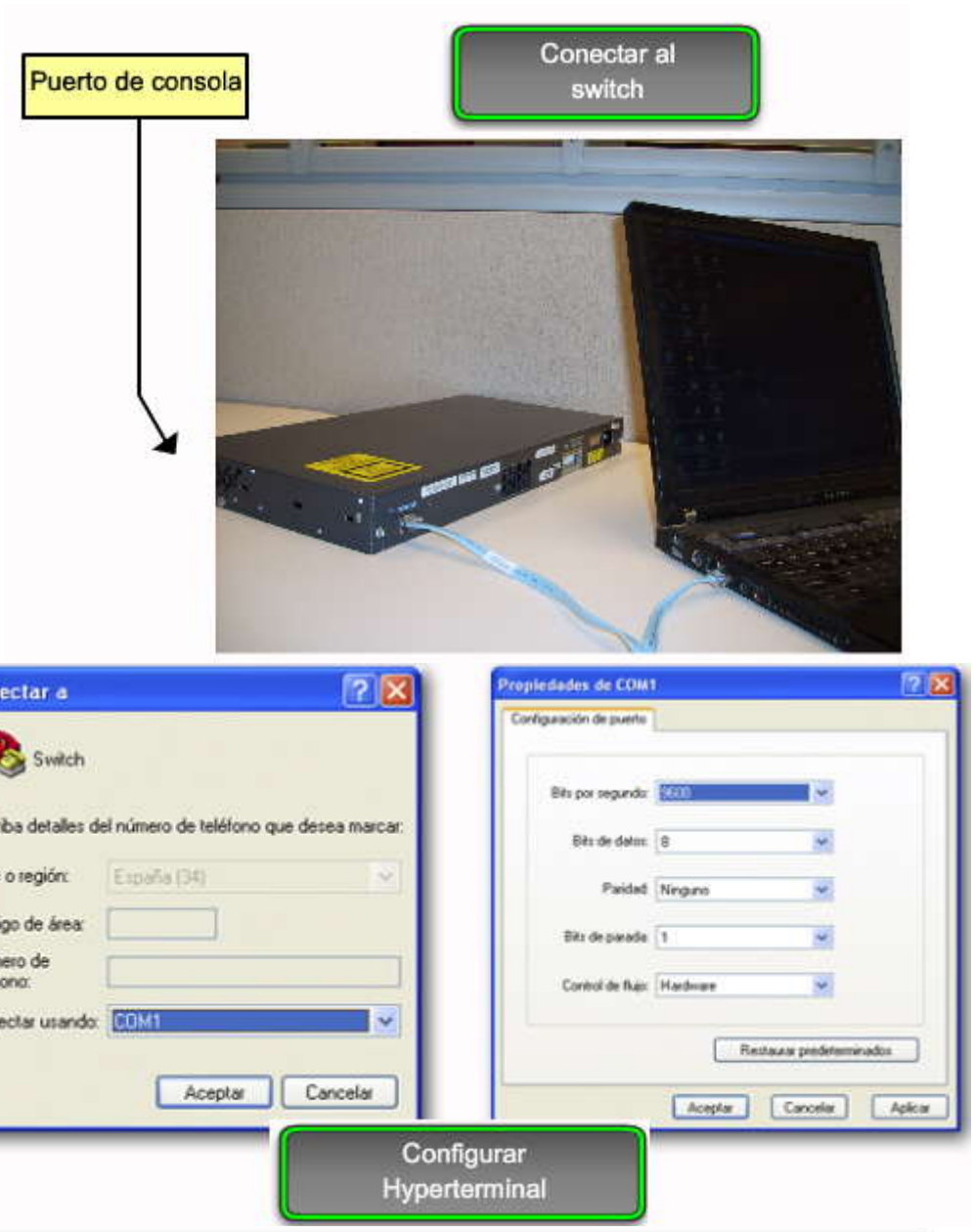
Cuando se enciende el switch, se inicia la prueba POST. Durante la POST, los indicadores de los LED parpadean mientras una serie de pruebas determina si el switch está funcionando correctamente. Cuando la POST finaliza, el LED SYST parpadea rápidamente en color verde. Si el switch no pasa la POST, el LED SYST se vuelve de color ámbar. Si un switch no aprueba la POST, será necesario repararlo.

Observe en la consola el texto del resultado del software IOS de Cisco.

En la figura, haga clic en el botón Ver proceso de arranque en la consola.

La figura muestra el proceso de arranque en la consola de un switch Cisco.

En la primera etapa del inicio del switch, si se detectan fallas en la POST, se envía un informe a la consola, y el switch no se pone en funcionamiento. Si la prueba POST se lleva a cabo con éxito y el switch no se ha configurado previamente, se le requerirá que lo haga.




```
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh
Image text-base: 0x00003000, data-base: 0x00AA2F34
flashfs[1]: 602 files, 19 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 32514048
flashfs[1]: Bytes used: 7715328
flashfs[1]: Bytes available: 24798720
flashfs[1]: flashfs fsck took 1 seconds.
flashfs[1]: Initialization complete....done Initializing
flashfs.

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC PortASIC interface Loopback Tests : Begin
POST: CPU MIC PortASIC interface Loopback Tests : End, Status
```

Ver proceso de arranque en la consola

2.3.6 CONFIGURACION BÁSICA DE SWITCH.-

Consideraciones de la interfaz de administración

Un switch de capa de acceso se parece mucho a una PC en que se necesita configurar una dirección IP, una máscara de subred y una gateway predeterminada. Para manejar un switch en forma remota mediante TCP/IP, se necesita asignar al switch una dirección IP. En la figura, S1 debe manejarse desde la PC 1, que es una computadora utilizada para administrar la red. Para llevar esto a cabo se necesita asignar una dirección IP al switch S1. Se asigna la dirección IP a una interfaz virtual denominada LAN virtual (VLAN) y luego se necesita asegurar que la VLAN se asigne a uno o más puertos específicos del switch.

La configuración predeterminada del switch es que su administración sea controlada a través de la VLAN 1. Sin embargo, la configuración básica recomendada para el switch es que la administración esté controlada por una VLAN que no sea la VLAN 1. Los fundamentos y las implicancias de dicha acción se explicarán en el próximo capítulo. La figura ilustra la utilización de VLAN 99 como VLAN de administración. Sin embargo, es importante tener en cuenta que puede utilizarse otra VLAN 99 como interfaz de administración.

Nota: Se proporcionarán más detalles sobre las VLAN en el próximo capítulo. Aquí, el tema central es proporcionar acceso de administración al switch a través de una VLAN alternativa. Algunos de los comandos ya introducidos serán explicados con mayor profundidad en el próximo capítulo.

Por ahora, se ha creado la VLAN 99 y se le ha asignado una dirección IP. Luego, el correspondiente puerto del switch S1 es asignado a VLAN 99. La figura también muestra la información sobre esta configuración.

Haga clic en el botón Configurar interfaz de administración de la figura.

Configurar interfaz de administración

La configuración de una dirección IP y una máscara de subred en la VLAN de administración del switch debe realizarse desde el modo de configuración de interfaz VLAN. Utilice el comando **interface vlan 99** e ingrese el comando de configuración de dirección ip. Se debe utilizar el comando de configuración de interfaz **no shutdown** para que esta interfaz de Capa 3 se ponga en funcionamiento. Cuando vea "interface VLAN x", se refiere a la interfaz de Capa 3 relacionada con la VLAN x. Sólo la VLAN de administración tiene una VLAN vinculada a ella.

Tenga en cuenta que un switch de Capa 2, como el Cisco Catalyst 2960, permite que sólo una interfaz de la VLAN se encuentre activa por vez. Ello significa que la interfaz de Capa 3 VLAN 99 está activa pero la interfaz de Capa 3 VLAN 1 no lo está.

Haga clic en el botón Configurar gateway predeterminada que se muestra en la figura.

Configurar Gateway predeterminada

El switch debe configurarse de modo tal que pueda reenviar paquetes IP a redes remotas. Es el mecanismo para llevar esto a cabo es la gateway predeterminada. El switch reenvía paquetes IP con direcciones IP de destino fuera de la red local a la gateway predeterminada. En la figura, el router R1 es el router de siguiente salto. Su dirección IP es 172.17.99.1.

Para configurar una gateway predeterminada para el switch, utilice el comando ip default-gateway. Ingrese la dirección IP de la interfaz del router de siguiente salto que está conectada directamente al switch en el que se ha de configurar la gateway predeterminada. Asegúrese de guardar la configuración en ejecución en un switch o router. Use el comando **copy running-config startup-config** para realizar una copia de respaldo de la configuración.

Haga clic en el botón Verificar Configuración de la figura.

Verificación Configuración

La imagen de pantalla que aparece en la parte superior de la figura es un resultado abreviado de pantalla que indica que se ha configurado la VLAN 99 con una dirección IP y máscara de subred, y que se ha asignado la interfaz de administración VLAN 99 al puerto Fast Ethernet F0/18.

Mostrar las interfaces IP

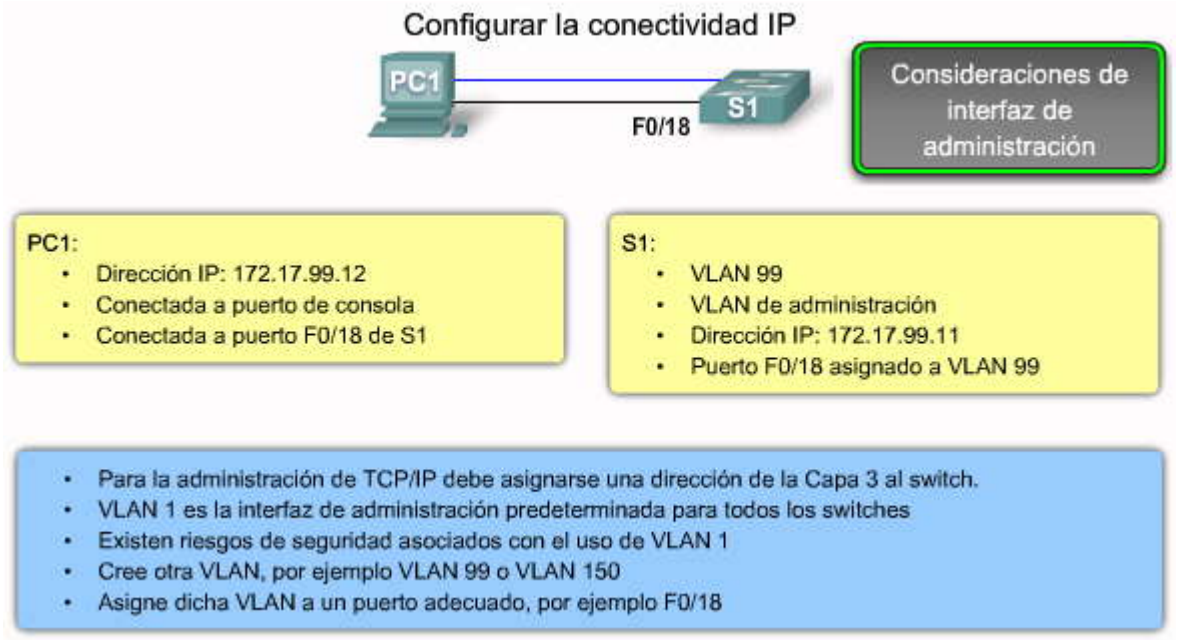
Use el comando **show ip interface brief** para verificar el estado y funcionamiento del puerto. Ensayará el uso del comando **switchport access vlan 99** en las prácticas de laboratorio y de Packet Tracer.

El comando mdix auto

Se solía requerir la utilización de ciertos tipos de cables (de conexión cruzada o conexión directa) para realizar conexiones entre dispositivos, por ejemplo, entre switches o entre un switch y un router. Ahora, en cambio, se puede utilizar el comando de configuración de interfaz **mdix auto** de la CLI para habilitar la función automática de conexión cruzada de interfaz dependiente del medio (auto-MDIX).

Al habilitar la función auto-MDIX, el switch detecta el tipo de cable que se requiere para las conexiones Ethernet de cobre y, conforme a ello, configura las interfaces. Por lo tanto, se puede utilizar un cable de conexión directa o cruzada para realizar la conexión con un puerto 10/100/1000 de cobre situado en el switch, independientemente del tipo de dispositivo que se encuentre en el otro extremo de la conexión.

La función auto-MDIX se habilita de manera predeterminada en los switches que ejecutan el software Cisco IOS, versión 12.2(18)SE o posterior. En el caso de las versiones existentes entre Cisco IOS, versión 12.1(14)EA1 y 12.2(18)SE, la función auto-MDIX está deshabilitada de manera predeterminada.



Configurar la conectividad IP

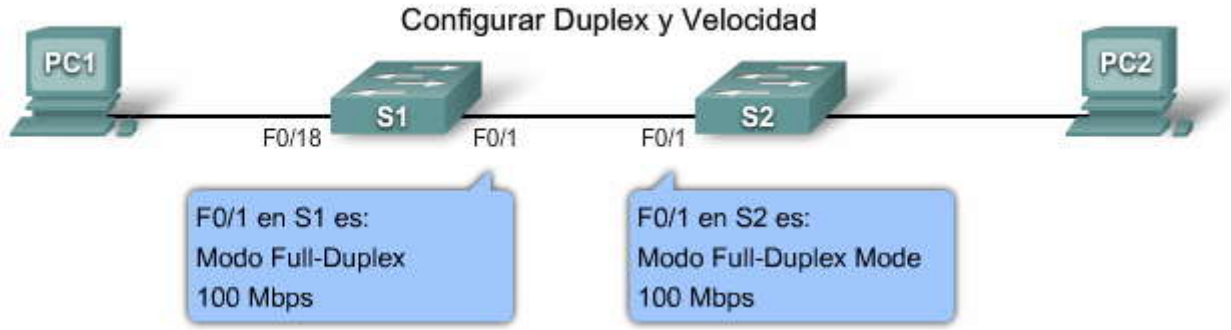
Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Ingrese al modo de configuración de interfaz para la interfaz de VLAN 99.	`S1(config)#interface vlan 99`
Configurar la dirección IP de la interfaz.	`S1(config-if)#dirección IP 172.17.99.11 255.255.255.0`
Habilitar la interfaz.	`S1(config-if)#no shutdown`
Regrese al modo EXEC privilegiado.	`S1(config-if)#end`
Ingrese al modo de configuración global.	`S1#configure terminal`
Ingrese la interfaz para asignar la VLAN.	`S1(config)#interface fastethernet 0/18`
Defina el modo de membresía de la VLAN para el puerto.	`S1(config-if)#switchport mode access`
Asigne el puerto a una VLAN.	`S1(config-if)#switchport acces vlan 99`
Regrese al modo EXEC privilegiado.	`S1(config-if)#end`
Guardar la configuración en ejecución en la configuración de inicio del switch.	`S1#copy running-config startup-config`

Configurar interfaz de administración

Sintaxis del comando de CLI IOS de Cisco	
Configura la gateway predeterminada en el switch.	`S1(config)#ip default-gateway 172.17.99.1`
Regrese al modo EXEC privilegiado.	`S1(config)#end`
Guardar la configuración en ejecución en la configuración de inicio del switch.	`S1#copy running-config startup-config`

Configurar duplex y velocidad

Se puede utilizar el comando de configuración de interfaz **duplex** para establecer el modo de operación dúplex en los puertos del switch. Es posible establecer manualmente el modo dúplex y la velocidad de los puertos del switch para evitar problemas entre distintos fabricantes con la autonegociación. Si bien pueden presentarse problemas al configurar los parámetros dúplex de los puertos del switch en **auto**, en este ejemplo los switches S1 y S2 cuentan con los mismos parámetros de velocidad y dúplex. La figura describe los pasos para configurar el puerto F0/1 en el switch S1.



Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Ingresar al modo de configuración de interfaz.	`S1(config)#Interface fastethernet 0/1`
Configurar el modo duplex de interfaz para activar la configuración duplex automática.	`S1(config-if)#duplex auto`
Configurar duplex y velocidad de la interfaz y activar la configuración de velocidad automática.	`S1(config-if)#speed auto`
Volver al modo EXEC privilegiado.	`S1(config-if)#end`
Guardar la configuración en ejecución en la configuración inicial del switch.	`S1#copy running-config startup-config`

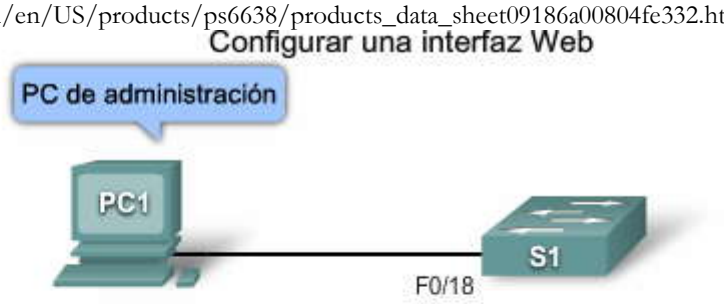
Configurar una interfaz de Web

Los switches modernos de Cisco cuentan con una serie de herramientas de configuración basadas en Web que requieren que el switch se configure como servidor HTTP. Estas aplicaciones incluyen la interfaz de usuario de explorador Web de Cisco, el Administrador de router y dispositivo de seguridad de Cisco, y las aplicaciones Telephony Service del IOS de Cisco e IP Phone.

Para controlar las personas que obtienen acceso a los servicios HTTP del switch, puede configurarse de manera opcional la autenticación. Los métodos de autenticación pueden ser complejos. Es probable que sean tantas las personas que utilizan los servicios HTTP que se requeriría un servidor independiente utilizado específicamente para administrar la autenticación de los usuarios. Los modos de autenticación AAA y TACACS son ejemplos que utilizan este tipo de método de autenticación remota. AAA y TACACS son protocolos de autenticación que pueden utilizarse en las redes para validar las credenciales del usuario. Posiblemente se necesite un método de autenticación menos complejo. El método enable requiere que los usuarios utilicen la contraseña de **enable** del servidor. El método de autenticación local requiere que el usuario ingrese la combinación de nombre de usuario de inicio de sesión, contraseña y acceso de nivel privilegiado especificados en la configuración del sistema local (a través del comando de configuración global **username**).

Si desea obtener más información sobre TACACS, visite el sitio:
http://www.cisco.com/en/US/tech/tk583/tk642/tsd_technology_support_sub-protocol_home.html.

Si desea obtener más información sobre AAA, visite el sitio:
http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.html.



Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Configurar la interfaz del servidor HTTP para el tipo de autenticación activado. Las otras opciones son. enable: se usa la contraseña enable, que es el método predeterminado de autenticación de usuario de servidor HTTP. local: se usa la base de datos local del usuario, según se define en el router Cisco o servidor de acceso tacacs: se usa el servidor TACACS.	`S1(config)#ip http authentication enable`
Activar el servidor HTTP.	`S1(config)#ip http server`
Volver al modo EXEC privilegiado.	`S1(config)#end`
Guardar la configuración en ejecución en la configuración inicial del switch.	`S1#copy running-config startup -config`

Gestión de la tabla de direcciones MAC

Los switches utilizan tablas de direcciones MAC para determinar cómo enviar tráfico de puerto a puerto. Estas tablasde direcciones MAC incluyen direcciones estáticas y dinámicas. La figura muestra un ejemplo de tabla de direcciones MAC, en el resultado del comando **show mac-address-table**, que incluye direcciones MAC estáticas y dinámicas.

Nota: La tabla de direcciones MAC fue previamente definida como memoria de contenido direccionable (CAM) o tabla CAM.

Las direcciones dinámicas son las direcciones MAC de origen que el switch registra y que luego expiran cuando no están en uso. Es posible cambiar el valor del tiempo de expiración de las direcciones MAC. El tiempo predeterminado es de 300 segundos. Si se establece un período de expiración muy corto, las direcciones podrían eliminarse de la tabla de manera prematura. Luego, cuando el switch reciba un paquete para un destino desconocido, lo enviará en forma masiva a todos los puertos de una misma LAN (o VLAN). Esta flooding innecesaria puede afectar el funcionamiento. Si, en cambio, se establece un período de expiración muy largo, la tabla de direcciones podría llenarse de direcciones no utilizadas e impedir que puedan registrarse las nuevas. Esto también puede provocar flooding.

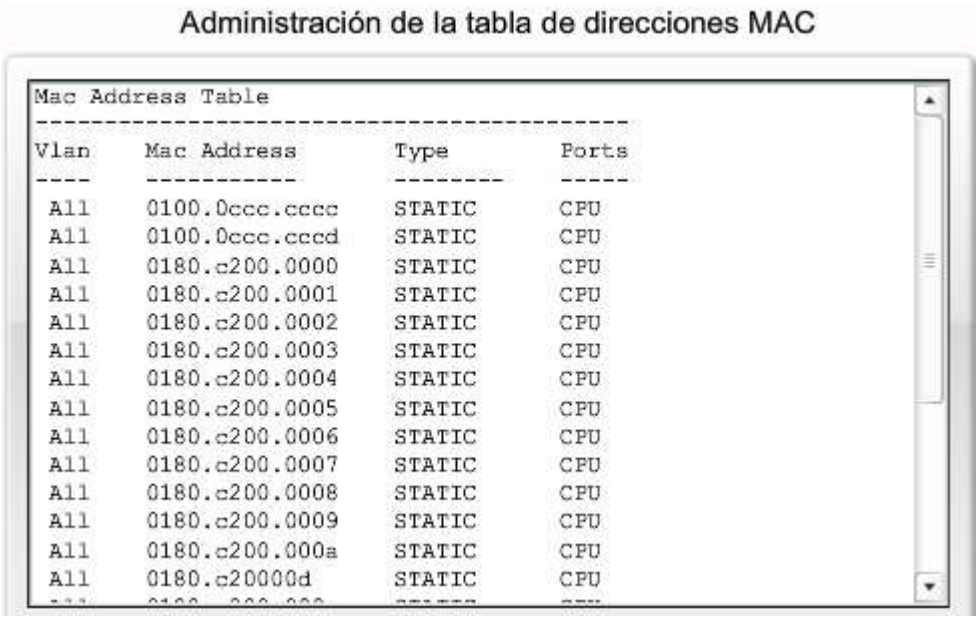
El switch proporciona direccionamiento dinámico al registrar la dirección MAC de origen de cada trama que recibe en cada puerto y al agregar luego la dirección MAC de origen y el número de puerto relacionado con ella a la tabla de direcciones MAC. A medida que se agregan o eliminan computadoras de la red, el switch actualiza la tabla de direcciones MAC al agregar nuevas entradas y eliminar las que ya no están en uso.

Un administrador de red puede asignar direcciones MAC estáticas a determinados puertos de manera específica. Las direcciones estáticas no expiran y el switch siempre sabe a qué puerto enviar el tráfico destinado a esa dirección MAC en particular. Por lo tanto, no necesita volver a registrar o realizar una actualización para saber a qué puerto se encuentra vinculada la dirección MAC. Una razón para implementar direcciones MAC estáticas es de proporcionar al administrador de red un completo control sobre el acceso a la red. Sólo los dispositivos conocidos por el administrador de red podrán conectarse a la red.

Para crear una asignación estática en la tabla de direcciones MAC, ingrese el comando **mac-address-table static** <dirección MAC> **vlan {1-4096, ALL} interface ID de interfaz**.

Para eliminar una asignación estática en la tabla de direcciones MAC, ingrese el comando no **mac-address-table static** <dirección MAC> **vlan {1-4096, ALL} interface ID de interfaz**.

El tamaño máximo de la tabla de direcciones MAC varía con distintos switches. Por ejemplo: el switch de la serie Catalyst 2960 puede almacenar hasta 8192 direcciones MAC. Existen otros protocolos que pueden limitar la cantidad absoluta de direcciones MAC disponibles para un switch.



2.3.7 VERIFICACIÓN DE LA CONFIGURACIÓN DEL SWITCH

Uso de los comandos Show

Ya realizada la configuración inicial del switch, se deberá confirmar que se ha llevado a cabo de manera correcta. En este tema se explicará cómo verificar la configuración del switch a través de distintos comandos **show.**

Haga clic en el botón Comandos show de la figura.

Cuando se necesita verificar la configuración del switch Cisco, el comando show es de gran utilidad. El comando **show** se ejecuta desde el modo EXEC privilegiado. La figura presenta algunas de las opciones clave del comando **show** que verifican casi todas las características configurables del switch. Existen varios comandos **show** adicionales que se irán introduciendo a lo largo del curso.

Haga clic en el botón show running-config que se muestra en la figura.

Uno de los comandos **show** más importantes es el comando **show running-config**. Este comando muestra la configuración que se está ejecutando en el switch. Utilice este comando para verificar que la configuración del switch sehaya realizado de manera correcta. La figura muestra un resultado abreviado del comando show running-config. Los tres puntos indican que falta contenido. En la figura, se encuentra resaltado el resultado de pantalla del switch 1, que muestra:

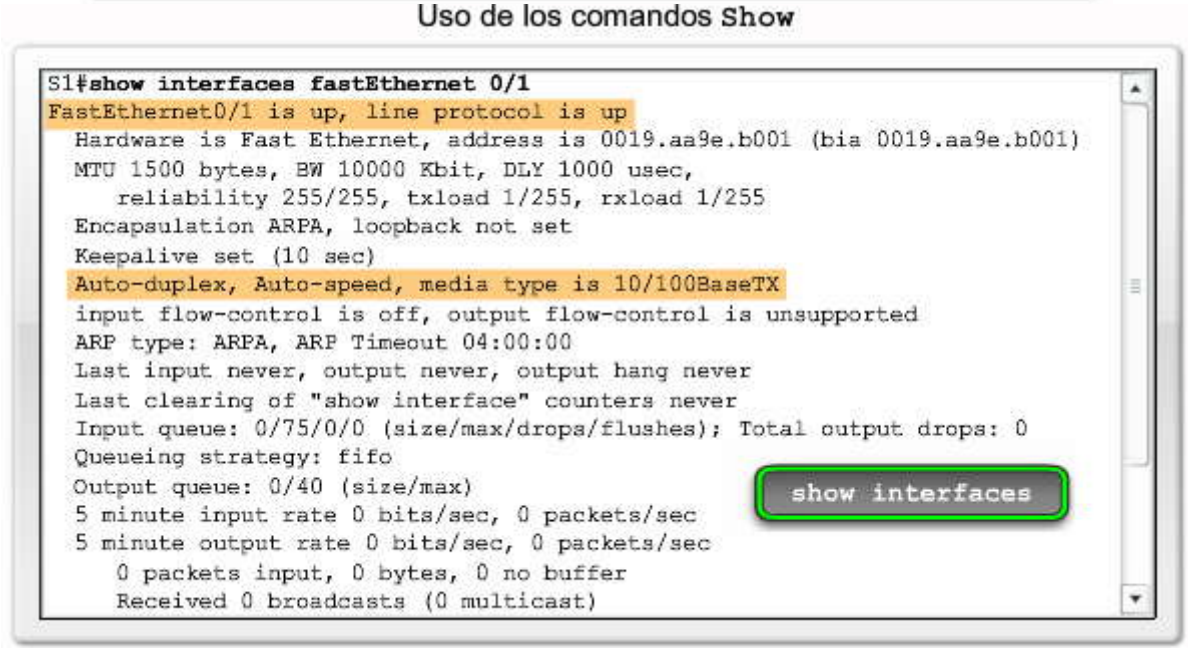
- Interfaz Fast Ethernet 0/18 configurada con la VLAN 99 de administración
- VLAN 99 configurada con una dirección IP de 172.17.99.11 255.255.0.0
- Gateway predeterminada establecida en 172.17.50.1
- Servidor HTTP configurado

Haga clic en el botón show interfaces que se muestra en la figura.

Otro comando frecuentemente utilizado es **show interfaces** que muestra la información estadística y el estado de las interfaces de red del switch. El comando **show interfaces** se utiliza habitualmente mientras se configuran y monitorean los dispositivos en la red. Recuerde que puede escribir un comando en forma parcial en la petición de entrada de comandos y que, siempre y cuando ninguna otra opción de comando sea la misma, el software IOS de Cisco lo interpretará de manera correcta. Por ejemplo: para este comando puede ingresar **show int**. La figura muestra el resultado de un **comando show interfaces FastEthernet 0/1**. La primera línea resaltada en la figura indica que la interfaz Fast Ethernet 0/1 está activa y en funcionamiento. La siguiente línea resaltada muestra que la configuración de dúplex es automática y la de velocidad también lo es.

Uso de los comandos Show

Sintaxis del comando de CLI IOS de Cisco	
Muestra el estado de la interfaz y la configuración para una o todas las interfaces disponibles del switch.	`show interfaces [interface-id]`
Muestra el contenido de la configuración de inicio.	`show startup-config`
Muestra la configuración de funcionamiento actual.	`show running-config`
Muestra información acerca de flash: sistema de archivos.	`show flash:`
Muestra el estado del hardware y el software del sistema.	`show version`
Muestra el historial de comandos de sesión.	`show history`
Muestra información de IP. La opción interface muestra el estado de la interfaz de IP y la configuración. La opción http muestra información de HTTP acerca del administrador de dispositivos que se ejecuta en el switch. La opción arp muestra la tabla ARP de IP.	`show ip {interface | http | arp}` Comandos show
Muestra la tabla MAC de envío.	`show mac-address-table`



2.3.8 ADMINISTRACIÓN BÁSICA DEL SWITCH.-

Respaldar y restaurar el switch

Una tarea típica del técnico de red es la de cargar al switch una configuración. En este tema, se explicará cómo cargar y almacenar una configuración en la memoria flash del switch y en un servidor TFTP.

Haga clic en el botón Respaldar configuraciones en la figura.

Cómo realizar la copia de seguridad de la configuración

Ya se ha explicado cómo realizar la copia de seguridad de la configuración en ejecución de un switch en el archivo de configuración de inicio. Se ha utilizado el comando **copy running-config startup-config** del modo EXEC privilegiado para realizar la copia de seguridad de las configuraciones realizadas hasta el momento. Como es sabido, la configuración en ejecución se guarda en la DRAM y la configuración de inicio se almacena en la sección NVRAM de la memoria Flash. Al introducir el comando **copy running-config startup-config,** el software IOS de Cisco copia la configuración en ejecución en la NVRAM, de modo que cuando el switch arranque, la configuración de inicio se cargue con la nueva configuración.

No siempre se desea guardar los cambios que se realizan en la configuración en ejecución de un switch. Por ejemplo: quizás se necesite cambiar la configuración por un breve período y no en forma permanente.

Si el usuario desea mantener varios archivos de configuración de inicio en el dispositivo, puede copiar la configuración en archivos de distinto nombre utilizando el comando copy startup-config flash:filename. El almacenamiento de varias versiones de configuración de inicio brinda la posibilidad de recurrir a ellos en caso de tener dificultades con la configuración en determinado momento. La figura muestra tres maneras de realizar la copia de seguridad de la configuración en la memoria Flash. La primera es la sintaxis completa y formal. La segunda es la sintaxis frecuentemente utilizada. Utilice la primer sintaxis si no conoce bien el dispositivo de red con el que está trabajando y utilice la segunda sintaxis si sabe que el destino es la NVRAM flash instalada en el switch. La tercera es la sintaxis utilizada para guardar una copia del archivo de configuración de inicio en la memoria flash.

Haga clic en el botón Restaurar configuraciones en la figura.

Restauración de la configuración

La restauración de una configuración es un proceso sencillo. Sólo se debe copiar la configuración guardada sobre la configuración actual. Por ejemplo: si tiene una configuración guardada llamada config.bak1, puede restaurarla sobre la configuración de inicio existente ingresando el comando copy flash:config.bak1 startup-config del IOS de Cisco. Una vez que se ha restaurado la configuración de inicio, se debe proceder a reiniciar el switch, de modo que éste recargue la nueva configuración de inicio, por medio del comando reload en el modo EXEC privilegiado.

El comando **reload** detiene el sistema. Si el sistema está configurado para reiniciarse en caso de errores, lo hará automáticamente. Después de introducir la información de configuración en un archivo y guardarla en la configuración de inicio, introduzca el comando reload.

Nota: No puede recargarse desde un terminal virtual si el switch no está configurado para reiniciarse automáticamente. Esta restricción evita que el sistema se desconecte del monitor ROM (ROMMON) y quede, por consiguiente, el sistema fuera del control del usuario remoto.

Después de ingresar el comando **reload**, el sistema preguntará si desea guardar la configuración. Normalmente debería responderse "sí" pero, en este caso en particular, la respuesta deberá ser "no". Si se respondiera en forma afirmativa, se sobrescribiría el archivo recientemente restaurado. Siempre debe considerarse si la configuración actual en ejecución es la que se quiere mantener activa después de la recarga.

Si desea obtener más información sobre el comando **reload**, consulte la guía Cisco IOS Configuration Fundamentals Command Reference, Release 12.4 en el sitio Web: http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Nota: También existe la opción de introducir el comando **copy startup-config running-config**. Desafortunadamente, este comando no sobrescribe completamente la configuración en ejecución sino que sólo agrega los comandos existentes de la configuración de inicio a la configuración en ejecución. Se recomienda tener cuidado al hacerlo, ya que podrían obtenerse resultados no deseados.

Respaldar y restaurar el switch

Sintaxis del comando de CLI IOS de Cisco	
Versión formal del comando copy de IOS de Cisco. Confirmar el nombre de archivo de destino. Presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**copy system:running-config flash:startup-config** Destination filename [startup-config]?
Versión informal del comando copy. Se supone que running-config se está ejecutando en el sistema y que el archivo startup-config se almacenará en NVRAM flash. Presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**copy running-config startup-config** Destination filename [startup-config]? Respaldar configuraciones
Hacer una copia de respaldo de startup-config en un archivo almacenado en NVRAM flash. Confirmar el nombre de archivo de destino. Presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**copy startup-config flash:config.bak1** Destination filename [config.bak1]?

Respaldar y restaurar el switch

Sintaxis del comando de CLI IOS de Cisco	
Copia el archivo config.bak1 almacenado en flash a la configuración de inicio supuestamente almacenada en flash. Presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**copy flash:config.bak1 startup-config** Destination filename [startup-config]? Restaurar configuraciones
Permite que IOS de Cisco ejecute el reinicio del switch. Si se ha modificado el archivo de configuración en ejecución se le solicitará que lo guarde. Confirme con 'y' o con 'n'. Para confirmar la recarga presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**reload** Se ha modificado la configuracin del sistema. Save? [yes/no]: n Proceed with reload? [confirm]?

Archivos de configuración de respaldo en un servidor TFTP

Una vez configurado el switch con todas las opciones deseadas, se recomienda hacer una copia de seguridad de la configuración y colocarla en un archivo junto con las otras copias de seguridad del resto de la información de lared. Al tener la configuración almacenada de manera segura fuera del switch, éste queda protegido en caso de que surja algún problema serio.

Algunas configuraciones de switch tardan muchas horas en comenzar a funcionar correctamente. Si se pierde la configuración debido a una falla en el hardware del switch, se necesitará configurar uno nuevo. Si existe una copia de seguridad de la configuración del switch en falla, ésta podrá cargarse rápidamente en el nuevo switch. De no existir dicha copia de seguridad, se deberá configurar el nuevo switch desde cero.

Se puede utilizar TFTP para realizar la copia de seguridad de los archivos de configuración en la red. El software IOS de Cisco viene con un cliente de TFTP incorporado que permite que el usuario se conecte con un servidor TFTP en su red.

Nota: Existen paquetes de software de servidores TFTP gratis en Internet que el usuario puede utilizar en caso de no contar con ninguno de éstos. Un servidor TFTP que se utiliza frecuentemente es de www.solarwinds.com.

Creación de la copia de seguridad de la configuración

Para subir un archivo de configuración del switch al servidor TFTP para su almacenamiento, se deberán seguir los siguientes pasos:

Paso 1. Verifique que el servidor TFTP se esté ejecutando en la red.

Paso 2. Inicie sesión en el switch a través del puerto de consola o sesión Telnet. Habilite el switch y luego haga ping al servidor TFTP.

Paso 3. Suba la configuración del switch en el servidor TFTP. Especifique la dirección IP o el nombre de host delservidor TFTP y el nombre del archivo de destino. El comando del IOS de Cisco es: **#copy system:running-config** tftp:[[[//ubicación]/directorio]/nombre del archivo] or**#copy nvram:startup-config** tftp:[[[//ubicación]/directorio]/nombre del archivo].

La figura muestra un ejemplo de cómo realizar la copia de seguridad de la configuración en un servidor TFTP.

Restauración de la configuración

Una vez que la configuración se ha almacenado correctamente en el servidor TFTP, se la puede copiar nuevamente en el switch mediante los siguientes pasos:

Paso 1. Copie el archivo de configuración en el correspondiente directorio del servidor TFTP (si es que ya no se encuentra allí).

Paso 2. Verifique que el servidor TFTP se esté ejecutando en la red.

Paso 3. Inicie sesión en el switch a través del puerto de consola o sesión Telnet. Habilite el switch y luego haga ping al servidor TFTP.

Paso 4. Descargue el archivo de configuración del servidor TFTP para configurar el switch. Especifique la dirección IP o el nombre de host del servidor TFTP y el nombre del archivo que desea descargar. El comando del IOS de Cisco es: #copy **tftp**:[[[//ubicación]/directorio]/nombre del archivo] **system:running-config** or **#copy tftp:**[[[//ubicación]/directorio]/nombre del archivo] **nvram:startup-config**.

Si el archivo de configuración se descarga en la configuración en ejecución, los comandos se ejecutan mientras el archivo se analiza sintácticamente línea por línea. Si el archivo de configuración se descarga en la configuración de inicio, se deberá volver a cargar el switch para hacer efectivos los cambios.

Copia de respaldo de los archivos de configuración en un servidor TFTP

```
S1#copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
Writing tokyo-confg!!! [OK]
```

Eliminación de los archivos de configuración

Es posible borrar la información de la configuración de inicio. Puede llevar esto a cabo en caso de tener que enviar un switch usado a un cliente o bien a otro departamento y desee asegurarse de que se configure el switch nuevamente. Al borrar el archivo de configuración de inicio, cuando el switch se reinicia, se ejecuta el programa de configuración inicial para que éste pueda reconfigurarse con los nuevos parámetros.

Para borrar el contenido de la configuración de inicio, utilice el comando **erase nvram: o erase startup-config** del modo EXEC privilegiado. La figura muestra un ejemplo de eliminación de los archivos de configuración almacenados en NVRAM.

Precaución: No se podrá restaurar el archivo de configuración de inicio una vez que se ha borrado el archivo correspondiente. Por consiguiente, asegúrese de guardar una copia de seguridad de ella en caso de necesitar restaurarla más adelante.

Eliminación de un archivo de configuración almacenado

Puede haber estado trabajando en una compleja tarea de configuración y haber guardado varias copias de seguridad de los archivos en Flash. Para borrar un archivo de la memoria Flash, utilice el comando **delete flash**: nombre del archivo del modo EXEC privilegiado. Según los parámetros del comando de configuración global de indicación de archivos, es posible que se le pida una confirmación antes de borrar el archivo. De manera predeterminada, el switch solicita una confirmación antes de borrar un archivo.

Precaución: No se podrá restaurar el archivo de configuración de inicio una vez que se ha borrado el archivo correspondiente. Por consiguiente, asegúrese de guardar una copia de seguridad de ella en caso de necesitar restaurarla más adelante.

Una vez que se ha borrado o eliminado la configuración, se puede volver a cargar el switch con una nueva configuración.

Eliminación de los archivos de configuración

```
S1#erase nvram:
Erasing the nvram filesystem will remove all configuration
files!
Continue? [confirm]
[OK]
Erase of nvram: complete
S1#
```

2.4 CONFIGURACION DE LA SEGURIDAD DEL SWITCH.-

2.4.1 CONFIGURACIÓN DE OPCIONES DE LAS CONTRASEÑAS.

Configurar el acceso a la consola

En este tema, se explicará cómo configurar las contraseñas para el acceso a la consola, al terminal virtual y al modo EXEC. También se detallará cómo encriptar y recuperar contraseñas en un switch.

Esta información es sumamente importante y debe permanecer muy bien guardada y protegida. La Oficina Federal de Investigación (FBI, Federal Bureau of Investigation) de los Estados Unidos calcula que las empresas pierden

aproximadamente 67 200 millones de dólares por año como consecuencia de los delitos relacionados con la informática. En particular, la información personal de los clientes se vende a precios altísimos. A continuación, se presentan algunos precios actuales de datos robados:

- Cajeros automáticos (ATM, Automatic Teller Machine) o tarjeta de débito con número de identificación personal (PIN): $500
- Número de licencia de conducir: $150
- Número del seguro social: $100
- Número de tarjeta de crédito con fecha de vencimiento: de $15 a $20

La seguridad de los switches comienza con la protección de ellos contra el acceso no autorizado.

Se pueden realizar todas las opciones de configuración desde la consola. Para acceder a la consola, se necesita tener acceso físico local al dispositivo. Si no se asegura la consola de forma adecuada, usuarios malintencionados podrían comprometer la configuración del switch.

Protección de la consola

Para proteger el puerto de consola contra el acceso no autorizado, establezca una contraseña utilizando el comando de modo de configuración de línea **password** <password>. Utilice el comando **line console 0** para conmutar del modo de configuración global al modo de configuración de línea para la consola 0, que es el puerto de consola de los switches Cisco. La indicación cambia a (config-line)#, señalando que ahora el switch está en el modo de configuración de línea. Desde el modo de configuración de línea se puede establecer la contraseña para la consola mediante el comando**password** <password>. Para asegurar que el usuario que desee tener acceso al puerto de consola deba introducir la contraseña, utilice el comando **login**. Aun cuando se ha establecido una contraseña, no se solicitará que se la introduzca si no se ha introducido el comando **login.**

La figura muestra los comandos utilizados para configurar y solicitar la contraseña para el acceso a la consola. Recuerde que puede utilizar el comando **show running-config** para verificar la configuración. Antes de completar la configuración del switch, recuerde guardar el archivo de configuración en ejecución en la configuración de inicio.

Eliminación de la contraseña de consola

Si necesita eliminar la contraseña y la solicitud de ingreso de contraseña al iniciar sesión, siga los pasos a continuación:

Paso 1. Cambie de modo EXEC privilegiado a modo de configuración global. Ingrese el comando **configure terminal**.

Paso 2. Cambie del modo de configuración global al modo de configuración de línea para la consola 0. La indicación del comando (config-line)# señala que se encuentra en el modo de configuración de línea. Ingrese el comando **line console 0.**

Paso 3. Elimine la contraseña de la línea de la consola mediante el comando **no password**.

Precaución: Si no se ha establecido ninguna contraseña y el inicio de sesión aún se encuentra habilitado, no se podrá tener acceso a la consola.

Paso 4. Elimine la solicitud de ingreso de contraseña al iniciar sesión en la consola mediante el comando **no login**.

Paso 5. Salga del modo de configuración de línea y regrese al modo EXEC privilegiado mediante el comando **end.**

Configuración del acceso a la consola

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Cambio del modo de configuración global a modo de configuración de línea para la consola 0.	`S1(config)#line con 0`
Establece cisco como contraseña para la línea de la consola 0 del switch.	`S1(config-line)#password cisco`
Establece la línea de consola para que solicite el ingreso de la contraseña antes de conceder el acceso.	`S1(config-line)#login`
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	`S1(config-line)#end`

Protección de los Puertos vty

Los puertos vty de un switch Cisco permiten obtener acceso remoto al dispositivo. Es posible llevar a cabo todas las opciones de configuración mediante los puertos de terminal vty. No se necesita acceso físico al switch para obtener acceso a los puertos vty. Por ello, es muy importante que estén protegidos. Cualquier usuario con acceso de red al switch puede establecer una conexión remota de terminal vty. Si no se aseguran los puertos vty en forma adecuada, usuarios malintencionados podrían comprometer la configuración del switch.

Para proteger los puertos vty contra el acceso no autorizado, se puede establecer que se requiera una contraseña de vty permitir el acceso.

La contraseña de los puertos vty debe establecerse desde el modo de configuración de línea.

Un switch de Cisco puede contar con varios puertos vty disponibles. Varios puertos permiten que más de un administrador pueda conectarse y administrar el switch. Para proteger todas las líneas vty, asegúrese de que se establezca una contraseña y que el inicio de sesión sea obligatorio en todas las líneas. La falta de protección en algunas líneas compromete la seguridad y permite el acceso no autorizado al switch.

Utilice el **comando line vty 0 4** para cambiar del modo de configuración global al modo de configuración de línea para las líneas vty de 0 a 4.

Nota: Si el switch tiene más líneas vty disponibles, ajuste el intervalo para proteger a todas ellas. Por ejemplo: el Cisco 2960 tiene disponibles desde la línea 0 hasta la 15.

La figura muestra los comandos utilizados para configurar y solicitar la contraseña para el acceso a vty. Puede utilizar el comando **show running-config** para verificar la configuración y el comando **copy running-config startup config** para guardar el trabajo realizado.

Eliminación de la contraseña de vty

Si necesita eliminar la contraseña y la solicitud de ingreso de contraseña al iniciar sesión, siga los pasos a continuación:
Paso 1. Cambie de modo EXEC privilegiado a modo de configuración global. Ingrese el comando **configure terminal**.
Paso 2. Cambie del modo de configuración global al modo de configuración de línea para los terminales de 0 a 4. La indicación del comando (config-line)# señala que está en el modo de configuración de línea. Ingrese el comando **line vty 0 4.**
Paso 3. Elimine la contraseña de la línea de la consola mediante el comando **no password**.
Precaución: Si no se ha establecido ninguna contraseña y el inicio de sesión aún se encuentra habilitado, no se podrá tener acceso a la consola.
Paso 4. Elimine la solicitud de ingreso de contraseña al iniciar sesión en la consola mediante el comando **no login**.
Paso 5. Salga del modo de configuración de línea y regrese al modo EXEC privilegiado mediante el comando **end.**

Configuración del acceso del terminal virtual

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Cambio del modo de configuración global a modo de configuración de línea para la consola 0.	`S1(config)#line vty 0 4`
Establece cisco como contraseña para la línea de la consola 0 del switch.	`S1(config-line)#password cisco`
Establece la línea de consola para que solicite el ingreso de la contraseña antes de conceder el acceso.	`S1(config-line)#login`
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	`S1(config-line)#end`

Configurar contraseñas del modo EXEC

El modo EXEC privilegiado permite que cualquier usuario habilite este modo en un switch Cisco para configurar cualquier opción disponible en el switch. También puede ver todos los parámetros de la configuración en curso del switch e incluso algunas de las contraseñas encriptadas. Por este motivo, es importante resguardar el acceso al modo EXEC privilegiado.

El comando de configuración global **enable password** permite especificar una contraseña para restringir el acceso al modo EXEC privilegiado. Sin embargo, una desventaja del comando **enable password** es que almacena la contraseña en texto legible en la configuración de inicio y en la configuración en ejecución. Si alguna persona obtuviese acceso a un archivo de configuración de inicio almacenado o bien acceso temporal a una sesión de Telnet o de consola que se encuentre en el modo EXEC privilegiado, podría leer la contraseña. Como consecuencia, Cisco introdujo una nueva opción de contraseña para controlar el acceso al modo EXEC privilegiado que almacena dicha contraseña en un formato encriptado.

Se puede asignar una forma encriptada de la contraseña de enable, llamada contraseña secreta de enable, ingresando el comando **enable secret** con la contraseña deseada en la solicitud del modo de configuración global. Si se configura la contraseña secreta de enable, se utiliza ésa en lugar de la contraseña de enable y no además de ella. El software IOS de Cisco también cuenta con una salvaguarda incorporada que evita que el usuario configure la contraseña secreta de enablecon la misma contraseña utilizada para la contraseña de enable.

La figura muestra los comandos utilizados para configurar las contraseñas del modo EXEC privilegiado. Puede utilizar el comando **show running-config** para verificar la configuración y el comando **copy running-config startup config** para guardar el trabajo realizado.

Eliminación de la contraseña del modo EXEC

Si desea eliminar la solicitud de contraseña para obtener acceso al modo EXEC privilegiado, puede utilizar los comandos **no enable password** y **no enable secret** desde el modo de configuración global.

Configuración de las contraseñas para modo EXEC

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Configura la **contraseña de habilitación** para ingresar al modo EXEC privilegiado.	`S1(config)#enable password password`
Configura la **contraseña de habilitación** secreta para ingresar al modo EXEC privilegiado.	`S1(config)#enable secret password`
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	`S1(config)#end`

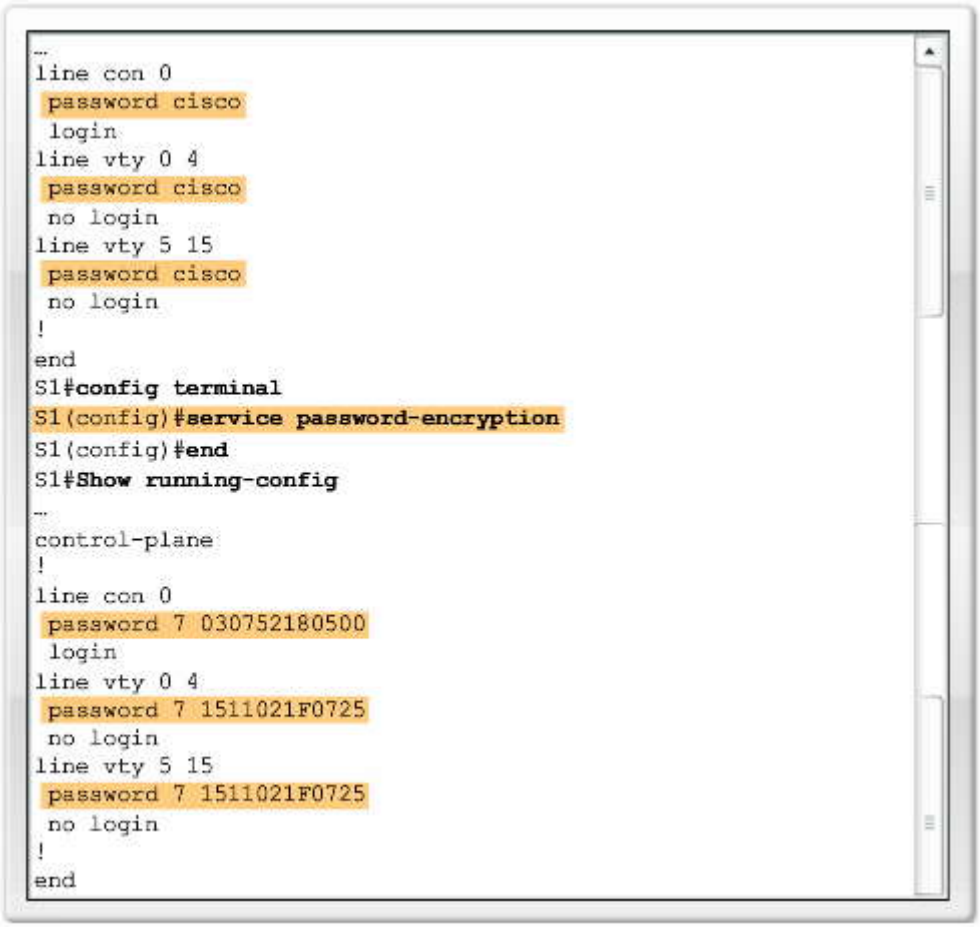
Configurar contraseñas encriptadas

Cuando se configuran contraseñas en la CLI del IOS de Cisco, todas ellas, excepto la contraseña secreta de enable, se almacenan de manera predeterminada en formato de texto sin cifrar dentro de la configuración de inicio y de la configuración en ejecución. La figura muestra un resultado de pantalla abreviado del comando **show running-config** del switch S1. Las contraseñas en texto sin cifrar están resaltadas en color naranja. Como norma universal, las contraseñas deben estar encriptadas y no almacenadas en formato de texto sin cifrar. El comando del IOS de Cisco **service password-encryption** habilita la encriptación de la contraseña de servicio.

Cuando se ingresa el comando **service password-encryption** desde el modo de configuración global, todas las contraseñas del sistema se almacenan en formato encriptado. No bien se ingresa el comando, todas las contraseñas establecidas en el momento se convierten en contraseñas encriptadas. En la parte inferior de la figura, las contraseñas encriptadas están resaltadas en color naranja.

Si desea eliminar el requisito de almacenar todas las contraseñas del sistema en formato encriptado, ingrese el comando no service password-encryption desde el modo de configuración global. La eliminación de la característica de encriptación de contraseñas no vuelve a convertir las contraseñas ya encriptadas en formato de texto legible. No obstante, todas las contraseñas que se configuren de allí en más se almacenarán en formato de texto legible.

Nota: El comando service password-encryption se conoce como tipo 7. Este estándar de encriptación es muy débil y existen herramientas de fácil acceso en Internet para descifrar las contraseñas encriptadas con dicho estándar. El tipo 5 es más seguro, pero debe realizarse de forma manual para cada contraseña que se configure.



Recuperación de contraseña de Enable

Después de configurar contraseñas para controlar el acceso a la CLI del IOS de Cisco, el usuario debe asegurarse de recordarlas. En caso de que se pierdan u olviden las contraseñas de acceso, Cisco cuenta con un mecanismo de recuperación de contraseña que permite a los administradores obtener acceso a los dispositivos de Cisco. El proceso de recuperación de contraseña requiere el acceso físico al dispositivo. La figura muestra una captura de pantalla del visualizador de la consola que indica que se ha habilitado la recuperación de contraseña. El visualizador se verá después del paso 3 más abajo.

Tenga en cuenta que probablemente no pueda recuperar realmente las contraseñas del dispositivo Cisco, especialmente si se ha habilitado la encriptación de contraseñas, pero sí podrá restablecerlas con un nuevo valor.

Si desea obtener más información sobre el procedimiento de contraseñas, visite el sitio: http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Para recuperar la contraseña de un switch Cisco 2960, lleve a cabo los siguientes pasos:

Paso 1. Conecte un terminal o PC, con el software de emulación de terminal, al puerto de consola del switch.

Paso 2. Establezca la velocidad de línea del software de emulación en 9600 baudios.

Paso 3. Apague el switch. Vuelva a conectar el cable de alimentación al switch y, en no más de 15 segundos, presione el botón Mode mientras la luz verde del LED del sistema esté parpadeando. Siga presionando el botón Mode hasta que el LED del sistema cambie al color ámbar durante unos segundos y luego verde en forma permanente. Suelte el botón Mode.

Paso 4. Inicialice el sistema de archivos Flash a través del comando **flash_init.**

Paso 5. Cargue archivos helper mediante el comando **load_helper.**

Paso 6. Visualice el contenido de la memoria Flash a través del comando **dir flash:**

Se mostrará el sistema de archivos del switch:

Directory of flash:/

13 drwx 192 Mar 01 1993 22:30:48 c2960-lanbase-mz.122-25.FX
11-rwx 5825 Mar 01 1993 22:31:59 config.text
18 -rwx 720 Mar 01 1993 02:21:30 vlan.dat
16128000 bytes total (10003456 bytes free)

Paso 7. Cambie el nombre del archivo de configuración por config.text.old, que contiene la definición de la contraseña, mediante el comando **rename flash:config.text flash:config.text.old.**

Paso 8. Reinicie el sistema con el comando **boot.**

Paso 9. Se solicitará que ejecute el programa de configuración inicial. Ingrese **N** ante la solicitud y, luego, cuando el sistema pregunte si desea continuar con el diálogo de configuración, ingrese **N.**

Paso 10. Ante la indicación de switch, ingrese al modo EXEC privilegiado por medio del comando **enable.**

Paso 11. Cambie el nombre del archivo de configuración y vuelva a colocarle el nombre original mediante el comando **rename flash:config.text.old flash:config.text.**

Paso 12. Copie el archivo de configuración en la memoria a través del comando **copy flash:config.text system:running-config**. Después de ingresar este comando, se mostrará el siguiente texto en la consola:

Source filename [config.text]?

Destination filename [running-config]?

Presione Return en respuesta a las solicitudes de confirmación. El archivo de configuración se ha cargado nuevamente y, ahora, se puede cambiar la contraseña.

Paso 13. Ingrese al modo de configuración global mediante el comando **configure terminal.**

Paso 14. Cambie la contraseña mediante el comando **enable secret password.**

Paso 15. Regrese al modo EXEC privilegiado mediante el comando **exit**.

Paso 16. Escriba la configuración en ejecución en el archivo de configuración de inicio mediante el comando **copy running-config startup-config.**

Paso 17. Vuelva a cargar el switch mediante el comando **reload.**

Nota: El procedimiento de recuperación de contraseña puede variar según la serie del switch de Cisco. Por lo tanto, deberá consultar la documentación pertinente al producto antes de intentar recuperaruna contraseña.

Recuperación de contraseña Enable Password

El sistema se ha interrumpido antes de inicializar el sistema de archivos flash. Los siguientes comandos inicializarán el sistema de archivos flash y finalizarán la carga del software del sistema operativo:

```
flash_init
load_helper
boot
```

2.4.2 MENSAJES DE INICIO DE SESIÓN.-

Configurar un título de inicio de sesión

El conjunto del comando IOS de Cisco incluye una característica que permite configurar los mensajes que cualquier persona puede ver cuando inicia sesión en el switch. Estos mensajes se llaman mensajes de inicio de sesión y mensajes del día (MOTD). En este tema, aprenderá a configurarlos.

El usuario puede definir un mensaje personalizado para que se muestre antes de los avisos de inicio de sesión del nombre de usuario y la contraseña utilizando el comando **banner login** en el modo de configuración global. Coloque el texto del mensaje en citas o utilizando un delimitador diferente a cualquier carácter que aparece en la cadena de MOTD.

La figura muestra el switch S1 configurándose con un mensaje de inicio de sesión **¡Personal autorizado únicamente!**

Para eliminar el mensaje MOTD, ingrese el formato **no** de este comando en el modo de configuración global, por ejemplo, S1(config)#no **banner login.**

Configurar un mensaje de inicio de sesión

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	S1#**configure terminal**
Configurar un mensaje de inicio de sesión.	S1(config)#**banner login "¡Personal autorizado únicamente!"**

Configurar un título de MOTD

El mensaje MOTD se muestra en todos los terminales conectados en el inicio de sesión y es útil para enviar mensajes que afectan a todos los usuarios de la red (como desconexiones inminentes del sistema). Si se configura, el mensaje MOTD se muestra antes que el mensaje de inicio de sesión.

Defina el mensaje MOTD utilizando el comando **banner motd** en el modo de configuración global. Coloque el texto del mensaje en citas.

La figura muestra el switch S1 configurándose con un mensaje MOTD para mostrar **¡El mantenimiento del dispositivo se realizará el viernes!**

Para eliminar el mensaje de inicio de sesión, ingrese el formato **no** de este comando en el modo de configuración global, por ejemplo, S1(config)#**no banner motd**.

Configurar un mensaje de MOTD

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	S1#**configure terminal**
Configurar un mensaje de MOTD de inicio de sesión.	S1(config)#**banner motd "¡El mantenimiento del dispositivo se realizará el viernes!"**

2.4.3 CONFIGURE TELNET Y SSH.-

Telnet y SSH

Los switches más antiguos quizás no admitan la comunicación segura con el shell seguro (SSH, Secure Shell). Este tema lo ayudará a elegir entre los métodos Telnet y SSH para comunicarse con un switch.

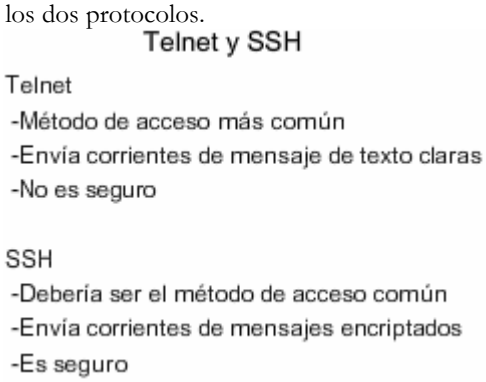
Existen dos opciones para acceder en forma remota avty en un switch de Cisco.

Telnet es el método original que los primeros modelos de switch de Cisco admitían. Telnet es un protocolo popular utilizado para acceder al terminal debido a que la mayoría de los sistemas operativos actuales vienen con un cliente Telnet incorporado. Sin embargo, Telnet es una manera insegura de acceder a un dispositivo de red, porque envía todas las comunicaciones a través de la red en un texto claro. Mediante el software de monitoreo de red, un atacante puede leer todas las teclas que se envían entre el cliente Telnet y el servicio Telnet ejecutándose en el switch de Cisco. Debido a las cuestiones de seguridad del protocolo de Telnet, SSH se ha convertido en el protocolo preferido para acceder remotamente a líneas de terminales virtuales en un dispositivo Cisco.

SSH proporciona el mismo tipo de acceso que Telnet, con el beneficio agregado de seguridad. La comunicación entre el cliente SSH y el servidor SSH está encriptada. SSH pasó por algunas versiones, con los dispositivos deCisco admitiendo

actualmente SSHv1 y SSHv2. Se recomienda que implemente SSHv2 cuando sea posible, debido a que utiliza un algoritmo de encriptación de seguridad mejor que SSHv1.

La figura presenta las diferencias entre los dos protocolos.



Configuración de Telnet

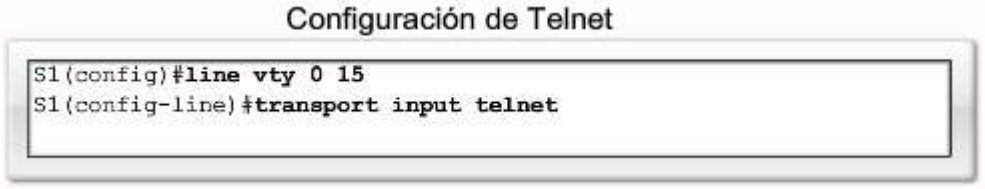
Telnet es el protocolo predeterminado que admite vty en un switch de Cisco. Cuando se asigna una dirección IP de administración al switch de Cisco, puede conectarlo utilizando el cliente Telnet. Inicialmente, las líneas vty son inseguras al permitir el acceso a cualquier usuario que intenta conectarse a ellas.

En el tema anterior, aprendió cómo asegurar el acceso al switch sobre las líneas vty solicitando una autenticación de contraseña. Esto hace que la ejecución del servicio de Telnet sea un poco más segura.

Como Telnet es el transporte predeterminado para las líneas vty, no necesita especificarlo después de que se lleve a cabo la configuración inicial del switch. Sin embargo, si ha conmutado el protocolo de transporte en las líneas vty parapermitir sólo SSH, debe habilitar el protocolo de Telnet para permitir el acceso manual de Telnet.

Si necesita volver a habilitar el protocolo de Telnet en un switch 2960 de Cisco, utilice el siguiente comando desde el modo de configuración de línea: (config-line)#**transport input telnet** o (config-line)#**transport input all**.

Al permitir todos los protocolos de transporte, todavía permite el acceso SSH al switch, como también el acceso a Telnet.



Configuración de SSH

SSH es una característica criptográfica de seguridad que está sujeta a exportar restricciones. Para utilizar esta característica se debe instalar una imagen criptográfica en su switch.

La característica SSH tiene un servidor SSH y un cliente integrado SSH, que son aplicaciones que se ejecutan en el switch. Puede utilizar cualquier cliente SSH que se ejecuta en una PC o el cliente SSH de Cisco que se ejecuta en el switch para conectar a un switch que se ejecuta en el servidor SSH.

El switch admite SSHv1 o SSHv2 para el componente de servidor. El switch admite sólo SSHv1 para el componente de cliente.

SSH admite el algoritmo Estándar de encriptación de datos (DES) , el algoritmo DES triple (3DES) y la autenticación de usuario basada en la contraseña. DES ofrece encriptación de 56 bits, y 3DES ofrece encriptación de 168 bits. La encriptación lleva tiempo, pero DES demora menos que 3DES en encriptar texto. Típicamente, los estándares de encriptación los especifica el cliente. Entonces, si tiene que configurar SSH, pregunte cuál utilizar. (El análisis de los métodos de encriptación de datos está más allá del alcance de este curso).

Para implementar SSH, debe generar claves RSA. RSA incluye una clave pública, guardada en un servidor público de RSA y una clave privada, guardada sólo por el emisor y el receptor. La clave pública la pueden conocer todos y se utiliza para encriptar mensajes. Los mensajes encriptados con la clave pública sólo se pueden descifrar utilizando la clave privada. Esto se conoce como encriptación asimétrica y se analizará con más detalle en Exploration: Acceso al curso WAN.

Debe generar las claves RSA encriptadas utilizando el comando **crypto key generate rsa**.

Necesita este proceso si está configurando el switch como un servidor SSH. Comenzando en el modo EXEC privilegiado, siga estos pasos para configurar un nombre de host y nombre de dominio IP y para generar un par de claves RSA.

Paso 1. Ingrese al modo de configuración global mediante el comando **configure terminal.**

Paso 2. Configure un nombre de host para su switch utilizando el comando **hostname** nombre de host.

Paso 3. Configure un dominio de host para su switch utilizando el comando **ip domain-name** nombre de dominio.

Paso 4. Habilite el servidor SSH para la autenticación remota y local en el switch y genere un par de claves RSA utilizando el comando **crypto key generate rsa.**

Cuando genera claves RSA, se le indica que ingrese una longitud de módulo. Cisco recomienda utilizar un tamaño de módulo de 1024 bits. Una longitud de módulo más larga puede ser más segura, pero demora más en generar y utilizar.

Paso 5. Regrese al modo EXEC privilegiado utilizando el comando **end.**

Paso 6. Muestre el estado del servidor SSH en el switch utilizando el comando **show ip ssh o show ssh.**

Para eliminar el par de claves RSA, utilice el comando crypto key zeroize rsa de configuración global. Después de eliminarse el par de claves RSA, el servidor SSH se deshabilita automáticamente.

Configuración del servidor SSH

Comenzando en el modo EXEC privilegiado, siga estos pasos para configurar el servidor SSH.

Paso 1. Ingrese al modo de configuración global mediante el comando **configure terminal.**

Paso 2. (Opcional) Configure el switch para ejecutar SSHv1 o SSHv2 utilizando el comando **ip ssh version [1 | 2].**

Si no ingresa este comando o no especifica una palabra clave, el servidor SSH selecciona la última versión admitida por el cliente SSH. Por ejemplo: si el cliente SSH admite SSHv1 y SSHv2, el servidor SSH selecciona SSHv2.

Paso 3. Configure los parámetros de control de SSH:

Especifique el valor del tiempo muerto en segundos; la opción predeterminada es 120 segundos. El intervalo es de 0 a 120 segundos Para que se conecte SSH para estar establecido, se deben completar un número de fases, como conexión, negociación de protocolo y negociación de parámetros. El valor del tiempo muerto se aplica a la cantidad de tiempo que el switch permite para que se establezca una conexión.

De manera predeterminada, están disponibles hasta cinco conexiones SSH simultáneas encriptadas para varias sesiones basadas en CLI sobre la red (sesión 0 a sesión 4). Después de que comienza la ejecución de shell, el valor del tiempo muerto de la sesión basada en CLI regresa a los 10 minutos predeterminados.

Especifique el número de veces que un cliente puede volver a autenticarse al servidor. La opción predeterminada es 3; el intervalo es de 0 a 5. Por ejemplo: un usuario puede permitir que la sesión SSH se mantenga por más de 10 minutos tres veces antes de que finalice la sesión SSH.

Repita este paso cuando configure ambos parámetros. Para configurar ambos parámetros utilice el comando **ip ssh {timeout** segundos **| authentication-retries** número**}.**

Paso 4. Regrese al modo EXEC privilegiado mediante el comando end.

Paso 5. Muestre el estado de las conexiones del servidor SSH en el switch utilizando el comando **show ip ssh o show ssh**.

Paso 6. (Opcional) Guarde sus entradas en el archivo de configuración utilizando el comando **copy running-config startup-config.**

Si quiere evitar conexiones que no sean de SSH, agregue el comando **transport input ssh** en el modo configuración en línea para limitar al switch a conexiones sólo de SSH. Las conexiones de Telnet directas (no SSH) se rechazan.

Para obtener un análisis más detallado sobre SSH, visite:
http://www.cisco.com/en/US/tech/tk583/tk617/tsd_technology_support_protocol_home.html.

Para obtener una descripción general de la tecnología de RSA, visite: http://en.wikipedia.org/wiki/Public-key_cryptography.

Para obtener un análisis más detallado sobre tecnología de RSA, visite: http://www.rsa.com/rsalabs/node.asp?id=2152.

Configuración de SSH

```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```

2.4.4 ATAQUES DE SEGURIDAD COMUNES.-

Saturación de la dirección MAC

Desafortunadamente, la seguridad de switch básica no detiene los ataques maliciosos. En este tema aprenderá acerca de unos pocos ataques de seguridad comunes y lo peligrosos que pueden ser. Este tema proporciona información de nivel introductorio acerca de los ataques de seguridad. Los detalles sobre la forma en que funcionan estos ataques comunes exceden el alcance de este curso. Si le interesa la seguridad de red, investigue el curso CCNA Exploration: acceso a la WAN.

Saturación de la dirección MAC

La flooding de direcciones MAC es un ataque común. Recuerde que la tabla de direcciones MAC del switch contiene las direcciones MAC disponibles de un puerto físico determinado de un switch y los parámetros asociados para cada uno. Cuando un switch de la Capa 2 recibe una trama, el switch busca en la tabla de direcciones MAC la dirección MAC de destino. Todos los modelos de switches Catalyst utilizan una tabla de direcciones MAC para la conmutación en la Capa 2. A medida que las tramas llegan a los puertos del switch, las direcciones MAC de origen se aprenden y se registran en la tabla de direcciones MAC. Si existe una entrada para la dirección MAC, el switch envía la trama al puerto designado con esa dirección MAC en la tabla de direcciones MAC. Si la dirección MAC no existe, el switch actúa como un hub y envía la trama a todos los puertos del switch. Los ataques de sobrecarga de la tabla de direcciones MAC son también conocidos como ataques de flooding de MAC. Para comprender el mecanismo de un ataque de sobrecarga de la tabla de direcciones MAC, recuerde el funcionamiento básico del switch.

Haga clic en el botón Paso 1 de la figura para ver la forma en que comienza el ataque de sobrecarga de la tabla de direcciones MAC.

En la figura, el host A envía tráfico al host B. El switch recibe las tramas y busca la dirección MAC de destino en su tabla de direcciones MAC. Si el switch no encuentra la MAC de destino en la tabla de direcciones MAC, entonces copia la trama y la envía por broadcast a todos los puertos del switch.

Haga clic en el botón Paso 2 de la figura para ver el paso siguiente.

El host B recibe la trama y envía una respuesta al host A. El switch aprende entonces que la dirección MAC para el host B se encuentra en el puerto 2 y escribe esta información en la tabla de direcciones MAC.

El host C también recibe la trama que va del host A al host B, pero debido a que la dirección MAC de destino de la trama es el host B, el host C la descarta.

Haga clic en el botón Paso 3 de la figura para ver el paso siguiente.

Ahora, cualquier trama enviada por el host A (o por cualquier otro host) al host B se envía al puerto 2 del switch y no a todos los demás puertos.

La clave para entender cómo funcionan los ataques de sobrecarga de la tabla de direcciones MAC es saber que estas tablas poseen un límite de tamaño. Las flooding de MAC utilizan esta limitación para bombardear al switch con direcciones MAC falsas hasta que la tabla de direcciones MAC del switch esté llena. Luego el switch ingresa a lo que se conoce como modo de falla de apertura, comienza a actuar como un hub y envía paquetes de broadcast a todas las máquinas de la red. En consecuencia, el atacante puede ver todas las tramas enviadas por el host víctima a otro host que no posee una entrada en la tabla de direcciones MAC.

Haga clic en el botón Paso 4 de la figura para ver la forma en que un atacante utiliza herramientas legítimas de manera maliciosa.

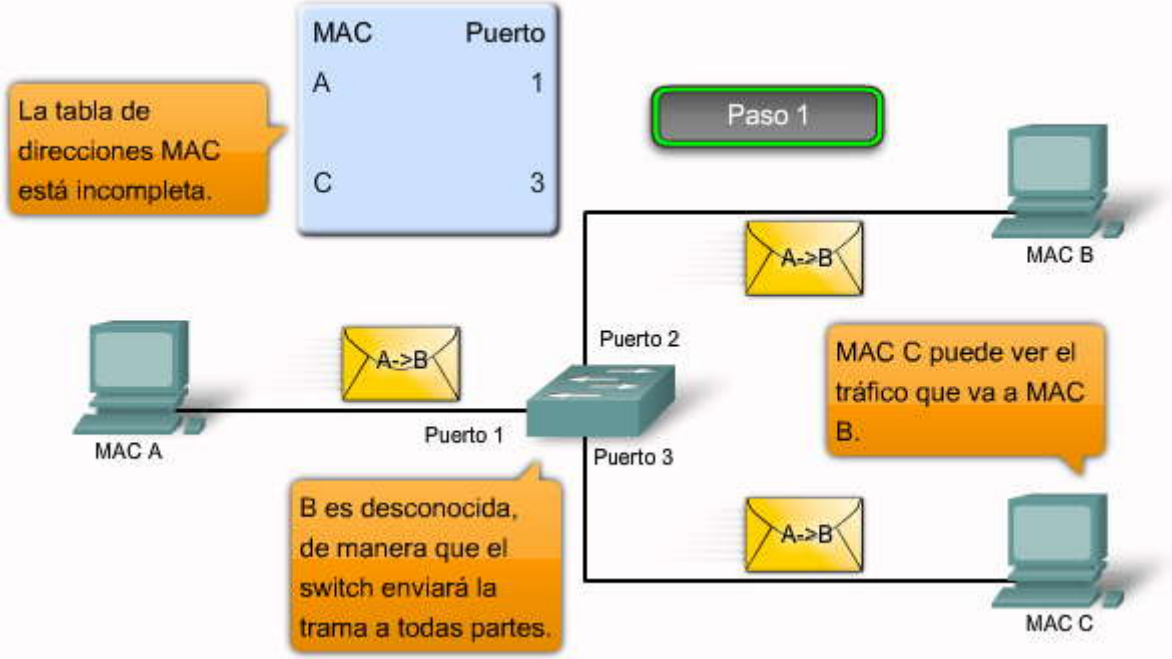
La figura muestra la forma en que un atacante puede utilizar las características de funcionamiento normales del switch para que deje de funcionar.

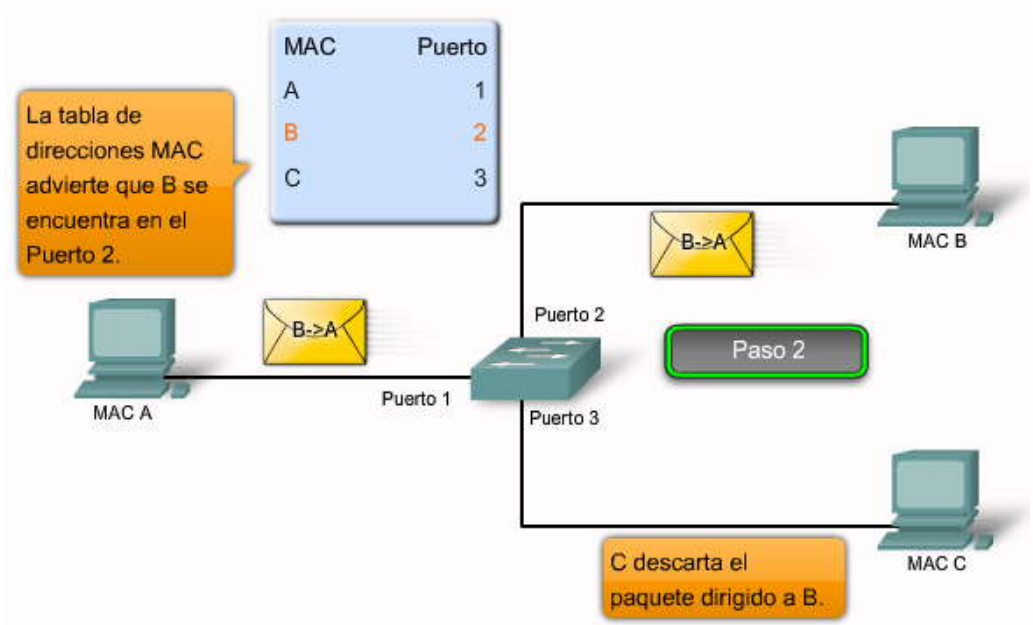
Las flooding de MAC pueden llevarse a cabo mediante una herramienta de ataque de red. El intruso de la red utiliza la herramienta de ataque para inundar el switch con una gran cantidad de direcciones MAC de origen no válidas hasta que se llene la tabla de direcciones MAC. Cuando la tabla de direcciones MAC está llena, el switch satura todos los puertos con tráfico de entrada, ya que no puede encontrar el número de puerto para una dirección MAC en particular en la tabla de direcciones MAC. En esencia, el switch actúa como un hub.

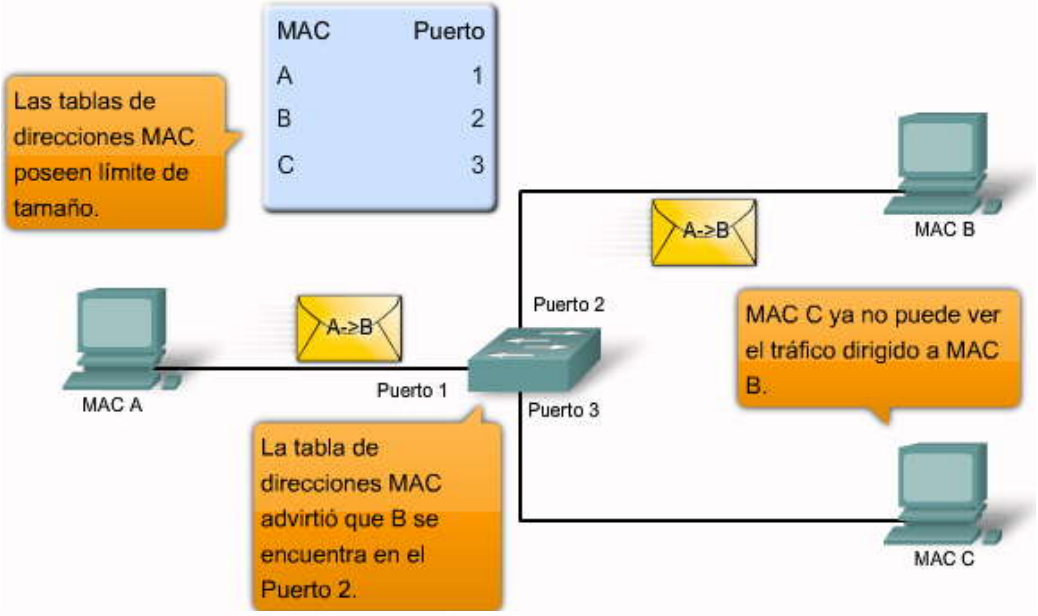
Algunas herramientas de ataque de red pueden generar 155 000 entradas de MAC en un switch por minuto. El tamaño máximo de la tabla de direcciones MAC varía en función del switch. En la figura, la herramienta de ataque se ejecuta en el host con dirección MAC C en la parte inferior derecha de la pantalla. Esta herramienta satura el switch con paquetes que contienen direcciones MAC e IP de origen y destino generadas de manera aleatoria. Después de un corto período de tiempo, la tabla de direcciones MAC del switch se llena hasta que no puede aceptar entradas nuevas. Cuando la tabla de direcciones MAC se llena con direcciones MAC de origen no válidas, el switch comienza a enviar todas las tramas que recibe a todos los puertos.

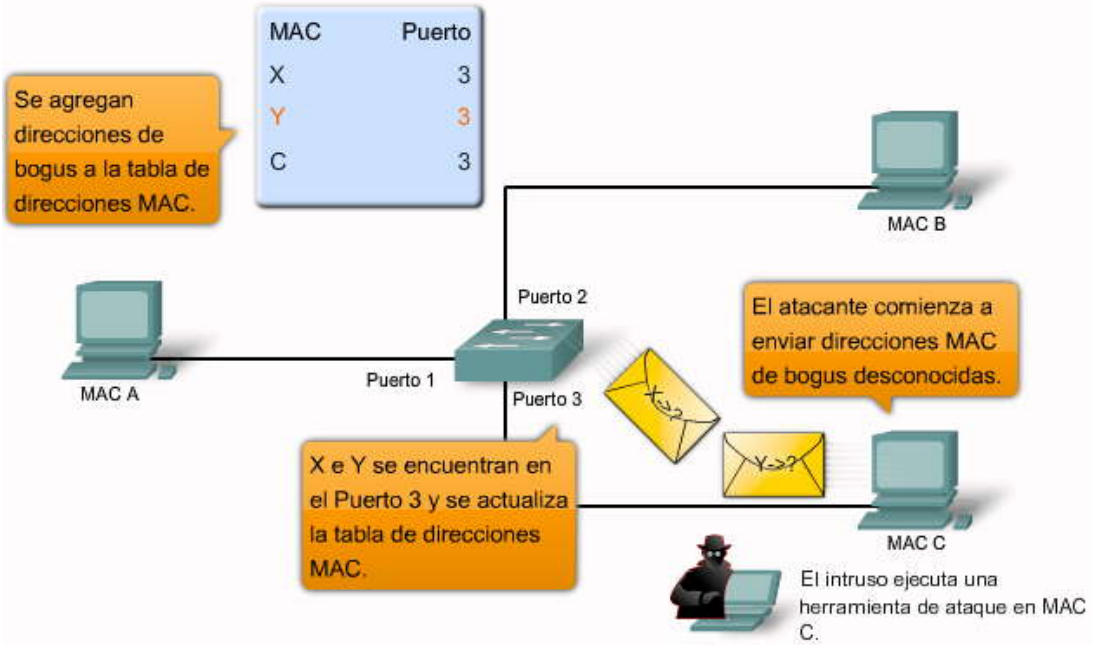
Haga clic en el botón Paso 5 de la figura para ver el paso siguiente.

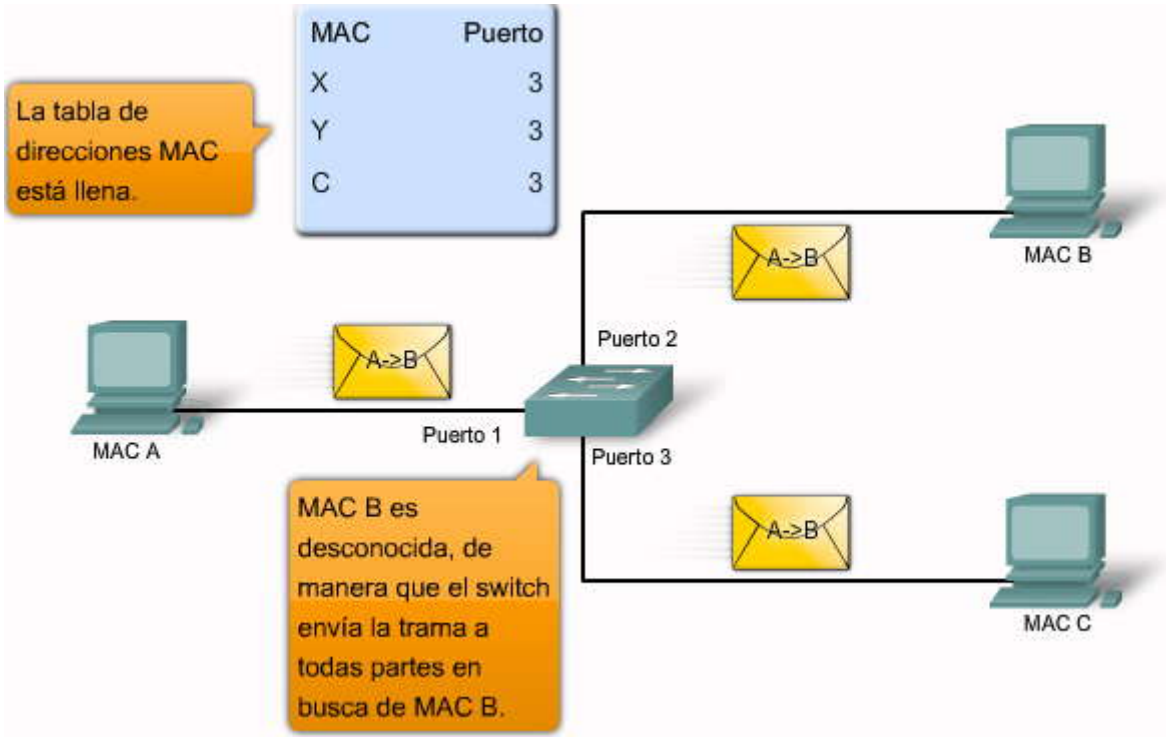
Mientras la herramienta de ataque de red continúe ejecutándose, la tabla de direcciones MAC del switch permanecerá llena. Cuando esto sucede, el switch comienza a enviar broadcast de todas las tramas recibidas a todos los puertos, de manera que las tramas enviadas del host A al host B también se envían por broadcast al puerto 3 del switch.




MAC Puerto
A 1
B 2
C 3
La tabla de direcciones MAC advierte que B se encuentra en el Puerto 2.
B->A
MAC B
B->A
Puerto 2
Paso 2
MAC A
Puerto 1
Puerto 3
MAC C
C descarta el paquete dirigido a B.


MAC Puerto
A 1
B 2
C 3
Las tablas de direcciones MAC poseen límite de tamaño.
A->B
MAC B
A->B
Puerto 2
MAC C ya no puede ver el tráfico dirigido a MAC B.
MAC A
Puerto 1
Puerto 3
La tabla de direcciones MAC advirtió que B se encuentra en el Puerto 2.
MAC C


MAC Puerto
X 3
Y 3
C 3
Se agregan direcciones de bogus a la tabla de direcciones MAC.
MAC B
Puerto 2
El atacante comienza a enviar direcciones MAC de bogus desconocidas.
MAC A
Puerto 1
Puerto 3
X->?
Y->?
X e Y se encuentran en el Puerto 3 y se actualiza la tabla de direcciones MAC.
MAC C
El intruso ejecuta una herramienta de ataque en MAC C.



Ataques de suplantación de identidad

Haga clic en el botón Suplantación de identidad que se muestra en la figura.

Una de las formas en que un atacante puede acceder al tráfico de la red es haciendo spoofsobre las respuestas enviadas por un servidor de DHCP válido. El dispositivo DHCP víctima de suplantación de identidad responde a las solicitudes de clientes de DHCP. El servidor legítimo también puede responder, pero si el dispositivo de suplantación deidentidad está en el mismo segmento que el cliente, la respuesta de este último llegará primero. La respuesta del DHCP intruso ofrece una dirección IP e información de soporte que designa al intruso como la gateway predeterminada o como servidor de Sistema de nombres de dominios (DNS). En el caso de una gateway, los clientes envían paquetes al dispositivo atacante, el cual, en respuesta, los envía al destino deseado. Esto se conoce como ataque de intermediario y puede pasar totalmente desapercibido a medida que el intruso intercepta el flujo de datos de la red.

Debe estar atento a otro tipo de ataque de DHCP denominado ataque de inanición de DHCP. La PC atacante solicita direcciones IP de manera continua a un servidor de DHCP real cambiando sus direcciones MAC de origen. Si da resultado, este tipo de ataque de DHCP produce que todos los arrendamientos del servidor de DHCP real queden asignados, lo que provoca que los usuarios reales (clientes de DHCP) no puedan obtener una dirección IP.

Para evitar los ataques de DHCP, se utiliza el snooping DHCP y las funciones de seguridad de puerto de los switches Catalyst de Cisco.

Snooping DHCP y funciones de seguridad de puerto de los switches Catalyst de Cisco

El snooping DHCP es una función que determina cuáles sonlos puertos de switch que pueden responder a solicitudes de DHCP. Los puertos se identifican como confiables o no confiables. Los puertos confiables pueden recibir todos los mensajes de DHCP, los no confiables sólo pueden recibir solicitudes. Los puertosconfiables de los hosts se alojan en el servidor de DHCP o pueden ser un enlace hacia dicho servidor. Si un dispositivo malicioso de un puerto no confiable intenta enviar un paquete de respuesta de DHCP a la red, el puerto se desactiva. Esta función puedeunirse con las opciones de DHCP donde la información del switch, como el ID de puerto o la solicitud de DHCP pueden insertarse en el paquete de solicitudes de DHCP.

Haga clic en el botón Snooping de DHCP.

Los puertos no confiables son aquellos que no están explícitamente configurados como confiables. Se construye una tabla enlazada de DHCP para los puertos no confiables. Cada entrada contiene una dirección MAC cliente, una dirección IP, un tiempo de arrendamiento, un número de VLAN y una ID de puerto registrados como clientes que realizan solicitudes de DHCP. Se utiliza entonces la tabla para filtrar el tráfico de DHCP subsiguiente. Desde la perspectiva del snooping en DHCP, los puertos de acceso no confiables no deben enviar ninguna respuesta a servidoresDHCP.

Estos pasos ilustran la forma en que se configura el snooping de DHCP en un switch de Cisco:

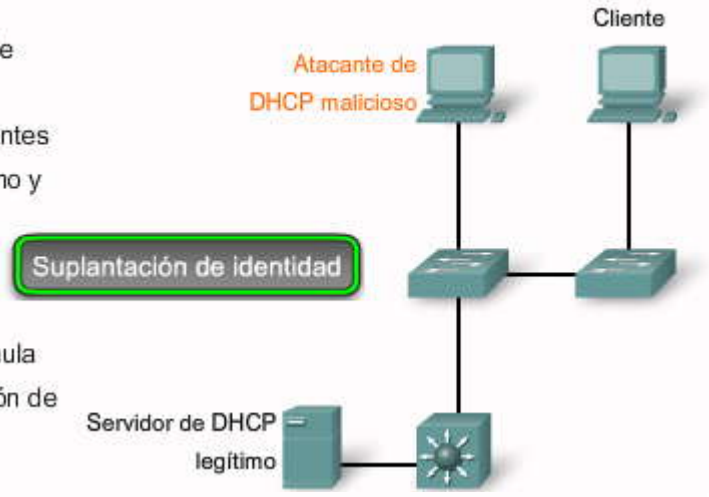
Paso 1. Habilitar el snooping de DHCP mediante el comando de configuración global **ip dhcp snooping**.

Paso 2. Habilitar el snooping de DHCP para VLAN específicas mediante el comando **ip dhcp snooping vlan number** [número].

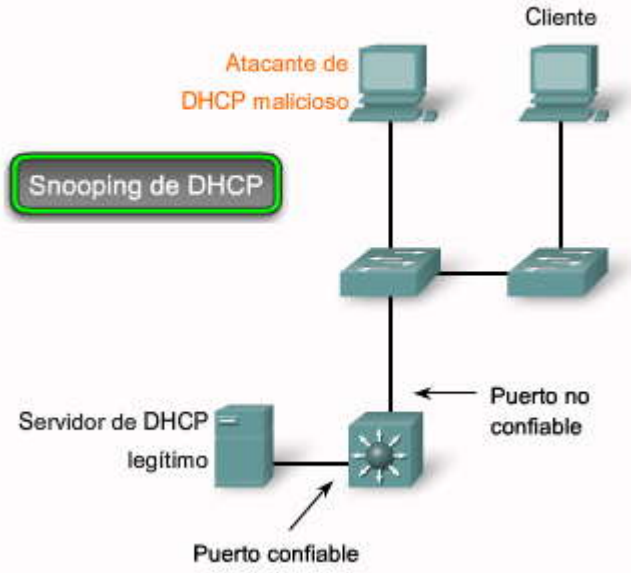
Paso 3. Definir los puertos como confiables o no confiables a nivel de interfaz identificando los puertos confiables mediante el comando **ip dhcp snooping trust.**

Paso 4. (Opcional) Limitar la tasa a la que un atacante puede enviar solicitudes de DHCP bogus de manera continua a través de puertos no confiables al servidor de DHCP mediante el comando **ip dhcp snooping limit rate rate.**

1) Un atacante activa un servidor de DHCP en un segmento de red.
2) El cliente envía un broadcast de solicitud de información de configuración de DHCP.
3) El servidor de DHCP malicioso responde antes de que lo haga el servidor de DHCP legítimo y asigna información de configuración de IP definida por el atacante.
4) Los paquetes de host son redirigidos a la dirección del atacante, ya que el mismo emula un gateway predeterminado para la dirección de DHCP errónea provista al cliente.



- El snooping de DHCP permite saber si la configuración de los puertos es confiable o no.
  - Los puertos confiables pueden enviar solicitudes de DHCP y acuses de recibo.
  - Los puertos no confiables sólo pueden enviar solicitudes de DHCP.
- El snooping de DHCP permite que el switch construya una tabla enlazada que asigna una dirección MAC de cliente, dirección IP, VLAN e ID de puerto.
- Utilice el comando `ip dhcp snooping`.



Ataques en CDP

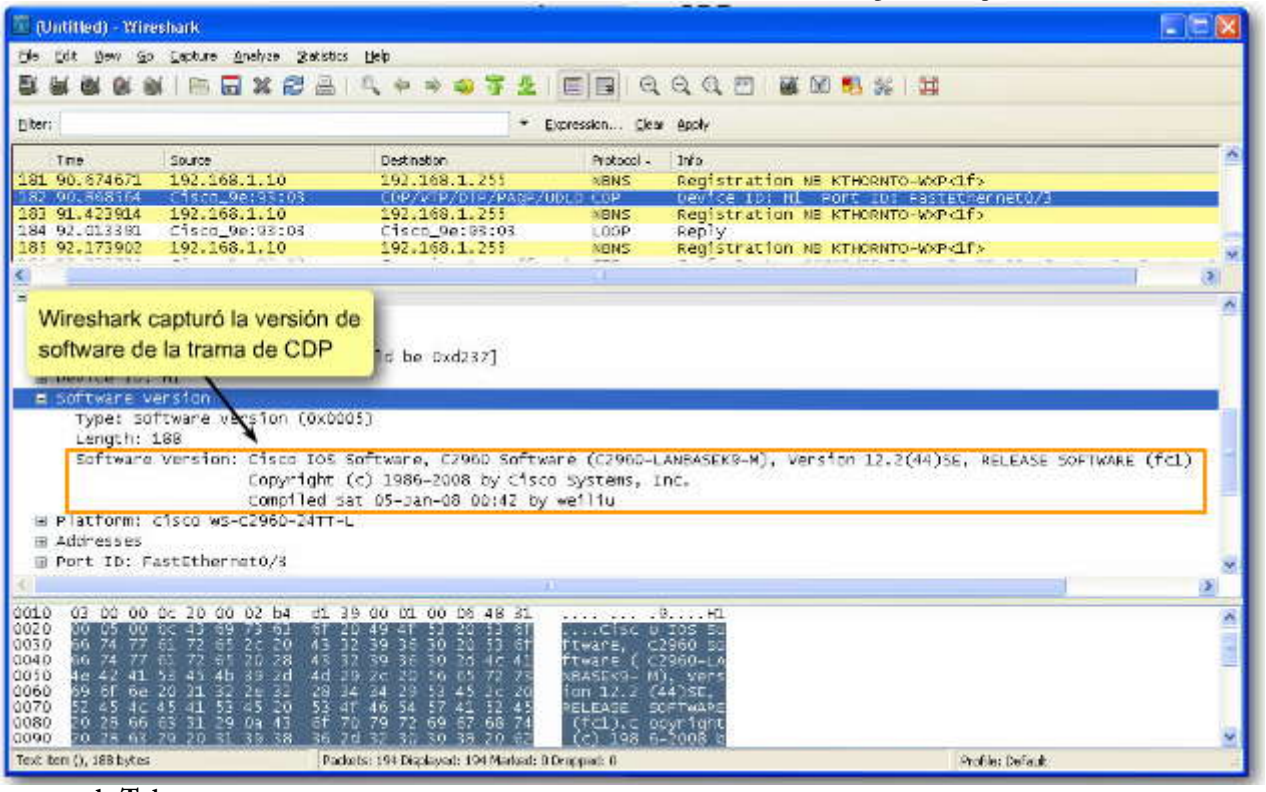
El Protocolo de descubrimiento de Cisco (CDP) es un protocolo de propiedad de Cisco que puede configurarse en todos los dispositivos de Cisco. CDP descubre otros dispositivos de Cisco conectados directamente, lo que permite que configuren sus conexiones en forma automática, simplificando la configuración y la conectividad. Los mensajes de CDP no están encriptados.

De manera predeterminada, la mayoría de los routers y switches de Cisco poseen CDP habilitado. La información de CDP se envía en broadcasts periódicos que se actualizan de manera local en cada base de datos de CDP de todos los dispositivos. Debido a que CDP es un protocolo de la Capa 2, no se propaga por los routers.

CDP contiene información sobre el dispositivo, como la dirección IP, la versión del software, la plataforma, las capacidades y la VLAN nativa. Cuando esta información está disponible para el atacante, puede utilizarla para encontrar vulnerabilidades para atacar la red, en general en la forma de ataque de Denegación de servicio (DoS).

La figura representa una parte de un rastreo de paquete de Ethereal que muestra el interior de un paquete CDP. En particular, la versión de software IOS de Cisco descubierta por CDP permitirá que el atacante investigue y determine si existen vulnerabilidades de seguridad específicas para esa versión del código en particular. Además, debido a que CDP no está autenticado, un atacante puede generar paquetes de CDP bogus y hacer que éstos se reciban en el dispositivo Cisco conectado en forma directa.

Para enfrentar esta vulnerabilidad se recomienda deshabilitar el uso de CDP en los dispositivos que no necesitan utilizarlo.



Ataques de Telnet

Un atacante puede utilizar el protocolo de Telnet para acceder de manera remota a un switch de red de Cisco. En temas anteriores se configuró una contraseña de inicio de sesión para las líneas vty y se establecieron dichas líneas para que soliciten autenticación por contraseña para el acceso. Esto proporciona un nivel de seguridad esencial y básico que ayuda a proteger el switch del acceso no autorizado. Sin embargo, no es un método seguro para proteger el acceso a las líneas vty. Existen herramientas disponibles que permiten que un atacante inicie un ataque de decodificación de contraseñas de fuerza bruta contra las líneas vty del switch.

Ataque de contraseña de fuerza bruta

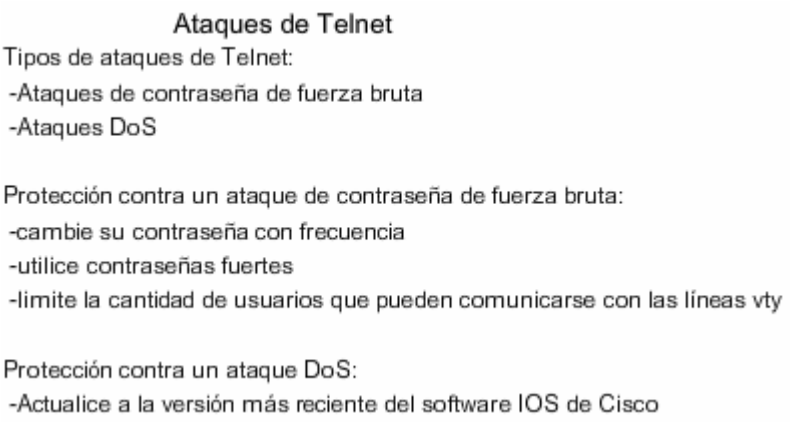
La primer fase de un ataque de contraseña de fuerza bruta comienza con el uso de contraseñas comunes por parte del atacante y de un programa diseñado para intentar establecer una sesión de Telnet mediante todas las palabras del diccionario. Por suerte, el usuario es lo suficientemente listo como para no utilizar una palabra del diccionario, de modo que, por el momento, se encuentra a salvo. En la segunda fase del ataque de fuerza bruta, el atacante utiliza un programa que genera combinaciones de caracteres secuenciales para poder "adivinar" la contraseña. Si dispone del tiempo suficiente, un ataque de contraseña de fuerza bruta puede decodificar casi todas las contraseñas utilizadas.

La acción más simple que puede llevarse a cabo para limitar la vulnerabilidad a los ataques de contraseña de fuerza bruta es cambiar la contraseña con frecuencia y utilizar contraseñas fuertes, que combinen letras en mayúscula y minúscula con números. Configuraciones más avanzadas permiten limitar las comunicaciones con las líneas vty mediante listas de acceso, pero eso excede el alcance de este curso.

Ataque DoS

Otro tipo de ataque de Telnet es el ataque de DoS. En un ataque de DoS, el atacante explota un desperfecto del software del servidor de Telnet que se ejecuta en el switch que torna al servicio de Telnet no disponible. Este tipo de ataque es en la mayoría de los casos una molestia, ya que evita que el administrador lleve a cabo las funciones de administración del switch.

En general, las vulnerabilidades en el servicio de Telnet que permiten que ocurran los ataques de DoS se enfrentan mediante parches de seguridad incluidos en las revisiones más recientes de IOS de Cisco. Si se experimenta un ataque de DoS contra el servicio de Telnet, o contra algún otro servicio de un dispositivo Cisco, verifique si existe una revisión reciente de IOS de Cisco disponible.



2.4.5 HERRAMIENTAS DE SEGURIDAD.-

Después de configurar la seguridad del switch, se debe verificar que no hayan quedado debilidades que puedan ser explotadas por un atacante. La seguridad de red es un tema complejo y cambiante. En esta sección se presenta la forma en que las herramientas de seguridad de red forman un componente utilizado para proteger una red de ataques maliciosos.

Las herramientas de seguridad de red ayudan a probar la red en busca de distintas debilidades. Son herramientas que permiten que el usuario actúe como pirata informático y como analista de seguridad de red. A través de estas herramientas se puede iniciar un ataque y llevar a cabo la auditoría de los resultados para determinar la forma de ajustar las políticas de seguridad para evitar un ataque determinado.

Las funciones que utilizan las herramientas de seguridad de red evolucionan de manera constante. Por ejemplo: hubo un tiempo en que las herramientas de seguridad de red se enfocaron sólo en los servicios de la red y examinaban los posibles defectos de dichos servicios. Actualmente, los virus y gusanos pueden propagarse debido a los defectos en los clientes de correo y en los exploradores Web. Las herramientas de seguridad de red modernas no sólo detectan los defectos remotos de los hosts de la red, sino que también determinan si existen defectos a nivel de aplicación, como parches faltantes en computadoras de clientes. La seguridad de red no sólo involucra a los dispositivos de red, sino también a los equipos de escritorios de los clientes. Las auditorías de seguridad y los pruebas de penetración son dos funciones básicas que llevan a cabo las herramientas de seguridad de red.

Auditoría de seguridad de red

Las herramientas de seguridad de red permiten realizar una auditoría de la red. Una auditoría de seguridad revela el tipo de información que un atacante puede recopilar con un simple monitoreo del tráfico de la red. Las herramientas de auditoría de seguridad de red permiten inundar la tabla MAC con direcciones MAC de bogus. Luego se puede realizar la auditoría en los puertos de switch a medida que el switch envía el tráfico a todos los puertos y las asignaciones de direcciones MAC legítimas expiran y son reemplazadas por asignaciones de direcciones MAC de bogus. De esta manera, se pueden determinar los puertos comprometidos y que no han sido configurados de manera correcta para evitar este tipo de ataque.

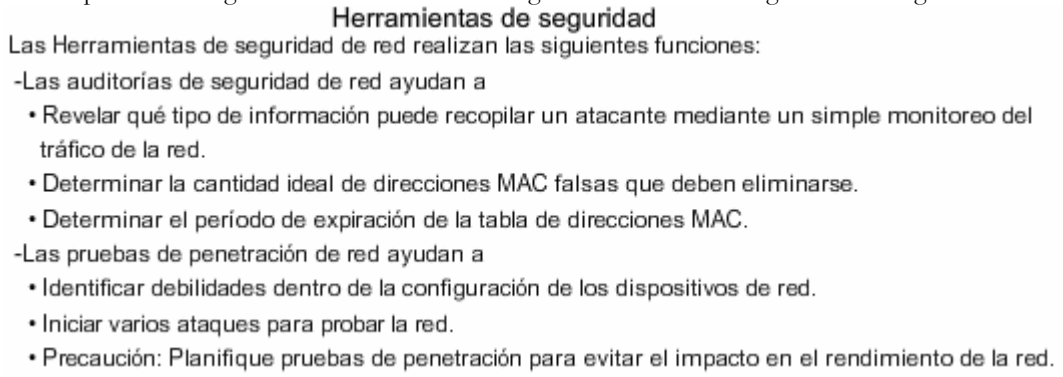
El tiempo es un factor importante para realizar la auditoría en forma correcta. Los diferentes switches admiten distintas cantidades de direcciones MAC en sus tablas MAC. Puede ser dificultoso determinar la cantidad ideal de direcciones MAC suplantadas para ser utilizadas en la red. También se debe lidiar con el período de expiración de la tabla MAC. Si las direcciones MAC suplantadas comienzan a expirar en el momento en que se realiza la auditoría de red, las direcciones MAC válidas comienzan a llenar la tabla MAC, lo que limita la cantidad de datos que pueden monitorearse con una herramienta de auditoría de red.

Pruebas de penetración de red

Las herramientas de seguridad de red también pueden utilizarse para pruebas de penetración en la red. Esto permite identificar las debilidades dentro de la configuración de los dispositivos de red. Se puede llevar a cabo una gran cantidad de

ataques y la mayoría de los conjuntos de herramientas son acompañados por documentación completa que detalla la sintaxis necesaria para ejecutar el ataque deseado. Debido a que este tipo de pruebas puede tener efectos adversos en la red, se llevan a cabo bajo condiciones muy controladas, respetando procedimientos documentados detallados en una política de seguridad de red completa. Por supuesto, si posee una pequeña red para salón de clases, puede trabajar con su instructor para ejecutar sus propias pruebas de penetración de red.

En el tema siguiente aprenderá la forma de implementar la seguridad de puerto en los switches de Cisco de manera de asegurar que estas pruebas de seguridad de red no revelen ningún defecto en la configuración de seguridad.



Características de las herramientas de seguridad de red

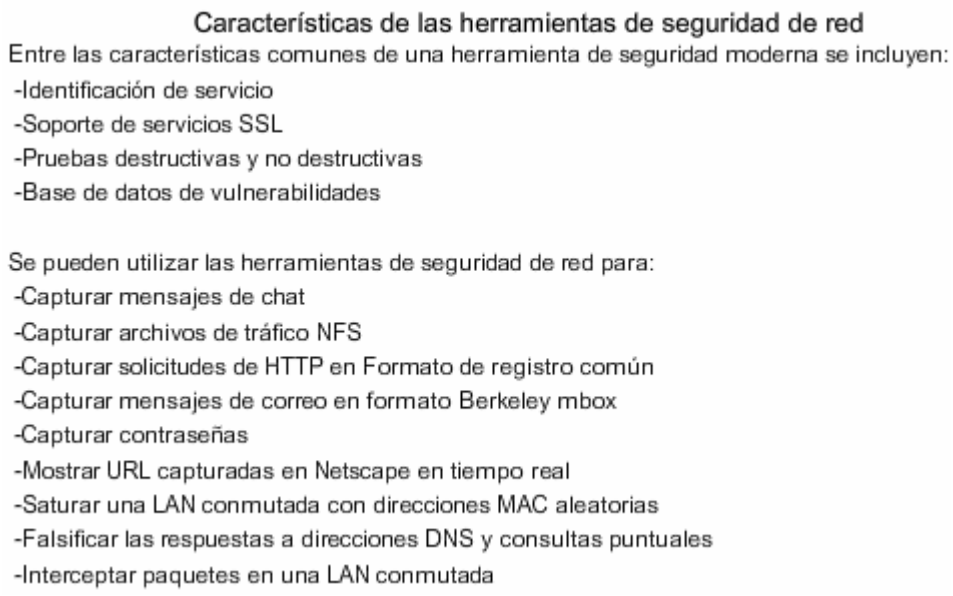
En realidad, la seguridad de red es un proceso, no un producto. No alcanza con habilitar el switch con una configuración segura y dar por terminado el trabajo. Para afirmar que una red es segura se debe contar con un plan de seguridad de red completo que defina la forma de verificar de manera periódica si la red puede enfrentar los más recientes ataques de red maliciosos. El panorama cambiante de los riesgos de seguridad implica que se debe contar con herramientas de auditoría y penetración que puedan actualizarse para enfrentar los riesgos de seguridad más recientes. Entre las características comunes de una moderna herramienta de seguridad de red, se incluyen:

- Identificación de servicio: Las herramientas se utilizan para alcanzar los hosts mediante números de puertos de la Autoridad de números asignada por Internet (IANA). Estas herramientas también deben descubrir un servidor FTP ejecutándose en un puerto no estándar o un servidor Web ejecutándose en el puerto 8080. La herramienta también debe probar todos los servicios que se ejecutan en el host.
- Soporte para servicios SSL: Pruebas de servicios que utilizan seguridad a nivel SSL, incluyendo HTTPS, SMTP, IMAP y certificado de seguridad.
- Pruebas destructivas y no destructivas: Realización de auditorías de seguridad no destructivas de rutina que no comprometan o que comprometan en forma moderada el rendimiento de la red. Las herramientas también deben permitir las auditorías destructivas que degradan en forma significativa el rendimiento de la red. Las auditorías destructivas permiten ver cómo enfrenta la red los ataques de intrusos.
- Base de datos de vulnerabilidades: Las vulnerabilidades cambian todo el tiempo.

Las herramientas de seguridad de red deben diseñarse para conectarse a un módulo de código y luego ejecutar una prueba para la vulnerabilidad. De esta manera, se puede mantener una gran base de datos de vulnerabilidades que puede subirse a la herramienta para asegurar que se están probando las vulnerabilidades más recientes.

Se pueden utilizar las herramientas de seguridad de red para:

- Capturar mensajes de chat
- Capturar archivos de tráfico de NFS
- Capturar solicitudes de HTTP en Formato de registro común
- Capturar mensajes de correo en formato Berkeley mbox
- Capturar contraseñas
- Mostrar URL capturadas del explorador en tiempo real
- Saturar una LAN conmutada con direcciones MAC aleatorias
- Falsificar las respuestas a direcciones DNS y consultas puntuales
- Interceptar paquetes en una LAN conmutada



2.4.6 CONFIGURACION DE LA SEGURIDAD DEL PUERTO.-

Uso de seguridad de puerto para mitigar ataques

En este tema, aprenderá acerca de los factores a considerar cuando se configura la seguridad de puerto en un switch. Se resumen los comandos de IOS de Cisco fundamentales de seguridad de puerto. También aprenderá acerca de la configuración de seguridad de puerto estática y dinámica.

Haga clic en el botón Seguridad de puerto en la figura.

Seguridad del puerto

Un switch que no cuenta con seguridad de puerto permite que un atacante conecte el sistema a un puerto habilitado en desuso, que recopile información o que genere ataques. Un switch puede configurarsepara actuar como un hub, lo que significa que todos los sistemas conectados al switch pueden ver de manera potencial todo el tráfico de la red que pasa a través de él y llega a todos los sistemas conectados a él. Además, un atacante puede recopilar tráfico que contiene nombres de usuario, contraseñas o información de configuración acerca de los sistemas de la red.

Todos los puertos e interfaces del switch deben asegurarse antes de implementarlo. La seguridad de puerto limita la cantidad de direcciones MAC válidas permitidas en el puerto. Cuando se asignan direcciones MAC seguras a un puerto seguro, el puerto no envía paquetes con direcciones origen que se encuentren fuera del grupo de direcciones definidas.

Si se limita la cantidad de direcciones MAC seguras a uno y se asigna una única dirección MAC segura a ese puerto, la estación de trabajo conectada a ese puerto cuenta con todo el ancho de banda de ese puerto y sólo esa estación de trabajo con esa dirección MAC segura en particular puede conectarse de manera adecuada a dicho puerto.

Si se configura un puerto como seguro y se alcanza la cantidad máxima de direcciones MAC seguras, la violación de seguridad se produce cuando la dirección MAC de una estación de trabajo que intenta acceder al puerto es distinta de cualquiera de las direcciones MAC seguras identificadas. La figura resume estos puntos.

Haga clic en el botón Tipos de direcciones MAC seguras en la figura.

Tipos de direcciones MAC seguras

Existen varias formas de configurar la seguridad de puerto. A continuación, se describen las formas de configurar la seguridad de puerto en un switch de Cisco:

- **Direcciones MAC seguras estáticas:** Las direcciones MAC se configuran manualmente mediante el comando de configuración de interfaz **switchport port-security mac-addressmac-address**. Las direcciones MAC configuradas de esta forma se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución del switch.
- **Direcciones MAC seguras dinámicas:** Las direcciones MAC se aprenden de manera dinámica y se almacenan sólo en la tabla de direcciones. Las direcciones MAC configuradas de esta manera se eliminan cuando el switch se reinicia.

- **Direcciones MAC seguras sin modificación:** Se puede configurar un puerto para que aprenda de manera dinámica las direcciones MAC y luego guardarlas en la configuración en ejecución.

Direcciones MAC sin modificación

Las direcciones MAC seguras sin modificación poseen las siguientes características:

- Cuando se habilita el aprendizaje sin modificación en una interfaz mediante el comando de configuración de interfaz **switchport port-security mac-address sticky**, la interfaz convierte todas las direcciones MAC seguras dinámicas, incluyendo aquellas que se aprendieron de manera dinámica antes de habilitar el aprendizaje sin modificación, en direcciones MAC seguras sin modificación y agrega todas estas últimas a la configuración en ejecución.
- Si se deshabilita el aprendizaje sin modificación mediante el comando de configuración de interfaz **no switchport port-security mac-address sticky,** las direcciones MAC seguras sin modificación permanecen como parte de la tabla de direcciones, pero se eliminan de la configuración activa.
- Cuando se configuran direcciones MAC seguras sin modificación mediante el comando de configuración de interfaz **switchport port-security mac-address sticky mac-address**, éstas se agregan a la tabla de direcciones y a la configuración en ejecución. Si se deshabilita la seguridad de puerto, las direcciones MAC seguras sin modificación permanecen en la configuración en ejecución.
- Si se guardan las direcciones MAC seguras sin modificación en el archivo de configuración, cuando se reinicia el switch o cuando se cierra la interfaz, esta última no necesita volver a aprender estas direcciones. Si no se guardan las direcciones seguras sin modificación, éstas se pierden.
- Si se deshabilita el aprendizaje sin modificación y se ingresa el comando de configuración de interfaz **switchport port-security mac-address sticky mac-address,** aparece un mensaje de error y la dirección MAC segura sin modificación no se agrega a la configuración en ejecución.

Haga clic en el botón Modos de violación de seguridad en la figura.

Modos de violación de seguridad

Se considera violación de seguridad si se produce alguna de las siguientes situaciones:

Se agregó a la tabla de direcciones la cantidad máxima de direcciones MAC seguras y una estación cuya dirección MAC no se encuentra en la tabla de direcciones intenta acceder a la interfaz.
Una dirección aprendida o configurada en una interfaz segura puede verse en otra interfaz segura de la misma VLAN.

Se puede configurar la interfaz para uno de tres modos de violación, en base a la acción a tomar en caso de que se produzca dicha violación. La figura muestra los tipos de tráficos de datos que se envían cuando se configura en el puerto uno de los siguientes modos de violación de seguridad.

protección: Cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitida. El usuario no advierte que se ha producido una violación de seguridad.
restricción: Cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitida. En este modo, el usuario advierte que se ha producido una violación de seguridad. De manera específica, se envía una trampa de SNMP, se registra un mensaje de syslog y se aumenta el contador de violaciones.
desactivación: En este modo, una violación de seguridad de puerto produce que la interfaz de deshabilite por error de manera inmediata y se apaga el LED del puerto. También se envía una trampa de SNMP, se registra un mensaje de syslog y se incrementa el contador de violaciones. Cuando un puerto seguro se encuentra en estado deshabilitado por error, se lo puede sacar de dicho estado mediante los comandos de configuración de interfaz **shutdown** y **no shutdown.** Éste es el modo predeterminado.

Configuración de la seguridad del puerto

Se implementa seguridad en todos los puertos de switch para:

- Especificar un grupo de direcciones MAC válidas permitidas en el puerto
- Permitir que sólo una dirección MAC acceda al puerto
- Especificar que el puerto se desactiva de manera automática si se detectan direcciones MAC no autorizadas.

Seguridad del puerto

Configuración de la seguridad del puerto

Los siguientes son los tipos de direcciones MAC seguras:

- Direcciones MAC seguras estáticas
- Direcciones MAC seguras dinámicas
- Direcciones MAC seguras sin modificación

Tipos de direcciones MAC seguras

Las direcciones MAC seguras sin modificación poseen las siguientes características:

- Se aprenden de manera dinámica y se convierten a direcciones MAC sin modificación almacenadas en la configuración de ejecución.
- Si se deshabilitan las direcciones MAC sin modificación, las mismas se eliminan de la tabla MAC, pero no de la configuración en ejecución.
- Las direcciones MAC seguras sin modificación se pierden cuando el switch se reinicia.
- Si se guardan las direcciones MAC seguras sin modificación en el archivo de configuración de inicio se pueden preservar para el momento de arranque del switch.
- Si se deshabilita el aprendizaje sin modificación, las direcciones MAC sin modificación se convierten en direcciones seguras dinámicas y se eliminan de la configuración en ejecución.

Configuración de la seguridad del puerto

Las violaciones a la seguridad se producen en estas situaciones:

- Una estación cuya dirección MAC no se encuentra en la tabla de direcciones intenta acceder a la interfaz cuando la tabla está llena.
- Se está utilizando una dirección en dos interfaces seguras de la misma LAN.

Entre los modos de violación de seguridad se incluyen: protección, restricción y desactivación.

Modo de violación	Envía tráfico	Envía un mensaje de Syslog	Muestra un mensaje de error	Aumenta el contador de violaciones	Cierra el puerto
Restricción	No	No	No	No	No
Protección	No	Sí	No	Sí	No
Desactivación	No	Sí	No	Sí	Sí

Modos de violación de seguridad

Configurar la seguridad del puerto

Haga clic en el botón Configuración predeterminada de la figura.

Los puertos de un switch de Cisco están preconfigurados de manera predeterminada. La figura resume la configuración de seguridad de puerto predeterminada.

Haga clic en el botón Configurar la seguridad de puerto dinámica en la figura.

La figura muestra los comandos de CLI IOS de Cisco necesarios para configurar la seguridad de puerto en un puerto Fast Ethernet F0/18 en el switch S1. Observe que el ejemplo no especifica un modo de violación. En este ejemplo, d modo de violación se establece en **desactivación**.

Haga clic en el botón Configurar la seguridad de puerto sin modificación en la figura.

La figura muestra la forma de habilitar la seguridad de puerto sin modificación en el puerto Fast Ethernet 0/18 del switch S1. Como se mencionó con anterioridad, se puede configurar la cantidad máxima de direcciones MAC seguras. En este ejemplo, se puede ver la sintaxis del comando IOS de Cisco utilizada para establecer la cantidad máxima de direcciones MAC en 50. El modo de violación se establece en **desactivación** predeterminada.

Existen otros parámetros de seguridad de puerto que pueden ser de utilidad. Para obtener una lista completa de las opciones de configuración de la seguridad del puerto, visite: http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_44_se/configuration/guide/swtrafc.html

Opciones predeterminadas de seguridad de puerto

Característica	Configuración predeterminada
Seguridad de puerto	Desactivada en un puerto.
Número máximo de direcciones MAC seguras	1
Modo de violación	Shutdown. El puerto se desactiva cuando se supera el número máximo de direcciones MAC seguras y se envía una notificación SNMP trap.
Aprendizaje de direcciones sin modificación	Desactivado.

Configuración predeterminada

Configuración de la seguridad de puerto en un switch Catalyst de Cisco

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar al modo de configuración global. Use este comando del IOS de Cisco:	S1#**configure terminal**
Especificar el tipo y número de interfaz física a configurar, por ejemplo fastEthernet F0/18, e ingresar al modo de configuración de interfaz. Use este comando del IOS de Cisco:	S1(config)#**interface fastEthernet 0/18**
Establecer el modo de interfaz como acceso. Una interfaz en el modo predeterminado deseado dinámico no se puede configurar como un puerto seguro. Use este comando del IOS de Cisco:	S1(config-if)#**switchport mode access**
Establecer la seguridad de puerto en la interfaz. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security**
Volver al modo EXEC privilegiado. Use este comando del IOS de Cisco:	S1(config-if)#**end**

Configurar la seguridad de puerto dinámica

Guión de configuración de seguridad de puerto

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global. Use este comando del IOS de Cisco:	S1#**configure terminal**
Especificar el tipo y número de interfaz física a configurar. Use este comando del IOS de Cisco:	S1(config)#**interface fastEthernet 0/18**
Establecer el modo de interfaz como acceso. Use este comando del IOS de Cisco:	S1(config-if)#**switchport mode access**
Activar la seguridad de puerto en la interfaz. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security**
Establecer el número máximo de direcciones seguras en 50. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security maximum 50**
Activar el aprendizaje sin modificaciones. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security mac-address sticky**
Volver al modo EXEC privilegiado. Use este comando del IOS de Cisco:	S1**(config-if)#end**

Configurar la seguridad de puerto sin modificación

Verificar la seguridad de puerto

Después de haber configurado la seguridad de puerto para el switch, se debe verificar que se haya configurado de manera correcta. Se deben revisar todas las interfaces para verificar que se ha establecido la seguridad de puerto de manera correcta. También se debe verificar si se han configurado las direcciones MAC estáticas en forma correcta.

Verificar la configuración de seguridad de puerto

Para mostrar la configuración de seguridad de puerto para el switch o para la interfaz especificada, utilice el comando **show port-security** [**interface**interface-id].

El resultado muestra lo siguiente:

- Cantidad máxima de direcciones MAC seguras para cada interfaz
- Cantidad de direcciones MAC seguras en la interfaz
- Cantidad de violaciones de seguridad que se han producido
- Modo de violación

Verificar las direcciones MAC seguras

Haga clic en el botón Verificar las direcciones MAC seguras en la figura.

Para mostrar todas las direcciones MAC seguras configuradas en todas las interfaces del switch o en una interfaz especificada, con la información de expiración para cada una, utilice el comando **show port-security** [interfaceinterface-id].

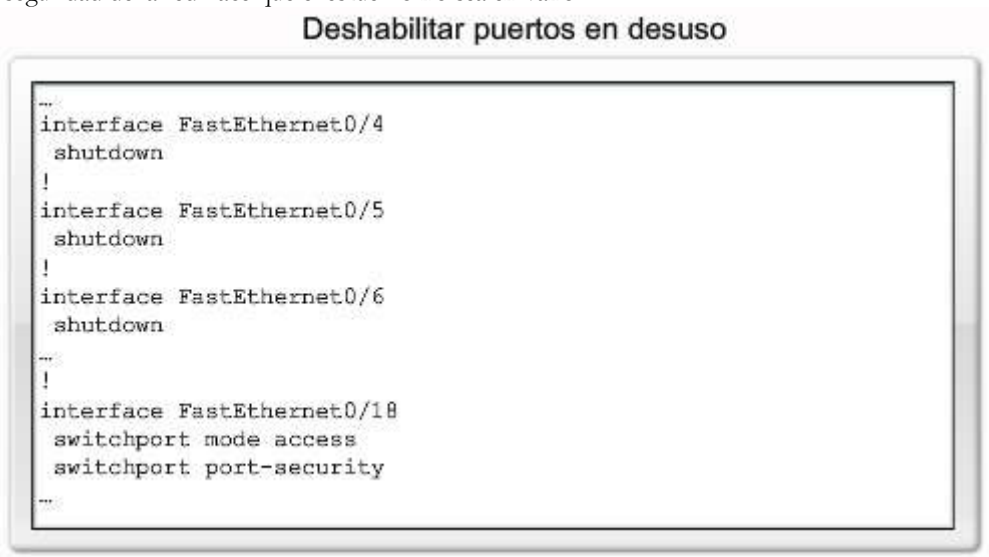
2.4.7 SEGURIDAD DE LOS PUERTOS NO UTILIZADOS.-

Deshabilitar puertos en desuso

En este tema aprenderá la forma de utilizar un simple comando IOS de Cisco para asegurar los puertos de switch que no se utilizan. Un método simple utilizado por muchos administradores para proteger la red del acceso no autorizado es deshabilitar todos los puertos no utilizados de un switch de la red. Por ejemplo: imagine que un switch 2960 de Cisco posee 24 puertos. Si existen tres conexiones Fast Ethernet que se utilizan, una buena práctica de seguridad demanda la deshabilitación de los 21 puertos que no se utilizan. La figura muestra el resultado parcial para esta configuración.

Es simple deshabilitar varios puertos en un switch. Explore todos los puertos no utilizados y emita el comando IOS de Cisco **shutdown**. Una forma alternativa de desactivar varios puertos es mediante el comando **interface range**. Si un puerto debe ser activado, se puede ingresar el comando **no shutdown** en forma manual para esa interfaz.

El proceso de habilitar y deshabilitar puertos puede convertirse en una tarea tediosa, pero el valor obtenido en términos de aumento de la seguridad de la red hace que el esfuerzo no sea en vano.



CAPITULO III – "VLAN"

3.0 INTRODUCCIÓN DEL CAPITULO.-

3.0.1 INTRODUCCIÓN DEL CAPITULO.-

El rendimiento de la red puede ser un factor en la productividad de una organización y su reputación para realizar sus transmisiones en la forma prevista. Una de las tecnologías que contribuyen al excelente rendimiento de la red es la división de los grandes dominios de broadcast en dominios más pequeños con las VLAN. Los dominios de broadcast más pequeños limitan el número de dispositivos que participan en los broadcasts y permiten que los dispositivos se separen en agrupaciones funcionales, como servicios de base de datos para un departamento contable y transferencia de datos a alta velocidad para un departamento de ingeniería. En este capítulo, aprenderá a configurar, manejar y solucionar problemas de las VLAN y los enlaces troncales.

En este capítulo aprenderá a:

- Explicar el rol de las VLAN en una red.
- Explicar el rol del enlace troncal de las VLAN en una red.
- Configurar las VLAN en los switches en una topología de la red.
- Realizar el diagnóstico de fallas comunes de la configuración de software o hardware asociadas con las VLAN en los switches en una topología de la red.

3.1 PRESENTACIÓN DE LAS VLAN.-

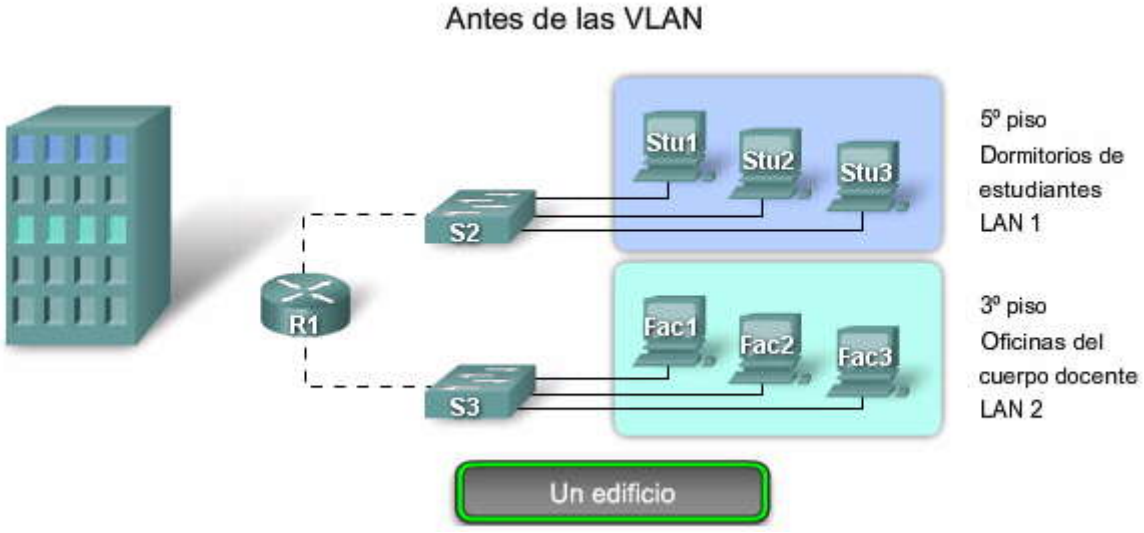
3.1.1 PRESENTACIÓN DE LAS VLAN.-

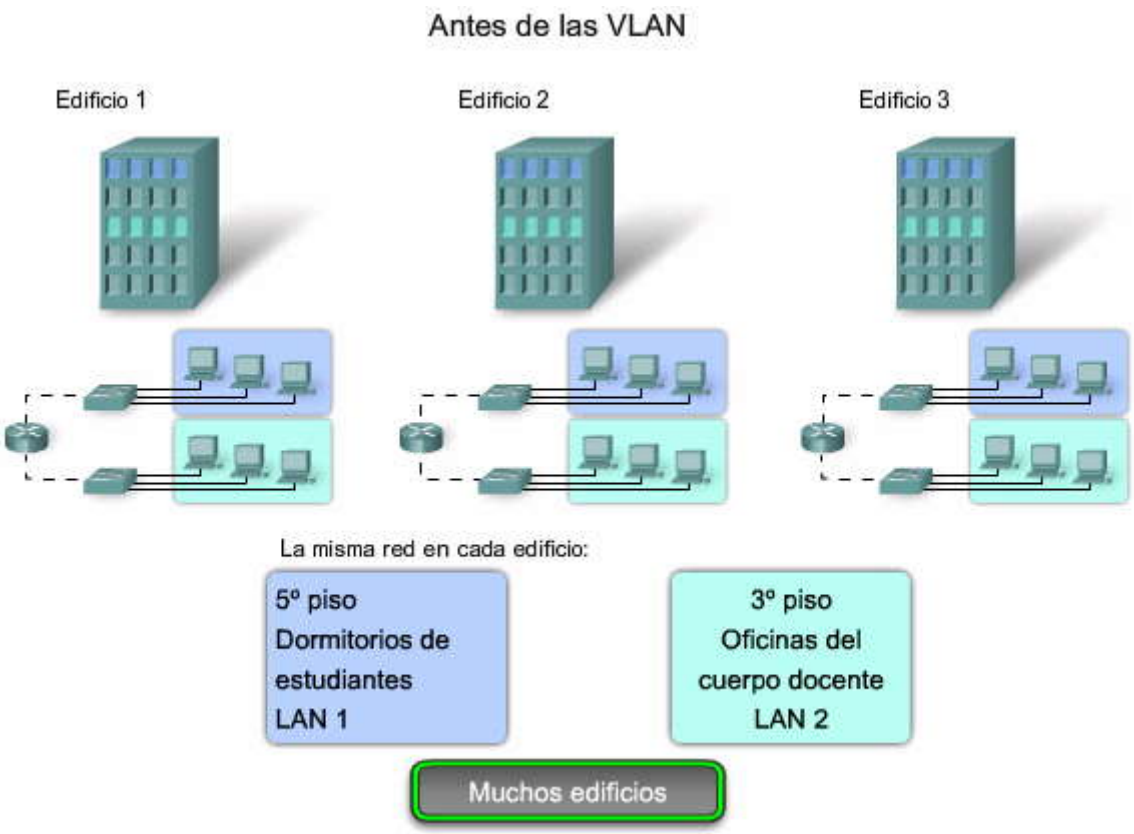
Antes de las VLAN

Para poder apreciar por qué las VLAN se utilizan tanto hoy en día, considere una pequeña comunidad con dormitorios de estudiantes y oficinas del cuerpo docente, todo en un solo edificio. La figura muestra las computadoras de los estudiantes en una LAN y las computadoras del cuerpo docente en otra LAN. Esto funciona bien debido a que todos los departamentos están juntos físicamente, por lo tanto, es fácil proporcionarles los recursos de la red.

Haga clic en el botón Muchos Edificios en la figura.

Un año después, la universidad creció y, ahora, tiene tres edificios. En la figura, la red original es la misma pero las computadoras de los estudiantes y del cuerpo docente están distribuidas en los tres edificios. Los dormitorios de los estudiantes permanecen en el quinto piso y las oficinas del cuerpo docente en el tercer piso. Sin embargo, el departamento de TI ahora quiere asegurarse de que todas las computadoras de los estudiantes compartan las mismas características de seguridad y controles de ancho de banda. ¿Cómo puede la red acomodar las necesidades compartidas de los departamentos separados geográficamente? ¿Crea una LAN grande y conecta por cable a todos los departamentos juntos? ¿Cuán fácil sería realizar cambios a esa red? Sería muy bueno agrupar a las personas con los recursos que utilizan sin tener en cuenta su ubicación geográfica, y sería más fácil administrar la seguridad específica y las necesidades de ancho de banda.





Visión general de VLAN

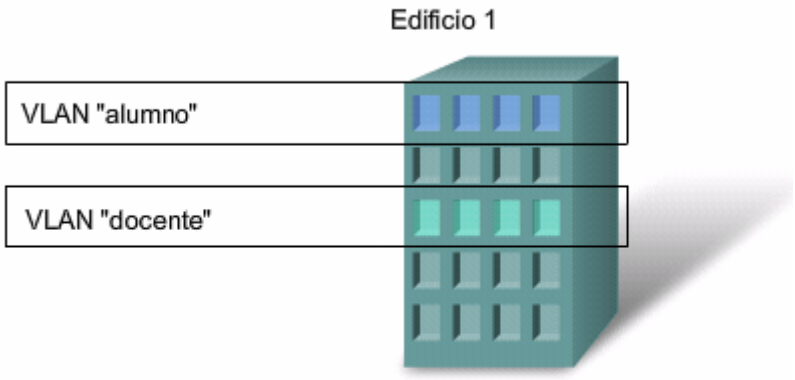
La solución para la comunidad de la universidad es utilizar una tecnología de red denominada LAN (VLAN) virtual. Una VLAN permite que un administrador de red cree grupos de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. Cuando configura una VLAN, puede ponerle un nombre para describir la función principal de los usuarios de esa VLAN. Como otro ejemplo, todas las computadoras de los estudiantes se pueden configurar en la VLAN "Estudiante". Mediante las VLAN, puede segmentar de manera lógica las redes conmutadas basadas en equipos de proyectos, funcioneso departamentos. También puede utilizar una VLAN para estructurar geográficamente su red para respaldar la confianza en aumento de las empresas sobre trabajadores domésticos. En la figura, se crea una VLAN para los estudiantes y otra para el cuerpo docente. Estas VLAN permiten que el administrador de la red implemente las políticas de acceso y seguridad para grupos particulares de usuarios. Por ejemplo: se puede permitir que el cuerpo docente, pero no los estudiantes, obtenga acceso a los servidores de administración de e-learning para desarrollar materiales de cursos en línea.

Haga clic en el botón Detalles en la figura.

Detalles de la VLAN

Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada. La figura muestra una red con tres computadoras. Para que las computadoras se comuniquen en la misma VLAN, cada una debe tener una dirección IP y una máscara de subred consistente con esa VLAN. En el switch deben darse de alta las VLANs y cada puerto asignarse a la VLAN correspondiente. Un puerto de switch con una VLAN singular configurada en el mismo se denomina puerto de acceso. Recuerde que si dos computadoras están conectadas físicamente en el mismo switch no significa que se puedan comunicar. Los dispositivos en dos redes y subredes separadas se deben comunicar a través de un router (Capa 3), se utilicen o no las VLAN. No necesita las VLAN para tener redes y subredes múltiples en una red conmutada, pero existen ventajas reales para utilizar las VLAN.

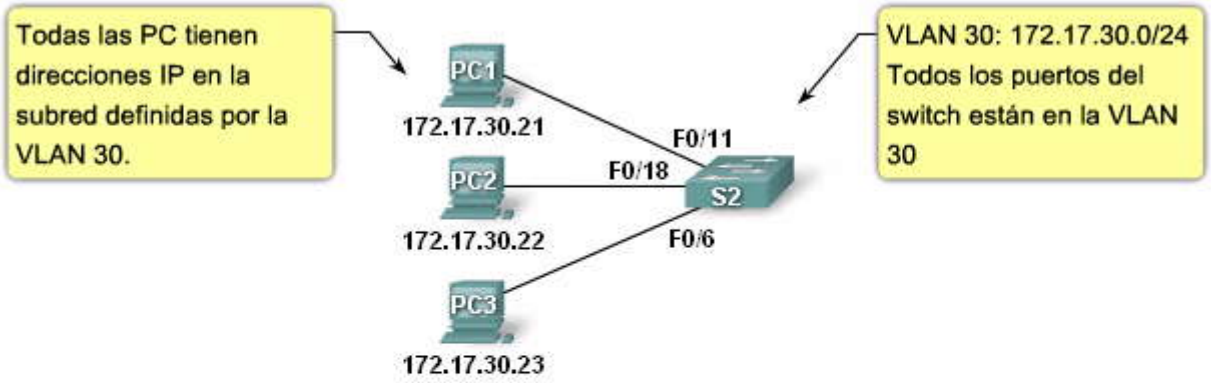
¿Qué es una VLAN?



- Una VLAN es una red LAN independiente.
- Una VLAN permite que las PC del alumno y del docente estén separadas, aunque compartan la misma infraestructura.
- Se le puede otorgar un nombre a la VLAN para facilitar su identificación

Descripción general

¿Qué es una VLAN?



- Una VLAN = Subred (en las LAN conmutadas modernas)
- En el switch
  - Configurar la VLAN
  - Asignar el puerto a la VLAN
- En la PC asignar una dirección IP en la subred de VLAN

Detalles

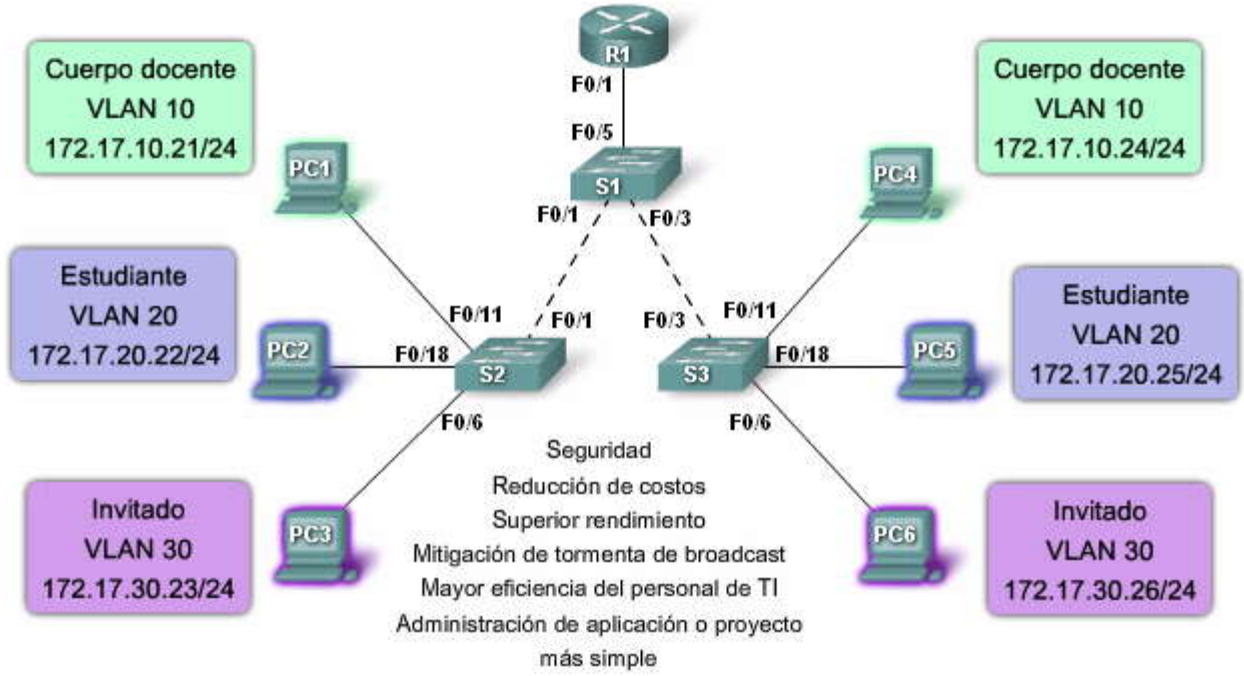
Ventajas de las VLAN

La productividad del usuario y la adaptabilidad de la red son impulsores clave para el crecimiento y el éxito del negocio. La implementación de la tecnología de VLAN permite que una red admita de manera más flexible las metas comerciales. Los principales beneficios de utilizar las VLAN son los siguientes:

Seguridad: los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial. Las computadoras del cuerpo docente se encuentran en la VLAN 10 y están completamente separadas del tráfico de datos del Invitado y de los estudiantes.

Reducción de costo: el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.

Mejor rendimiento: la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.
Mitigación de la tormenta de broadcast: la división de una red en las VLAN reduce la cantidad de dispositivos que pueden participar en una tormenta de broadcast. Como se analizó en el capítulo "Configure un switch", la segmentación de LAN impide que una tormenta de broadcast se propague a toda la red. En la figura puede observar que, a pesar de que hay seis computadoras en esta red, hay sólo tres dominios de broadcast: Cuerpo docente, Estudiante y Invitado .
Mayor eficiencia del personal de TI: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando proporciona un switch nuevo, todas las políticas y procedimientos que ya se configuraron para la VLAN particular se implementan cuando se asignan los puertos. También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre. En la figura, para una identificación más fácil se nombró "Estudiante" a la VLAN 20, la VLAN 10 se podría nombrar "Cuerpo docente" y la VLAN 30 "Invitado ".
Administración de aplicación o de proyectos más simples: las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales. Tener funciones separadas hace que gestionar unproyecto o trabajar con una aplicación especializada sea más fácil, por ejemplo una plataforma de desarrollo de e-learning para el cuerpo docente. También es fácil determinar el alcance de los efectos de la actualización de los servicios de red.



Rangos del ID de la VLAN
El acceso a las VLAN está dividido en un rango normal o un rango extendido.

VLAN de rango normal

- Se utiliza en redes de pequeños y medianos negocios y empresas.
- Se identifica mediante un ID de VLAN entre 1 y 1005.
- Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI.
- Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar. Aprenderá más acerca de VLAN 1 más adelante en este capítulo.
- Las configuraciones se almacenan dentro de un archivo de datos de la VLAN, denominado vlan.dat. El archivo vlan.dat se encuentra en la memoria flash del switch.
- El protocolo de enlace troncal de la VLAN (VTP), que ayuda a gestionar las configuraciones de la VLAN entre los switches, sólo puede asimilar las VLAN de rango normal y las almacena en el archivo de base de datos de la VLAN.

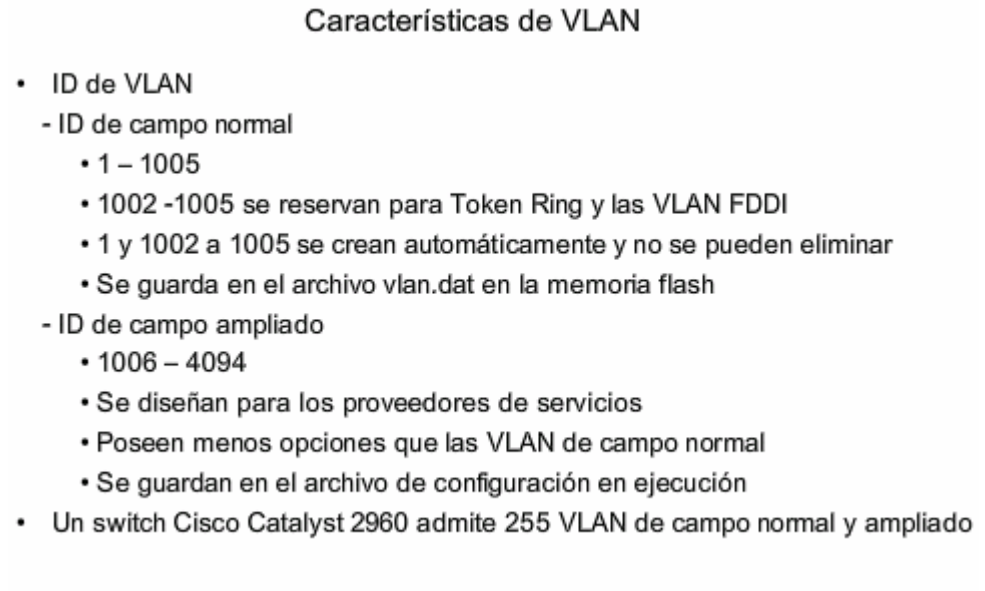
VLAN de rango extendido

- Posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor. Algunas empresas globales podrían ser lo suficientemente grandes como para necesitar los ID de las VLAN de rango extendido.
- Se identifican mediante un ID de VLAN entre 1006 y 4094.
- Admiten menos características de VLAN que las VLAN de rango normal.

- Se guardan en el archivo de configuración en ejecución.
- VTP no aprende las VLAN de rango extendido.

255 VLAN configurables

Un switch de Cisco Catalyst 2960 puede admitir hasta 255 VLAN de rango normal y extendido, a pesar de que el número configurado afecta el rendimiento del hardware del switch. Debido a que la red de una empresa puede necesitar un switch con muchos puertos, Cisco ha desarrollado switches a nivel de empresa que se pueden unir o apilar juntos para crear una sola unidad de conmutación que consiste en nueve switches separados. Cada switch por separado puedetener 48 puertos, lo que suma 432 puertos en una sola unidad de conmutación. En este caso, el límite de 255 VLAN por un solo switch podría ser una restricción para algunos clientes de empresas.



3.1.2 TIPOS DE VLAN.-

Hoy en día, existe fundamentalmente una manera de implementar las VLAN: VLAN basada en puerto. Una VLAN basada en puerto se asocia con un puerto denominado acceso VLAN.

Sin embargo, en las redes existe una cantidad de términos para las VLAN. Algunos términos definen el tipo de tráfico de red que envían y otros definen una función específica que desempeña una VLAN. A continuación, se describe la terminología común de VLAN:

Pase el mouse sobre el botón VLAN de Datos en la figura.

VLAN de Datos

Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario.

Pase el mouse sobre el botón VLAN Predeterminada en la figura.

VLAN Predeterminada

Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada luego del arranque inicial del switch. Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos parte del mismo dominio de broadcast. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches de Cisco es la VLAN 1. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no la puede volver a denominar y no la puede eliminar. El tráfico de control de Capa 2, como CDP y el tráfico del protocolo spanning tree se asociará siempre con la VLAN 1: esto no se puede cambiar. En la figura, el tráfico de la VLAN1 se envía sobre los enlaces troncales de la VLAN conectando los switches S1, S2 y S3. Es una optimización de seguridad para cambiar la VLAN predeterminada a una VLAN que no sea la VLAN 1; esto implica configurar todos los puertos en el switch para que se asocien con una VLAN predeterminada que no

sea la VLAN 1. Los enlaces troncales de la VLAN admiten la transmisión de tráfico desde más de una VLAN. A pesar de que los enlaces troncales de la VLAN se mencionan a lo largo de esta sección, se explican a detalle en la próxima sección.

Nota: Algunos administradores de red utilizan el término "VLAN predeterminada" para referirse a una VLAN que no sea la VLAN 1 que el administrador de red definió como la VLAN a la que se asignan todos los puertos cuando no están en uso. En este caso, la única función que cumple la VLAN 1 es la de manejar el tráfico de control de Capa 2 para la red.

Pase el mouse sobre el botón VLAN Nativa en la figura.

VLAN Nativa

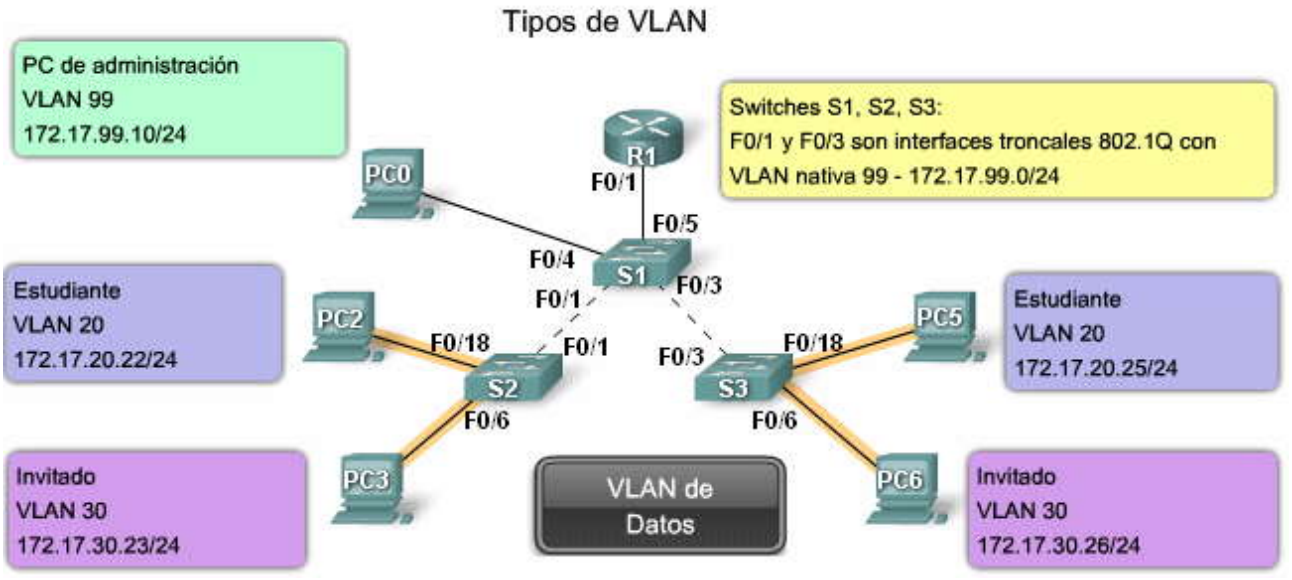
Una VLAN nativa está asignada a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa. En la figura, la VLAN nativa es la VLAN 99. El tráfico no etiquetado lo genera una computadora conectada a un puerto de switch que se configura con la VLAN nativa. Las VLAN se establecen en la especificación IEEE 802.1Q para mantener la compatibilidad retrospectiva con el tráfico no etiquetado común para los ejemplos de LAN antigua. Para nuestro fin, una VLAN nativa sirve como un identificador común en extremos opuestos de un enlace troncal. Es una optimización usar una VLAN diferente de la VLAN 1 como la VLAN nativa.

Pase el mouse sobre el botón VLAN de Administración en la figura.

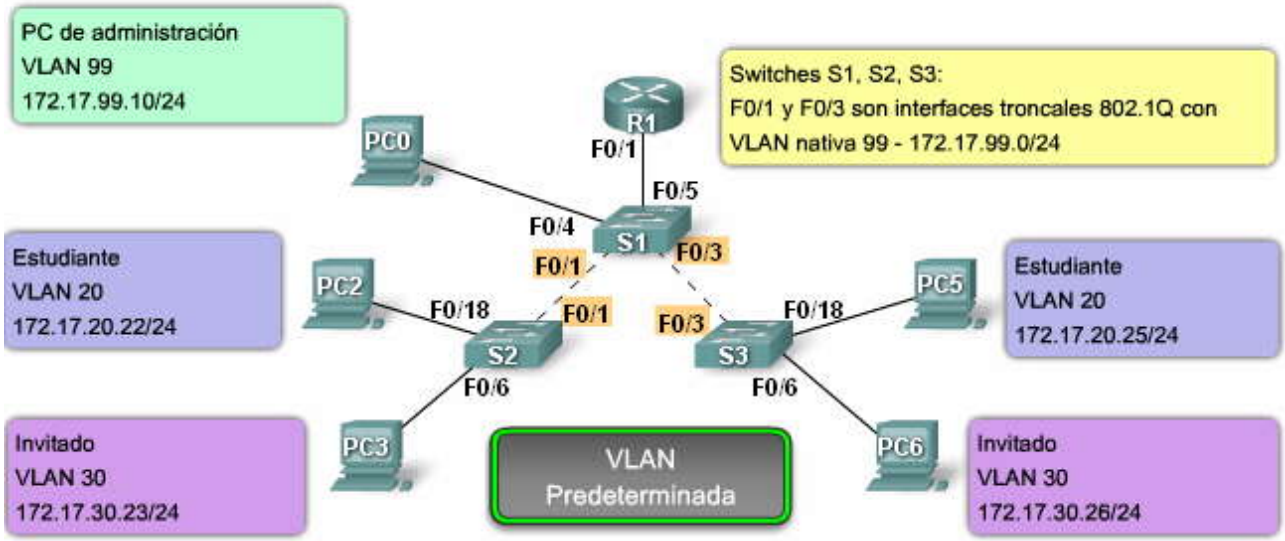
VLAN de Administración

Una VLAN de administración es cualquier VLAN que usted configura para acceder a las capacidades de administración de un switch. La VLAN 1 serviría como VLAN de administración si no definió proactivamente una VLAN única para que sirva como VLAN de administración. Se asigna una dirección IP y una máscara de subred a la VLAN de administración. Se puede manejar un switch mediante HTTP, Telnet, SSH o SNMP. Debido a que la configuración lista para usar de un switch de Cisco tiene a VLAN 1 como la VLAN predeterminada, puede notar que la VLAN 1 sería una mala opción como VLAN de administración; no querría que un usuario arbitrario se conectara a un switch para que se configurara de manera predeterminada la VLAN de administración. Recuerde que configuró la VLAN de administración como VLAN 99 en el capítulo Configuración y conceptos básicos de switch.

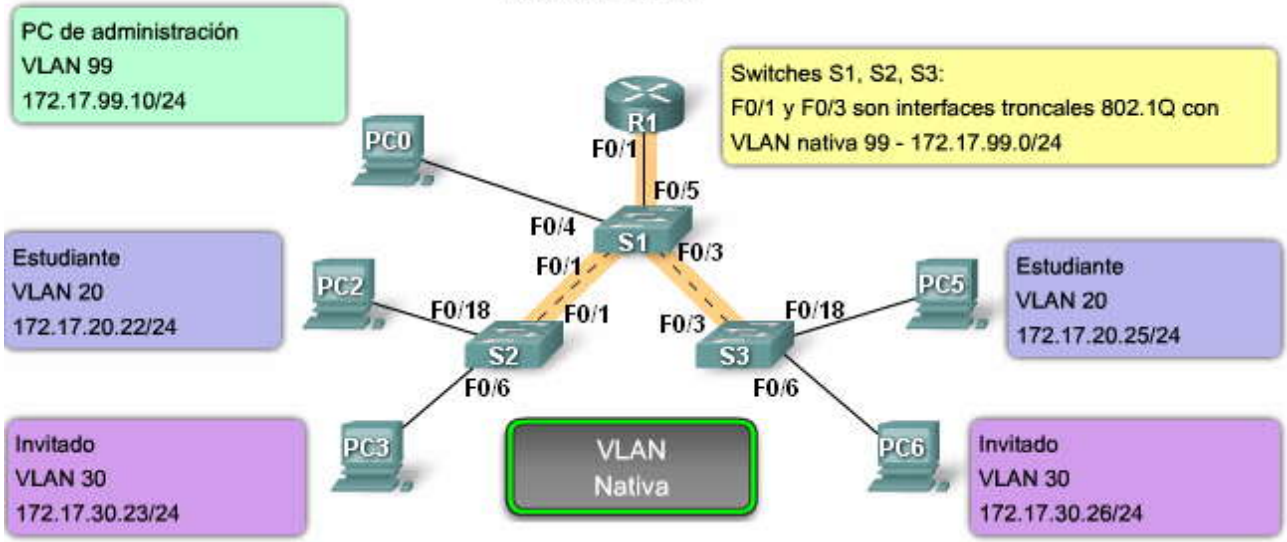
En la página siguiente, investigaremos el tipo de VLAN remanente: VLAN de voz.



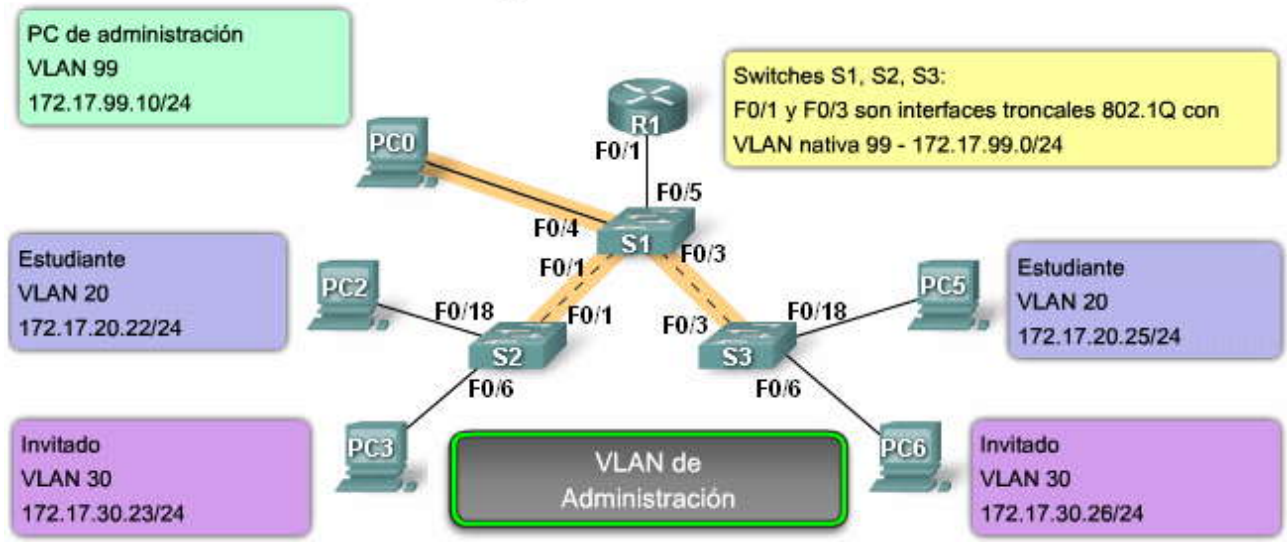
Tipos de VLAN



Tipos de VLAN



Tipos de VLAN



VLAN de voz
Es fácil apreciar por qué se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Imagine que está recibiendo una llamada de urgencia y de repente la calidad de la transmisión se distorsiona tanto que no puede comprender lo que está diciendo la persona que llama. El tráfico de VoIP requiere:

- Ancho de banda garantizado para asegurar la calidad de la voz
- Prioridad de la transmisión sobre los tipos de tráfico de la red
- Capacidad para ser enrutado en áreas congestionadas de la red
- Demora de menos de 150 milisegundos (ms) a través de la red

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP. Los detalles sobre cómo configurar una red para que admita VoIP están más allá del alcance del curso, pero es útil resumir cómo una VLAN de voz funciona entre un switch, un teléfono IP de Cisco y una computadora.

En la figura, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC5 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes. El puerto F0/18 en S3 se configura para que esté en modo de voz a fin de que diga al teléfono que etiquete las tramas de voz con VLAN 150. Las tramas de datos que vienen a través del teléfono IP de Cisco desde la PC5 no se marcan. Los datos que se destinan a la PC5 que llegan del puerto F0/18 se etiquetan con la VLAN 20 en el camino al teléfono, que elimina la etiqueta de la VLAN antes de que los datos se envíen a la PC5. Etiquetar se refiere a la adición de bytes a un campo en la trama de datos que utiliza el switch para identificar a qué VLAN se debe enviar la trama de datos. Más adelante, aprenderá cómo se etiquetan las tramas de datos.

Haga clic en el botón Detalles en la figura.

Un teléfono de Cisco es un switch

El teléfono IP de Cisco contiene un switch integrado de tres puertos 10/100, como se muestra en la figura. Los puertos proporcionan conexiones dedicadas para estos dispositivos:

- El puerto 1 se conecta al switch o a otro dispositivo de voz sobre IP (VoIP).
- El puerto 2 es una interfaz interna 10/100 que envía el tráfico del teléfono IP.
- El puerto 3 (puerto de acceso) se conecta a una PC u otro dispositivo.

La figura muestra una manera de conectar un teléfono IP.

La función de la VLAN de voz permite que los puertos de switch envíen el tráfico de voz IP desde un teléfono IP. Cuando se conecta el switch a un teléfono IP, el switch envía mensajes que indican al teléfono IP conectado que envíe el tráfico de voz etiquetado con el ID 150 de VLAN de voz. El tráfico de la PC conectada al teléfono IP pasa por el teléfono IP sin etiquetar. Cuando se configuró el puerto del switch con una VLAN de voz, el enlace entre el switch y el teléfono IP funciona como un enlace troncal para enviar tanto el tráfico de voz etiquetado como el tráfico de datos no etiquetado.

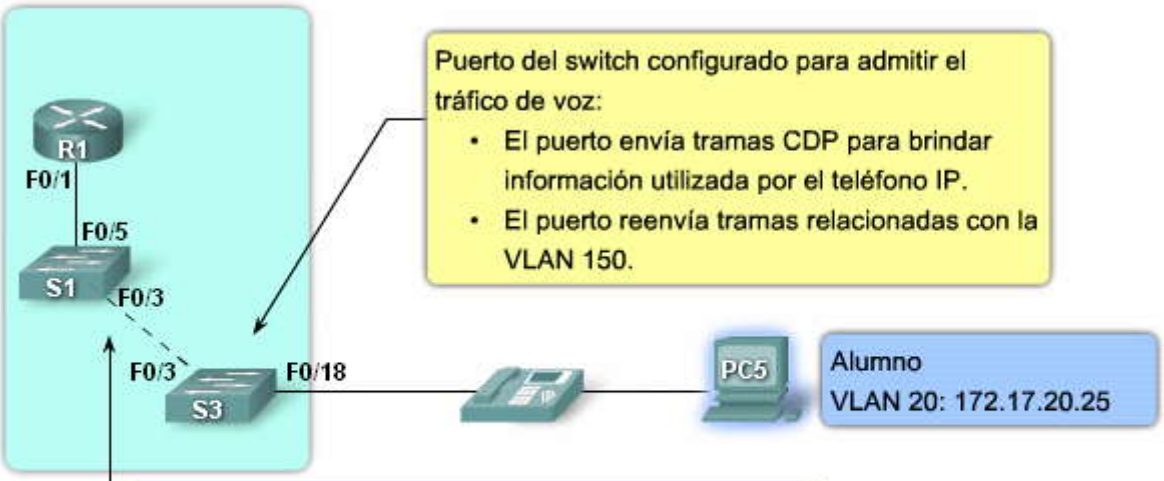
Nota: La comunicación entre el switch y el teléfono IP la facilita el protocolo CDP. Este protocolo se analizará en detalle en CCNA Exploration: Curso sobre Conceptos y protocolos de enrutamiento.

Haga clic en el botón Ejemplo de Configuración en la figura.

Ejemplo de configuración

La figura muestra el resultado del ejemplo. Un análisis de los comandos IOS de Cisco está más allá del alcance de este curso pero puede observar que las áreas destacadas en el resultado del ejemplo muestran la interfaz F0/18 configurada con una VLAN configurada para datos (VLAN 20) y una VLAN configurada para voz (VLAN 150).

VLAN de voz

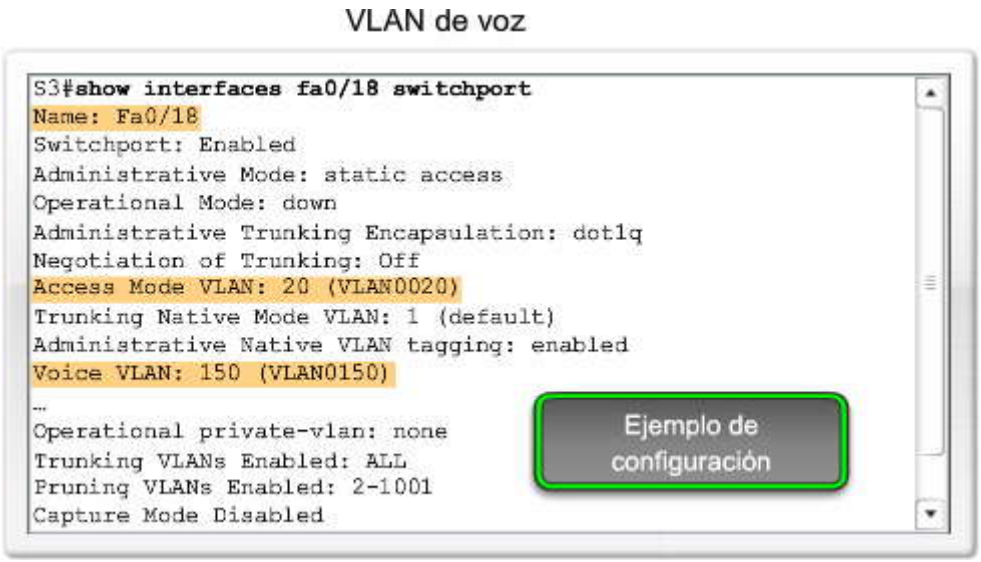


Teléfonos IP en la Red

VLAN de voz

Un teléfono IP de Cisco es un switch

Detalles



Tipos de tráfico de red

En CCNA Exploration: En Aspectos básicos de redes, aprendió sobre los diferentes tipos de tráfico que puede manejar una LAN. Debido a que una VLAN tiene todas las características de una LAN, una VLAN debe incorporar el mismo tráfico de red que una LAN.

Administración de red y tráfico de control

Muchos tipos diferentes de tráfico de administración de red y de control pueden estar presentes en la red, como las actualizaciones de Cisco Discovery Protocol (CDP), Simple Network Management Protocol (SNMP) y tráfico de Remote Monitoring (RMON).

Pase el mouse sobre el botón Administración de red en la figura.

Telefonía IP

Los tipos de tráfico de telefonía IP son el tráfico de señalización y el tráfico de voz. El tráfico de señalización es responsable de la configuración de la llamada, el progreso y la desconexión y atraviesa la red de extremo a extremo. El otro tipo de tráfico de telefonía consiste en paquetes de datos de la conversación de voz existente. Como acaba de ver, en una red configurada con VLAN, se recomienda con énfasis asignar una VLAN diferente a la VLAN 1 como VLAN de administración. El tráfico de datos debe asociarse con una VLAN de datos (diferente a la VLAN 1) y el tráfico de voz se asocia con una VLAN de voz.

Pase el mouse sobre el botón Telefonía IP en la figura.

IP Multicast

El tráfico IP multicast se envía desde una dirección de origen particular a un grupo multicast que se identifica mediante un único IP y un par de direcciones MAC de grupo de destino. Broadcasts Cisco IP/TV son ejemplos de aplicaciones que genera este tipo de tráfico. El tráfico multicast puede producir una gran cantidad de datos que se transmiten a través de la red. Cuando la red debe admitir tráfico multicast, las VLAN deben configurarse para asegurarse de que el tráfico multicast se dirija sólo a aquellos dispositivos de usuario que utilizan el servicio proporcionado, como aplicaciones de audio o video remoto. Los routers se deben configurar para asegurar que el tráfico multicast se envíe a las áreas de red cuando se le solicita.

Pase el mouse sobre el botón IP Multicast en la figura.

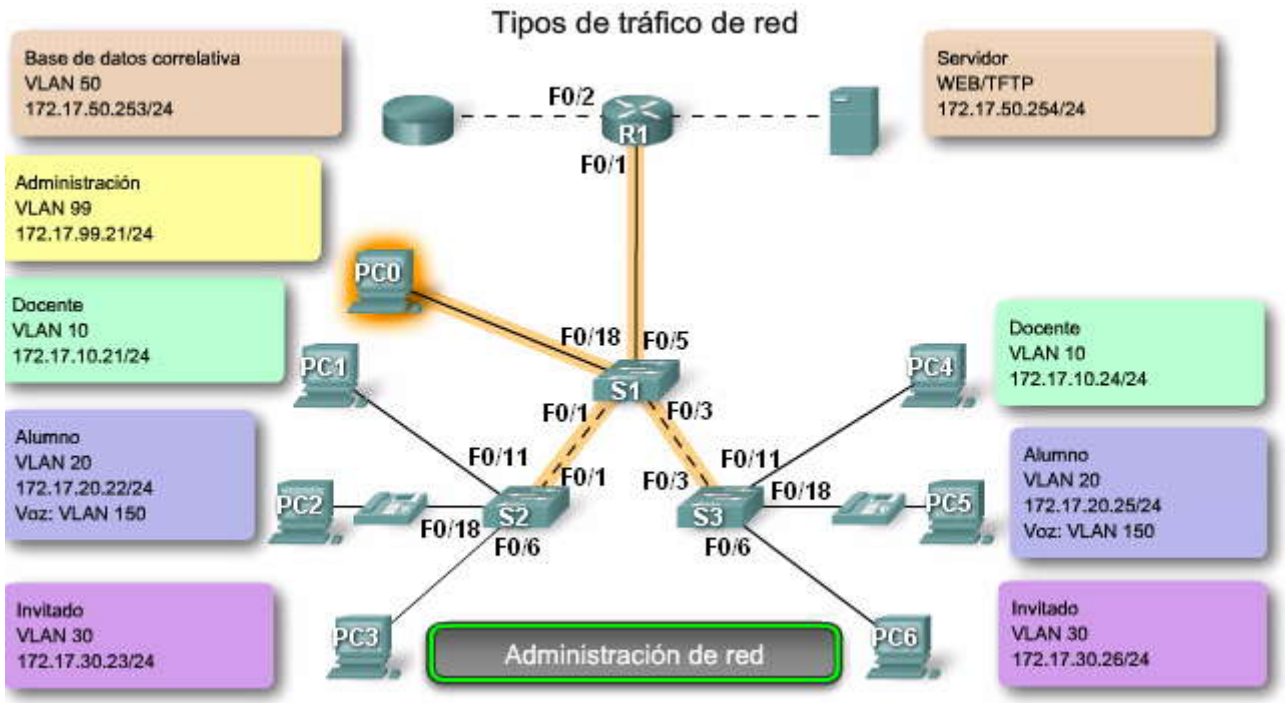
Datos normales

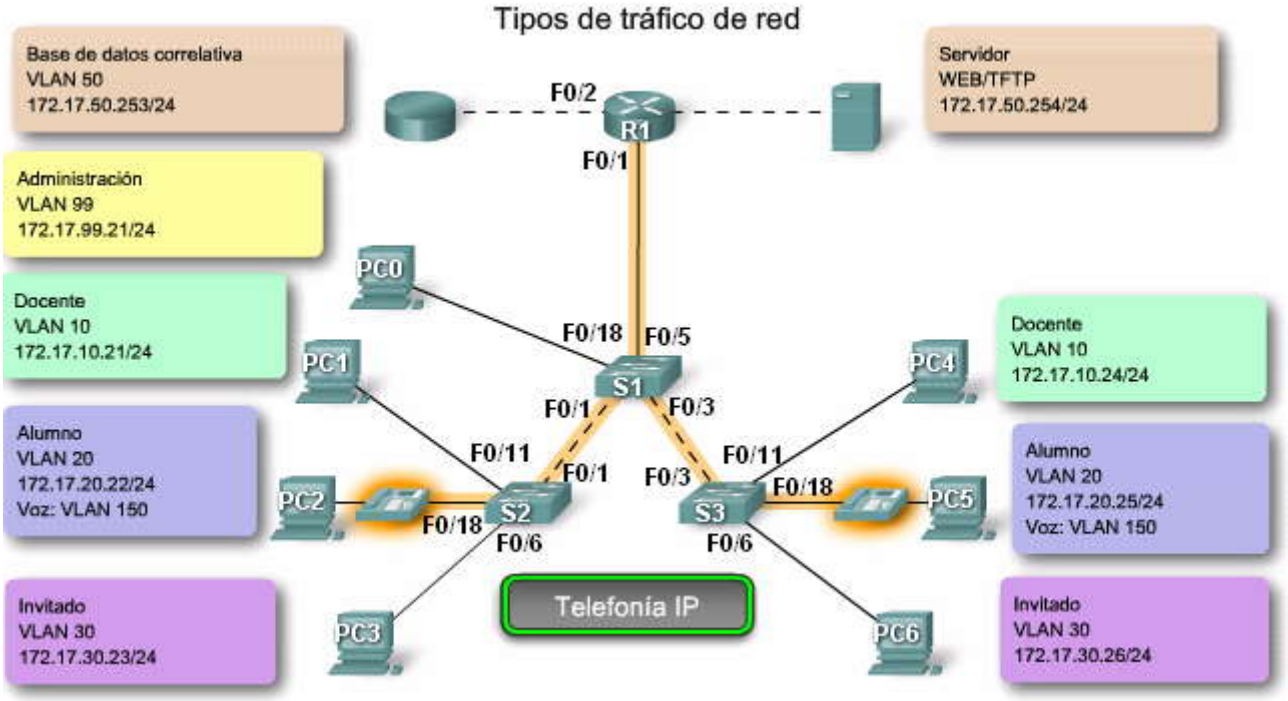
El tráfico de datos normales se relaciona con el almacenamiento y creación de archivos, servicios de impresión, acceso a la base de datos del correo electrónico y otras aplicaciones de red compartidas que son comunes para usos comerciales. Las VLAN son una solución natural para este tipo de tráfico, ya que pueden segmentar a los usuarios por sus funciones o área geográfica para administrar de manera más fácil las necesidades específicas.

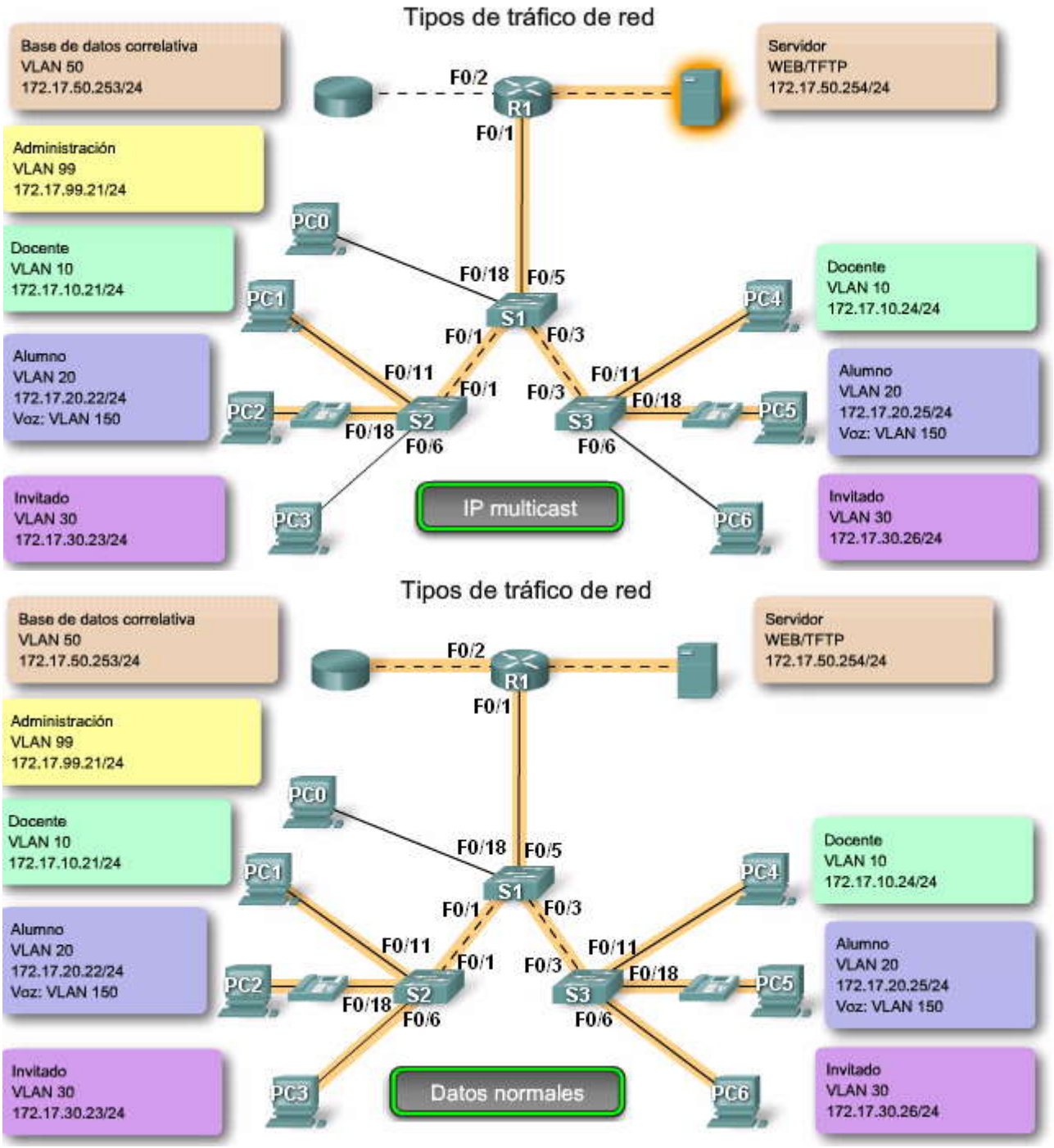
Pase el mouse sobre el botón Datos normales en la figura.

Clase Scavenger

Se pretende que la clase Scavenger proporcione servicios less-than-best-effort a ciertas aplicaciones. Las aplicaciones que se asignan a esta clase contribuyen poco o nada a los objetivos organizativos de la empresa y están generalmente orientadas, por su naturaleza, al entretenimiento. Esto incluye aplicaciones compartidas de medios entre pares (KaZaa, Morpheus, Groekster, Napster, iMesh, y demás), aplicaciones de juegos (Doom, Quake, Unreal Tournament, y demás) y cualquier aplicación de video de entretenimiento.







3.1.3 MODOS DE MEMBRESIS DEL PUERTO DE SWTICH.-

Puertos de switch

Los puertos de switch son interfaces de Capa 2 únicamente asociados con un puerto físico. Los puertos de switch se utilizan para manejar la interfaz física y los protocolos asociados de Capa 2. No manejan enrutamiento o puenteo. Los puertos de switch pertenecen a una o más VLAN.

Modos de puertos de switch de VLAN

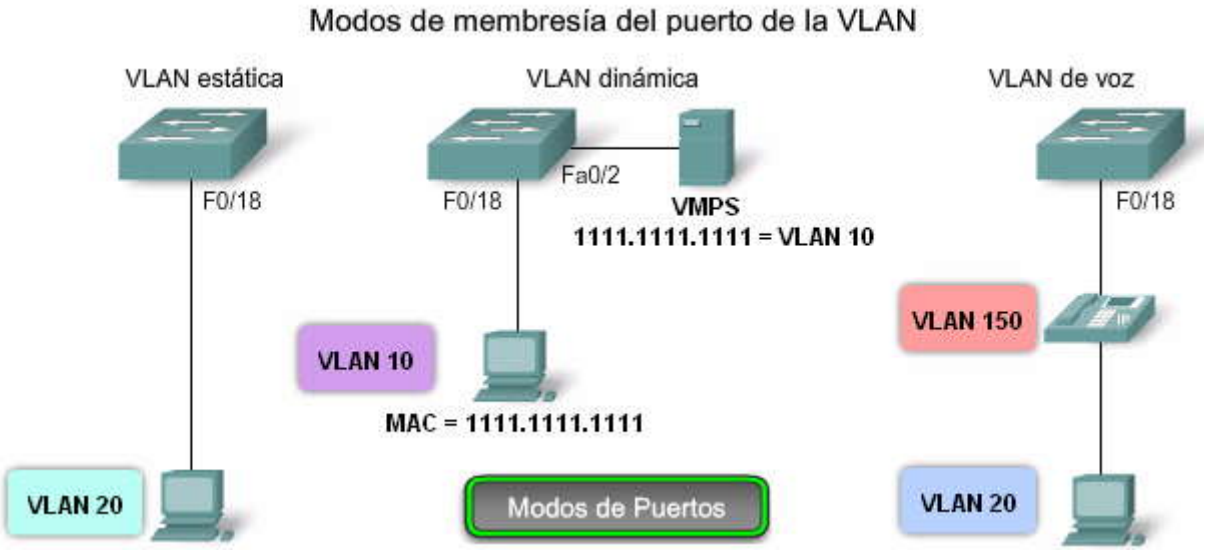
Cuando configura una VLAN, debe asignarle un número de ID y le puede dar un nombre si lo desea. El propósito de las implementaciones de la VLAN es asociar con criterio los puertos con las VLAN particulares. Se configura el puerto para enviar una trama a una VLAN específica. Como se mencionó anteriormente, el usuario puede configurar una VLAN en el modo de voz para admitir tráfico de datos y de voz que llega desde un teléfono IP de Cisco. El usuario puede configurar un puerto para que pertenezca a una VLAN mediante la asignación de un modo de membresía que especifique el tipo de tráfico que envía el puerto y las VLAN a las que puede pertenecer. Se puede configurar un puerto para que admita estos tipos de VLAN:

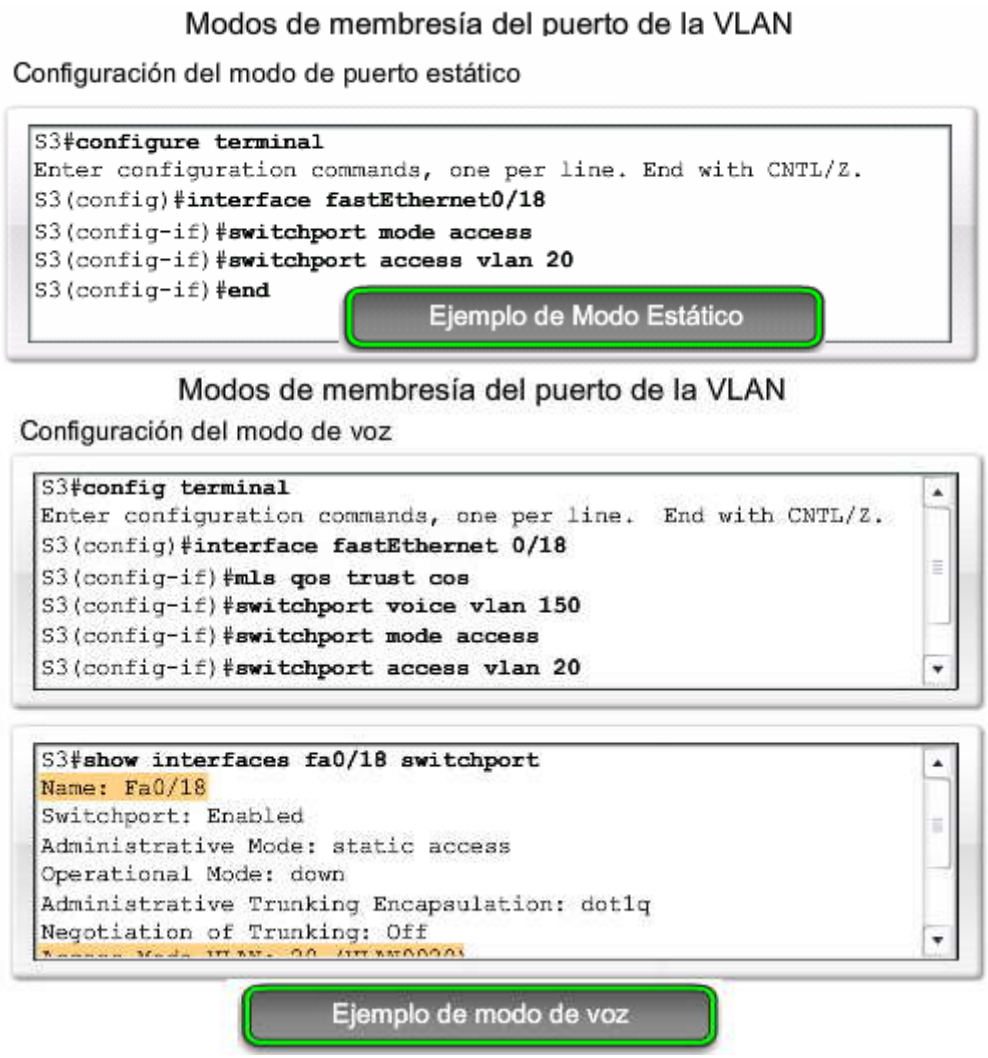
- **VLAN estática:** los puertos en un switch se asignan manualmente a una VLAN. Las VLAN estáticas se configuran por medio de la utilización del CLI de Cisco. Esto también se puede llevar a cabo con las aplicaciones de administración de GUI, como el Asistente de red Cisco. Sin embargo, una característica conveniente del CLI es que si asigna una interfaz a una VLAN que no existe, se crea la nueva VLAN para el usuario. Para ver un ejemplo de configuración de VLAN estática, haga clic en el botón Ejemplo de Modo Estático en la figura. Cuado haya finalizado, haga clic en el botón Modos de Puertos en la figura. Esta configuración no se examinará en detalle ahora. Se presentará más adelante en este capítulo.
- **VLAN dinámica:** este modo no se utiliza ampliamente en las redes de producción y no se investiga en este curso. Sin embargo, es útil saber qué es una VLAN dinámica. La membresía de una VLAN de puerto dinámico se configura utilizando un servidor especial denominado Servidor de política de membresía de VLAN (VMPS). Con el VMPS, asigna puertos de switch a las VLAN basadas en forma dinámica en la dirección MAC de origen del dispositivo conectado al puerto. El beneficio llega cuando traslada un host desde un puerto en un switch en la red hacia un puerto sobre otro switch en la red. El switch asigna en forma dinámica el puerto nuevo a la VLAN adecuada para ese host.
- **VLAN de voz:** el puerto está configurado para que esté en modo de voz a fin de que pueda admitir un teléfono IP conectado al mismo. Antes de que configure una VLAN de voz en el puerto, primero debe configurar una VLAN para voz y una VLAN para datos. En la figura, la VLAN 150 es la VLAN de voz y la VLAN 20 es la VLAN de datos. Se supone que la red ha sido configurada para garantizar que el tráfico de voz se pueda transmitir con un estado prioritario sobre la red. Cuando se enchufa por primera vez un teléfono en un puerto de switch que está en modo de voz, éste envía mensajes al teléfono proporcionándole la configuración y el ID de VLAN de voz adecuado. El teléfono IP etiqueta las tramas de voz con el ID de VLAN de voz y envía todo el tráfico de voz a través de la VLAN de voz.

Para examinar las partes de una configuración de modo de voz, haga clic en el botón Ejemplo de modo de voz en la figura:

- El comando de configuración **mls qos trust cos** garantiza que el tráfico de voz se identifique como tráfico prioritario. Recuerde que toda la red debe prepararse para que priorice el tráfico de voz. No puede simplemente configurar el puerto con este comando.
- El comando **switchport voice VLAN 150** identifica a la VLAN 150 como VLAN de voz. Puede observar esto verificado en la parte inferior de la captura de la pantalla: VLAN de voz: 150 (VLAN0150).
- El comando **switchport access VLAN 20** configura la VLAN 20 como la VLAN de modo de acceso (datos). Puede observar esto verificado en la parte inferior de la captura de la pantalla: VLAN de modo de acceso: 20 (VLAN0020).

Para obtener más detalles sobre la configuración de una VLAN de voz, visite este sitio de Cisco.com: http://www.cisco.com/en/US/products/ps6406/products_configuration_guide_chapter09186a008081d9a6.html#wp1050913.





3.1.4 CONTROL DE LOS DOMINIO DE BROADCAST CON LAS VLAN.-

Red sin VLAN

En funcionamiento normal, cuando un switch recibe una trama de broadcast en uno de sus puertos, envía la trama a todos los demás puertos. En la figura, toda la red está configurada en la misma subred, 172.17.40.0/24. Como resultado, cuandola computadora del cuerpo docente, PC1, envía una trama de broadcast, el switch S2 envía esa trama de broadcast a todos sus puertos. La red completa la recibe finalmente; la red es un dominio de broadcast.

Haga clic en los Broadcasts de red con segmentación de VLAN en la figura.

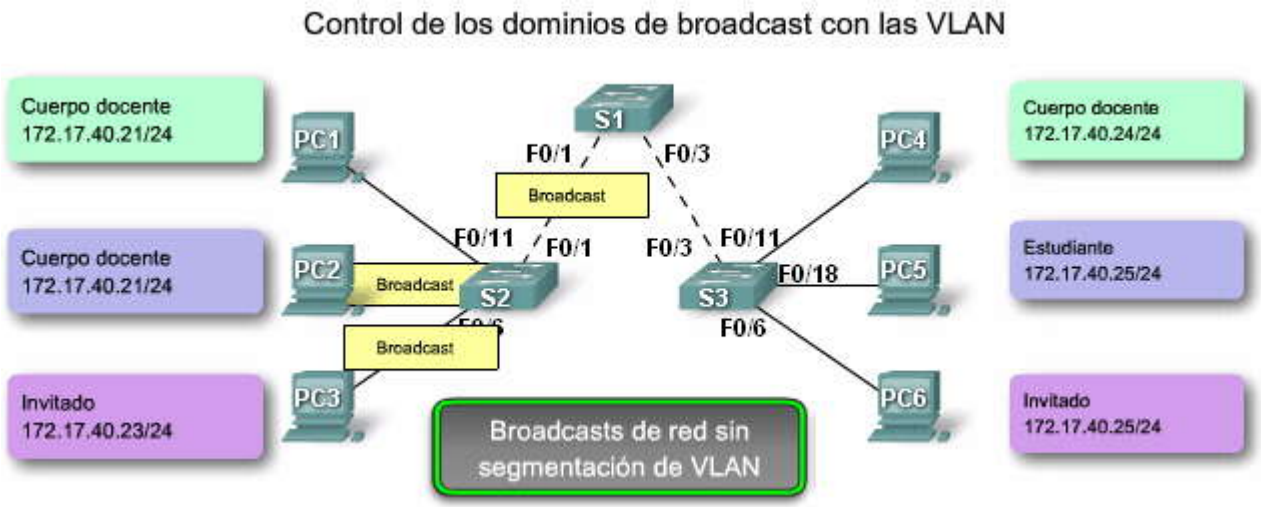
Red con VLAN

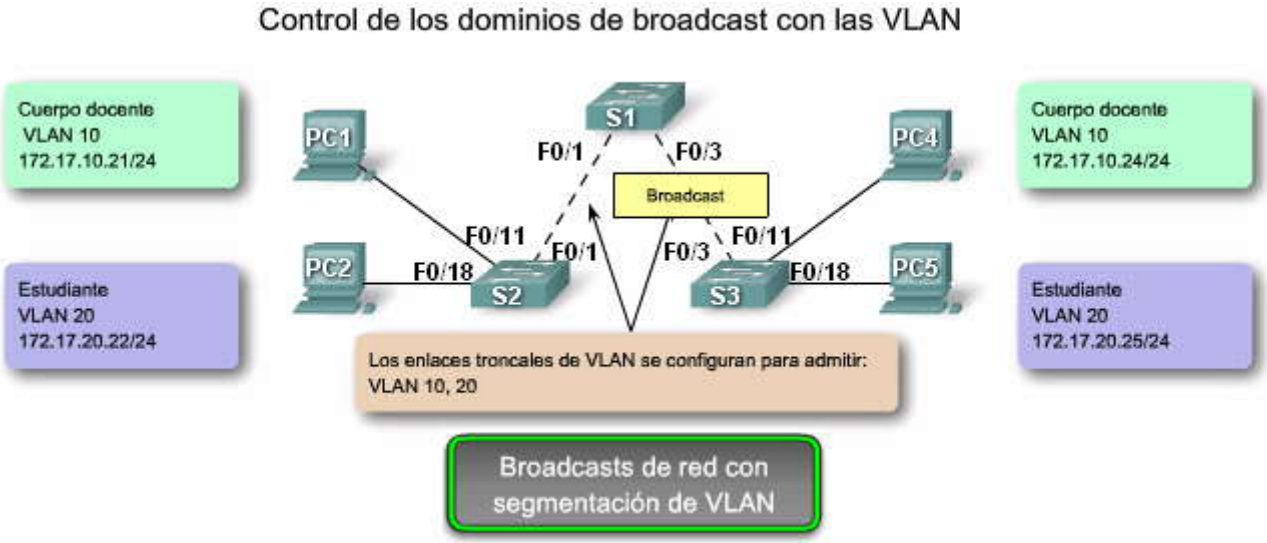
En la figura, se dividió la red en dos VLAN: Cuerpo docente como VLAN 10 y Estudiante como VLAN 20. Cuando se envía la trama de broadcast desde la computadora del cuerpo docente, PC1, al switch S2, el switch envíaesa trama de broadcast sólo a esos puertos de switch configurados para admitir VLAN 10.

En la figura, los puertos que componen la conexión entre los switches S2 y S1 (puertos F0/1) y entre S1 y S3 (puertos F0/3) han sido configurados para admitir todas las VLAN en la red. Esta conexión se denomina enlace troncal. Más adelante en este capítulo aprenderá más acerca de los enlaces troncales.

Cuando S1 recibe la trama de broadcast en el puerto F0/1, S1 envía la trama de broadcast por el único puerto configurado para admitir la VLAN 10, puerto F0/3. Cuando S3 recibe la trama de broadcast en el puerto F0/3, envía la trama de broadcast por el único puerto configurado para admitir la VLAN 10, puerto F0/11. La trama de broadcast llega a la única otra computadora en la red configurada en la VLAN 10, la computadora PC4 del cuerpo docente.

Cuando las VLAN se implementan en un switch, la transmisión del tráfico de unicast, multicast y broadcast desde un host en una VLAN en particular, se limitan a los dispositivos presentes en la VLAN.





Control de dominios de broadcast con switches y routers

La fragmentación de un gran dominio de broadcast en varias partes más pequeñas reduce el tráfico de broadcast y mejora el rendimiento de la red. La fragmentación de dominios en VLAN permite además una mejor confidencialidad de información dentro de una organización. La fragmentación de dominios de broadcast puede realizarse con las VLAN (en los switches) o con routers. Cada vez que dispositivos en diferentes redes de Capa 3 necesiten comunicarse, es necesario un router sin tener en cuenta si las VLAN están en uso.

Haga clic en el botón Comunicación dentro de la VLAN y en el botón Reproducir para que comience la animación.

Comunicación dentro de la VLAN

En la figura, la PC1 desea comunicarse con otro dispositivo, la PC4. La PC1 y la PC4 se encuentran en la VLAN 10. La comunicación con un dispositivo en la misma VLAN se denomina comunicación inter VLAN. A continuación se describe cómo se realiza este proceso:

Paso 1. La PC1 en la VLAN 10 envía su trama de petición ARP (broadcast) al switch S2. Los switches S2 y S1 envían la trama de petición ARP a todos los puertos en la VLAN 10. El switch S3 envía la petición ARP al puerto F0/11 para la PC4 en la VLAN 10.

Paso 2. Los switches en la red envían la trama de respuesta ARP (unicast) a todos los puertos configurados para la VLAN 10. La PC1 recibe la respuesta que contiene la dirección MAC de la PC4.

Paso 3. Ahora la PC1 tiene la dirección MAC de destino de la PC4 y la utiliza para crear una trama unicast con la dirección MAC de la PC4 como destino. Los switches S2, S1 y S3 envían la trama a la PC4.

Haga clic en el botón Comunicación entre VLAN y en el ícono reproducir para que comience la animación.

Comunicación entre VLAN

En la figura, la PC1 en la VLAN 10 desea comunicarse con la PC5 en la VLAN 20. La comunicación con un dispositivo en otra VLAN se denomina comunicación entre VLAN.

Nota: Existen dos conexiones desde el switch S1 hasta el router: una para enviar transmisiones enla VLAN 10 y la otra para enviar transmisiones en la VLAN 20 hacia la interfaz del router.

A continuación se describe cómo se realiza este proceso:

Paso 1. La PC1 en la VLAN 10 desea comunicarse con la PC5 en la VLAN 20. La PC1 envía una trama de petición ARP para la dirección MAC del gateway predeterminado R1.

Paso 2. El router R1 responde con una trama de respuesta ARP desde su interfaz configurada en la VLAN 10.

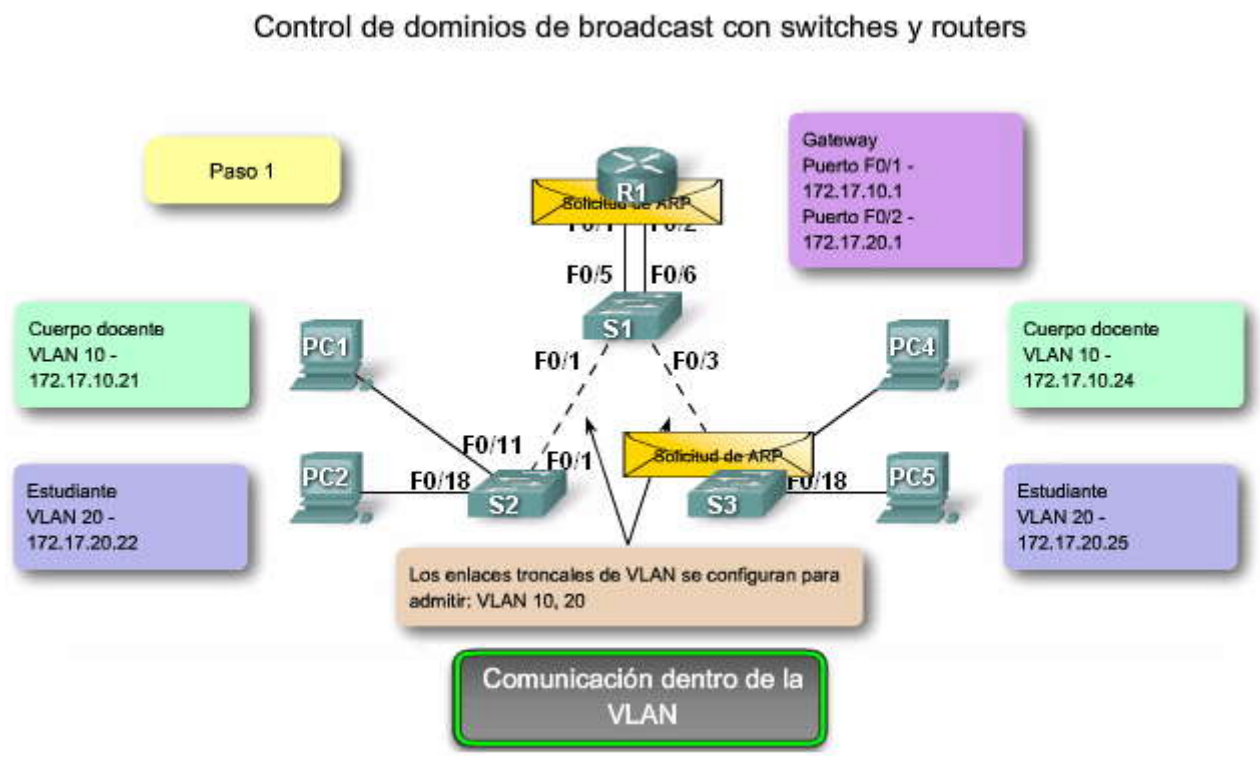
Todos los switches envían la trama de respuesta ARP y la PC1 la recibe. La respuesta ARP contiene la dirección MAC del gateway predeterminado.

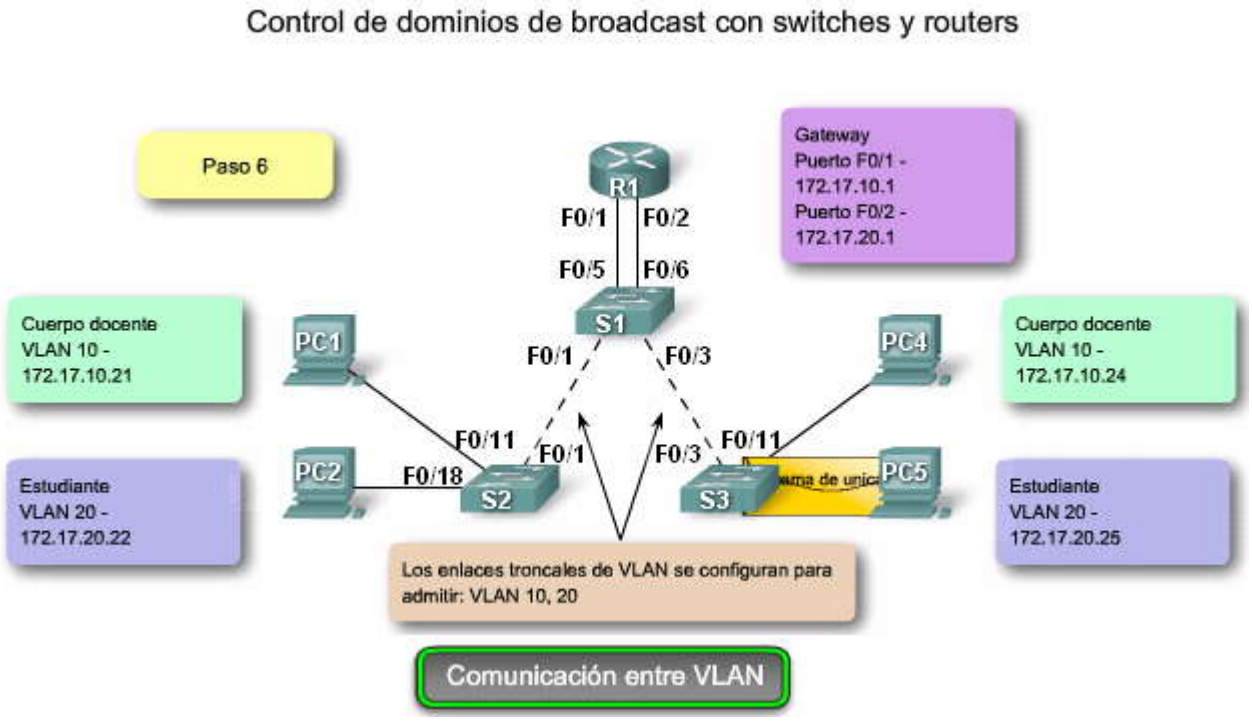
Paso 3. La PC1 crea, entonces, una trama de Ethernet con la dirección MAC del Gateway predeterminado. La trama se envía desde el switch S2 al S1.

Paso 4. El router R1 envía una trama de petición ARP en la VLAN 20 para determinar la dirección MAC de la PC5. Los switches S1, S2 y S3, emiten la trama de petición ARP a los puertos configurados para la VLAN 20. La PC5 en la VLAN 20 recibe la trama de petición ARP del router R1.

Paso 5. La PC5 en la VLAN 20 envía una trama de respuesta ARP al switch S3. Los switches S3 y S1 envían la trama de respuesta ARP al router R1 con la dirección MAC de destino de la interfaz F0/2 en el router R1.

Paso 6. El router R1 envía la trama recibida de la PC1 a S1 y S3 a la PC5 (en la vlan 20).





Control de dominios de broadcast con las VLAN y reenvío de capa 3

En el último capítulo, usted aprendió sobre algunas de las diferencias entre los switches de Capa 2 y Capa 3. La figura muestra el switch Catalyst 3750G-24PS, uno de los tantos switches de Cisco que admite el enrutamiento de Capa 3. El ícono que representa el switch de Capa 3 se visualiza. La explicación sobre la conmutación de la Capa 3 excede el alcance de este curso, pero es útil una breve descripción de la tecnología de interfaz virtual del switch (SVI, por su sigla en inglés) que permite al switch de Capa 3 enrutar transmisiones entre las VLAN.

SVI

SVI es una interfaz lógica configurada para una VLAN específica. Es necesario configurar una SVI para una VLANsi desea enrutar entre las VLAN o para proporcionar conectividad de host IP al switch. De manera predeterminada, una SVI se crea por la VLAN predeterminada (VLAN 1) para permitir la administración de switch remota.

Haga clic en el botón Ejemplo de Reenvío de Capa 3 en la figura para ver la animación que presenta una representación simplificada de cómo un switch de Capa 3 controla dominios de broadcast.

Reenvío de capa 3

Un switch de Capa 3 tiene la capacidad de enrutar transmisiones entre las VLAN. El procedimiento es el mismo que se describió para la comunicación entre VLAN utilizando un router distinto, excepto que las SVI actúan como las interfaces del router para enrutar los datos entre las VLAN. La animación describe este proceso.

En la animación, la PC1 desea comunicarse con la PC5. Los siguientes pasos detallan la comunicación a través del switch S1 de Capa 3:

Paso 1. La PC1 envía un broadcast de petición ARP en la VLAN10. S2 envía la petición ARP a todos los puertos configurados para la VLAN 10.

Paso 2. El switch S1 envía la petición ARP a todos los puertos configurados para la VLAN 10, incluida la SVI para la VLAN 10. El switch S3 envía la petición ARP a todos los puertos configurados para la VLAN 10.

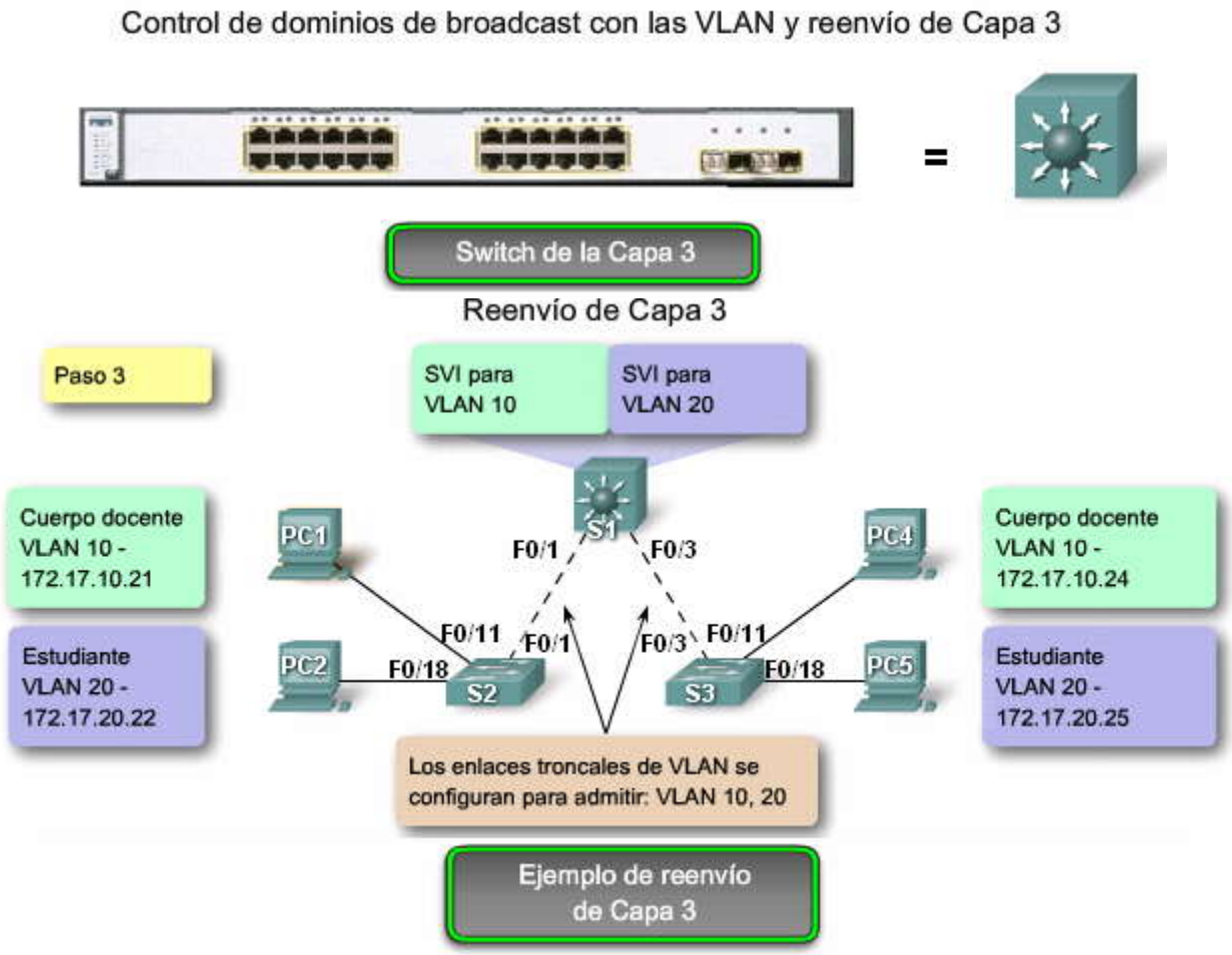
Paso 3. La SVI para la VLAN 10 en el switch S1 conoce la ubicación de la VLAN 20. La SVI para la VLAN 10 en el switch S1 envía una respuesta ARP de vuelta a la PC1 con esta información.

Paso 4. La PC 1 envía datos, destinados a la PC5, como trama de unicast a través del switch S2 a la SVI para la VLAN 10 en el switch S1.

Paso 5. La SVI para la VLAN 20 envía un broadcast de petición ARP a todos los puertos de switch configurados para la VLAN 20. El switch S3 envía ese broadcast de petición ARP a todos los puertos de switch configurados para la VIAN 20.

Paso 6. La PC5 en la VLAN 20 envía una respuesta ARP. El switch S3 envía esa respuesta ARP a S1. El switch S1 envía la respuesta ARP a la SVI para la VLAN 20.

Paso 7. La SVI para la VLAN 20 envía los datos enviados desde la PC1 en una trama de unicast a la PC5, mediante la utilización de la dirección de destino que obtuvo de la respuesta ARP en el paso 6.



3.2 ENLACE TRONCAL DE LAS VLAN.-

3.2.1 ENLACES TRONCALES DE LA VLAN.-

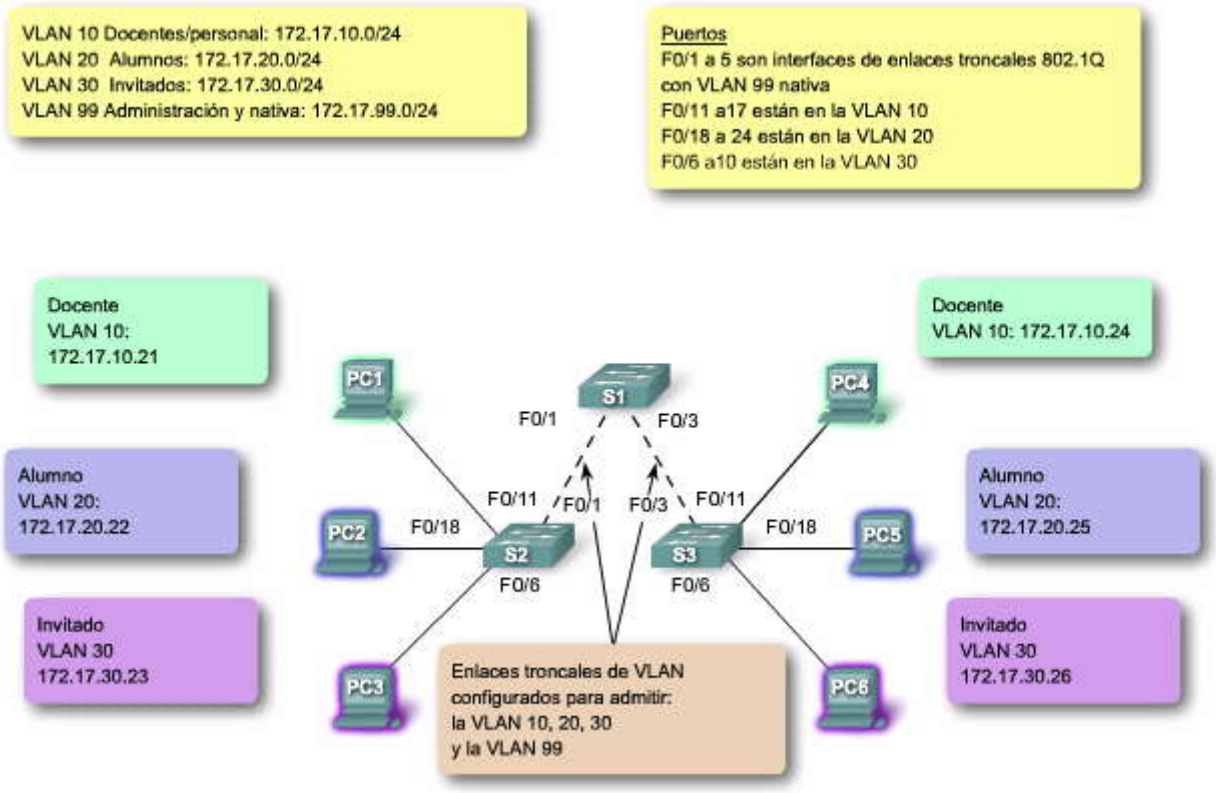
¿Qué es un enlace troncal?

Es difícil describir las VLAN sin mencionar los enlaces troncales de la VLAN. Aprendió acerca de controlar broadcasts de la red con segmentación de la VLAN y observó la manera en que los enlaces troncales de la VLAN transmitieron tráfico a diferentes partes de la red configurada en una VLAN. En la figura, los enlaces entre los switches S1 y S2 y entre S1 y S3 están configurados para transmitir el tráfico que proviene de las VLAN 10, 20, 30 y 99. Es posible que esta red no funcione sin los enlaces troncales de la VLAN. El usuario descubrirá que la mayoría de las redes que encuentra están configuradas con enlaces troncales de la VLAN. Esta sección une su conocimiento previo sobre el enlace troncal de la VLAN y proporciona los detalles necesarios para poder configurar el enlace troncal de la VLAN en una red.

Definición de enlace troncal de la VLAN

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Más adelante en esta sección, aprenderá acerca de 802.1Q.

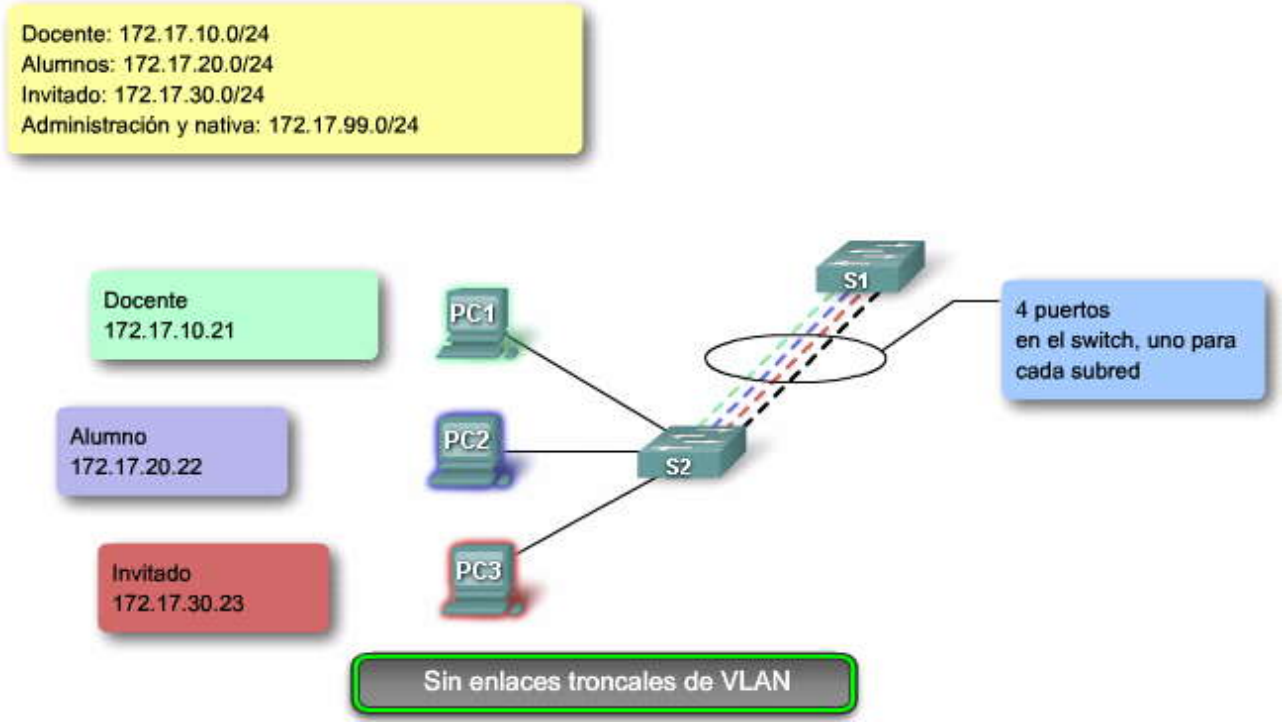
Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

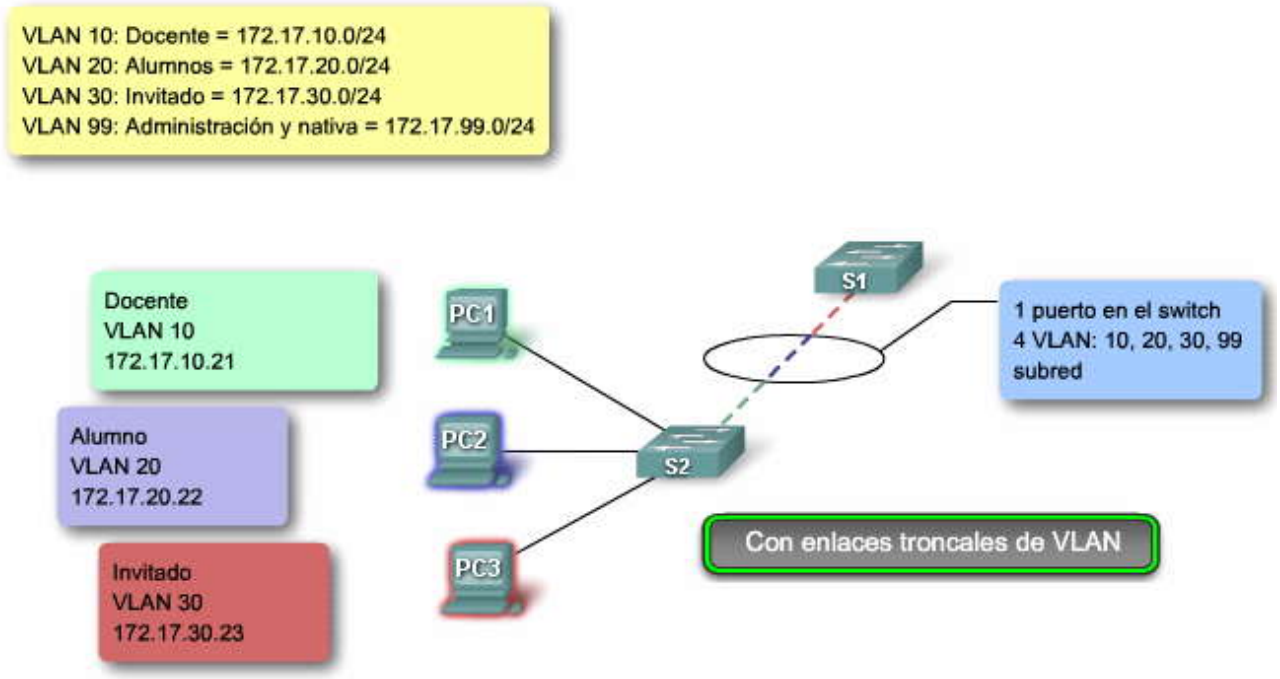


¿Cuál es el problema que resuelve un enlace troncal?
En la figura, se observa que la topología estándar utilizada en este capítulo, excepto en lugar del enlace troncal de la VLAN que el usuario está acostumbrado a ver entre los switches S1 y S2, hay un enlace individual para cada subred. Hay cuatro enlaces individuales que conectan los switches S1 y S2, lo que deja tres puertos menos para asignar a dispositivos de usuario final. Cada vez que se tiene en cuenta una subred nueva, se necesita un nuevo enlace para cada switch en la red.

Haga clic en el botón Con enlaces troncales de VLAN en la figura.

En la figura, la topología de red muestra un enlace troncal de la VLAN que conecta los switches S1 y S2 con un enlace físico único. Esta es la forma en que debe configurarse una red.





Etiquetado de trama 802.1Q

Recuerde que los switches son dispositivos de capa 2. Sólo utilizan la información del encabezado de trama de Ethernet para enviar paquetes. El encabezado de trama no contiene la información que indique a qué VLAN pertenece la trama. Posteriormente, cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q. Este encabezado agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama.

El etiquetado de la trama se mencionó en diferentes oportunidades. La primera vez se hizo en referencia a la configuración del modo de voz en un puerto de switch. En esa sección aprendió que una vez que se configura, un teléfono de Cisco (que incluye un switch pequeño) etiqueta las tramas de voz con un ID de VLAN. También aprendió que los ID de VLAN pueden estar en un rango normal, 1-1005 y en un rango ampliado, 1006-4094. ¿De qué manera se insertan los ID de la VLAN en la trama?

Descripción general del etiquetado de la trama de la VLAN

Antes de explorar los detalles de una trama 802.1Q, es útil comprender lo que hace un switch al enviar una trama a un enlace troncal. Cuando el switch recibe una trama en un puerto configurado en modo de acceso con una VLAN estática, el switch quita la trama e inserta una etiqueta de VLAN, vuelve a calcular la FCS y envía la trama etiquetada a un puerto de enlace troncal.

Nota: Más adelante, en esta sección, se presenta una animación de la operación de enlace troncal..

Detalles del campo de etiqueta de VLAN

El campo de etiqueta de la VLAN consiste de un campo EtherType, un campo deinformación de control de etiqueta y del campo de FCS.

Campo EtherType

Establecido al valor hexadecimal de 0x8100. Este valor se denomina valor de ID de protocolo de etiqueta (TPID, por su sigla en inglés). Con el campo EtherType configurado al valor TPID, el switch que recibe la trama sabe buscar la información en el campo de información de control de etiqueta.

Campo Información de control de etiqueta

El campo de información de control de etiqueta contiene:

- **3 bits de prioridad del usuario:** utilizado por el estándar 802.1p, que especifica cómo proporcionar transmisión acelerada de las tramas de la Capa 2. Una descripción de IEEE 802.1p está más allá del alcance de este curso; sin embargo el usuario aprendió algo sobre esto anteriormente en el análisis sobre las VLAN de voz.

- **1 bit de Identificador de formato ideal (CFI, por su sigla en inglés):** permite que las tramas Token Ring se transporten con facilidad a través de los enlaces Ethernet.
- **12 bits del ID de la VLAN (VID):** números de identificación de la VLAN; admite hasta 4096 ID de VLAN.

Campo FCS

Luego de que el switch inserta los campos de información de control de etiqueta y EtherType, vuelve a calcular los valores FCS y los inserta en la trama.

VLAN nativas y enlace troncal 802.1Q

Ahora que el usuario sabe más acerca de cómo un switch etiqueta una trama con la VLAN adecuada, es momento de explorar la manera en que la VLAN nativa admite el switch en el manejo de tramas etiquetadas y sin etiquetar que llegan en un puerto de enlace troncal 802.1Q.

Tramas etiquetadas en la VLAN nativa

Algunos dispositivos que admiten enlaces troncales etiquetan la VLAN nativa como comportamiento predeterminado. El tráfico de control enviado en la VLAN nativa debe estar sin etiquetar. Si un puerto de enlace troncal 802.1Q recibe una trama etiquetada en la VLAN nativa, éste descarta la trama. Como consecuencia, al configurar un puerto de switch en un switch Cisco, es necesario identificar estos dispositivos y configurarlos de manera que no envíen tramas etiquetadasen la VLAN nativa. Los dispositivos de otros proveedores que admiten tramas etiquetadas en la VLAN nativa incluyen: teléfonos IP, servidores, routers y switches que no pertenecen a Cisco.

Tramas sin etiquetar en la VLAN nativa

Cuando un puerto de enlace troncal de switch Cisco recibe tramas sin etiquetar, éste envía esas tramas a la VLAN nativa. Como debe recordar, la VLAN nativa predeterminada es la VLAN 1. Al configurar un puerto de enlace troncal 802.1Q, se asigna el valor del ID de la VLAN nativa al ID de la VLAN de puerto predeterminado (PVID). Todo el tráfico sin etiquetar que ingresa o sale del puerto 802.1Q se envía en base al valor del PVID. Por ejemplo: si la VLAN 99 se configura como la VLAN nativa, el PVID es 99 y todo el tráfico sin etiquetar se envía a la VLAN 99. Si la VLAN nativa no ha sido configurada nuevamente, el valor de PVID se configura para la VLAN 1.

Haga clic en el botón Ejemplo de configuración de la VLAN nativa que se muestra en la figura.

En este ejemplo, la VLAN 99 se configura como VLAN nativa en el puerto F0/1 en el switch S1. Este ejemplo muestra cómo volver a configurar la VLAN nativa desde su configuración predeterminada de la VLAN 1.

Comenzando en el modo EXEC privilegiado, la figura describe la manera de configurar la VLAN nativa en el puerto F0/1 en el switch S1 como un enlace troncal IEEE 802.1Q con la VLAN 99 nativa.

Haga clic en el botón Verificación de la VLAN nativa en la figura.

Al utilizar el comando **show interfaces interface-id switchport** puede verificar rápidamente si ha vuelto a configurar la VLAN nativa desde la VLAN 1 a la VLAN 99 de manera correcta. El resultado resaltado en la captura de pantalla indica que la configuración fue un éxito.

VLAN Nativas y Enlace troncal 802.1Q

Tramas con etiquetas en la VLAN nativa

- Descartadas por el switch
- Los dispositivos no deben etiquetar el tráfico de control destinado a la VLAN nativa

Tramas sin etiquetas en la VLAN nativa

- Tienen su PVID modificado al valor de la VLAN nativa configurada
- Permanece sin etiquetar
- Son reenviadas en la VLAN nativa configurada

Tramas con y sin etiquetas

VLAN Nativas y Enlace troncal 802.1Q

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global en el switch S1.	`S1#configure terminal`
Ingresar el modo de configuración de interfaz.	`S1(config)#interface F0/1`
Definir la interfaz F0/1 como un enlace troncal IEEE 802.1Q.	`S1(config-if)#switchport mode trunk`
Configurar la VLAN 99 para que sea la VLAN nativa.	`S1(config-if)#switchport trunk native vlan 99`
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

Ejemplo de configuración de la VLAN nativa

VLAN Nativas y Enlace troncal 802.1Q

```
S1#show interfaces F0/1 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 50
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
…
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
…
Trunking VLANs Enabled: ALL
```

El tres en "..." en el resultado en pantalla indica que se eliminó contenido para una mayor claridad.

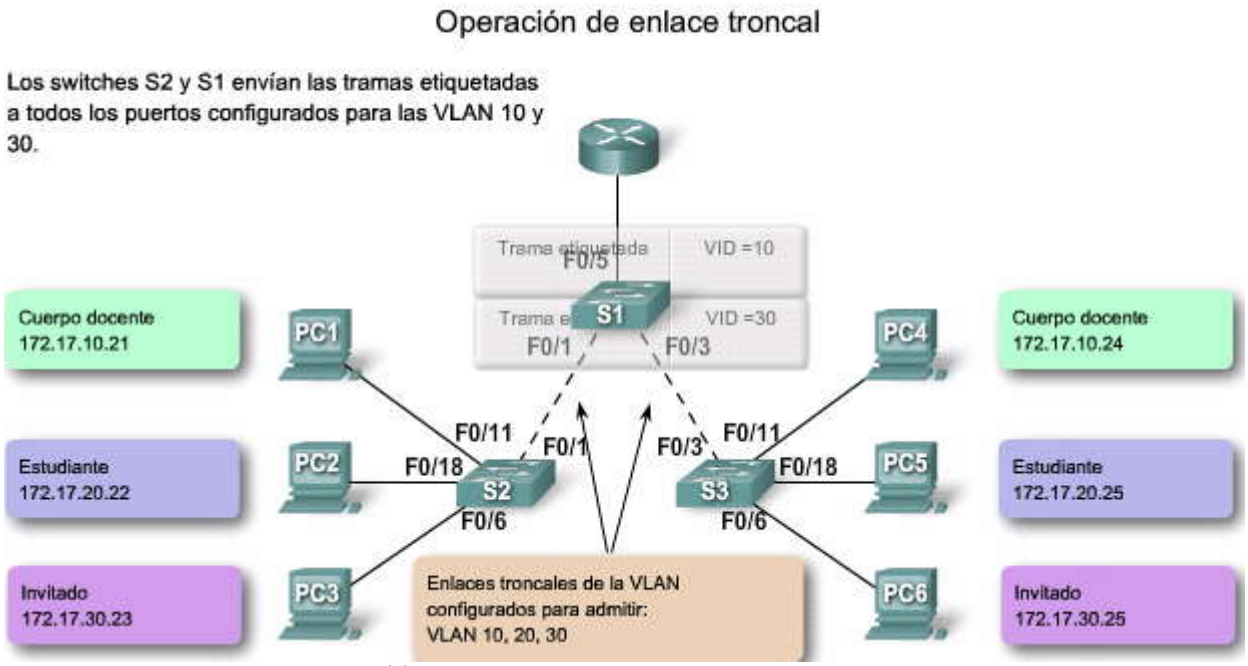
Verificación de la VLAN nativa

3.2.2 OPERACIÓN DE ENLACE TRONCAL.-

Enlace troncal en acción

El usuario ha aprendido la manera en que un switch maneja el tráfico sin etiquetar en un enlace troncal. El usuario sabe que las tramas que atraviesan un enlace troncal están etiquetadas con el ID de la VLAN del puerto de acceso donde llegó la trama. En la figura, la PC1 en la VLAN 10 y la PC3 en la VLAN 30 envían tramas de broadcast al switch S2. El switch S2 etiqueta esas tramas con el ID adecuado de la VLAN y luego envía las tramas a través del enlace troncal al switch S1. El switch S1 lee el ID de la VLAN en las tramas y los envía en broadcast a cada puerto configurado para admitir la VLAN 10 y la VLAN 30. El switch S3 recibe esas tramas, quita los ID de la VLAN y los envía como tramas sin etiquetar a la PC4 en la VLAN 10 y a la PC 6 en la VLAN 30.

Haga clic en el botón Reproducir en la barra de herramientas de la animación en la figura.



3.2.3 MODOS DE ENLACES TRONCALES.-

El usuario ha aprendido la manera en que el enlace troncal 802.1Q funciona en los puertos de switch de Cisco. Ahora es momento de examinar las opciones de configuración del modo de puerto de enlace troncal 802.1Q. Primero, es necesario analizar un protocolo de enlace troncal anterior de Cisco denominado enlace entre switch (ISL, Inter-Switch Link), debido a que verá esta opción en las guías de configuración de software del switch.

IEEE, no ISL

Aunque se puede configurar un switch de Cisco para admitir dos tipos de puertos de enlace troncal, IEEE 802.1Q e ISL; en la actualidad, sólo se usa el 802.1Q. Sin embargo, las redes antiguas siguen usando ISL, y es útil aprender sobre cada tipo de puerto de enlace troncal.

- Un puerto de enlace troncal IEEE 802.1Q admite tráfico simultáneo etiquetado y sin etiquetar. A un puerto de enlace troncal 802.1Q se le asigna un PVID predeterminado y todo el tráfico sin etiquetar se transporta en el PVID predeterminado del puerto. Se supone que todo el tráfico etiquetado y sin etiquetar con un ID nulo de la VLAN pertenece al PVID predeterminado del puerto. El paquete con un ID de VLAN igual al PVID predeterminado del puerto de salida se envía sin etiquetar. El resto del tráfico se envía con una etiqueta de VLAN.
- En un puerto de enlace troncal ISL se espera que todos los paquetes recibidos sean encapsulados con un encabezado ISL y que todos los paquetes transmitidos se envíen con un encabezado ISL. Las tramas nativas (sin etiquetar) recibidas de un puerto de enlace troncal ISL se descartan. ISL ya no es un modo de puerto de enlace troncal recomendado y no se admite en varios de los switches de Cisco.

DTP

El protocolo de enlace troncal dinámico (DTP) es un protocolo propiedad de Cisco. Los switches de otros proveedores no admiten el DTP. El DTP es habilitado automáticamente en un puerto de switch cuando algunos modos de enlace troncal se configuran en el puerto de switch.

El DTP administra la negociación de enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP. El DTP admite los enlaces troncales ISL y 802.1Q. Este curso se concentra en la implementación de 802.1Q del DTP. Un análisis detallado sobre el DTP está más allá de este curso, sin embargo aprenderá sobre esto en las prácticas de laboratorio y actividades asociadas con este capítulo. Los switches no necesitan que el DTP realice enlaces troncales, y algunos switches y routers de Cisco no admiten al DTP. Para aprender más sobre la admisión de DTP en switches de Cisco, visite:
http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a008017f86a.shtml.

Modos de enlaces troncales

Un puerto de switch en un switch de Cisco admite varios modos de enlaces troncales. El modo de enlace troncal define la manera en la que el puerto negocia mediante la utilización del DTP para configurar un enlace troncal con su puerto par. A continuación, se observa una breve descripción de los modos de enlaces troncales disponibles y la manera en que el DTP se implementa en cada uno.

Activado (de manera predeterminada)

El puerto del switch envía periódicamente tramas de DTP, denominadas notificaciones, al puerto remoto. El comando utilizado es switchport mode trunk. El puerto de switch local notifica al puerto remoto que está cambiando dinámicamente a un estado de enlace troncal. Luego, el puerto local, sin importar la información de DTP que el puerto remoto envía como respuesta a la notificación, cambia al estado de enlace troncal. El puerto local se considera que está en un estado de enlace troncal (siempre activado) incondicional.

Dinámico automático

El puerto del switch envía periódicamente tramas de DTP al puerto remoto. El comando utilizado es switchport mode dynamic auto. El puerto de switch local notifica al puerto de switch remoto que puede establecer enlaces troncales pero no solicita pasar al estado de enlace troncal. Luego de una negociación de DTP, el puerto local termina en estado de enlace troncal sólo si el modo de enlace troncal del puerto remoto ha sido configurado para estar activo o si es conveniente. Si ambos puertos en los switches se configuran en automático, no negocian para estar en un estado de enlace troncal. Negocian para estar en estado de modo de acceso (sin enlace troncal).

Las tramas de DTP convenientes y dinámicas

Las tramas de DTP se envían periódicamente al puerto remoto. El comando utilizado es switchport mode dynamic desirable. El puerto de switch local notifica al puerto de switch remoto que puede establecer enlaces troncales y solicita al puerto de switch remoto pasar al estado de enlace troncal. Si el puerto local detecta que el remoto ha sido configurado en modo activado, conveniente o automático, el puerto local termina en estado de enlace troncal. Si el puerto de switch remoto está en modo sin negociación, el puerto de switch local permanece como puerto sin enlace troncal.

Desactivación del DTP

Puede desactivar el DTP para el enlace troncal para que el puerto local no envíe tramas de DTP al puerto remoto. Utilice el comando switchport nonegotiate. Entonces el puerto local se considera que está en un estado de enlace troncal incondicional. Utilice esta característica cuando necesite configurar un enlace troncal con un switch de otro proveedor.

Ejemplo de modo de enlace troncal

En la figura, los puertos F0/1 en los switches S1 y S2 se configuran con modo de enlace troncal activado. Los puertos F0/3 en los switches S1 y S3 se configuran para que estén en modo de enlace troncal automático. Cuando se completen las configuraciones de switch y los switches están configurados por completo, ¿Qué enlace se configurará como enlace troncal?

Haga clic en el botón ¿Qué enlace se configurará como enlace troncal? en la figura.

El enlace entre los switches S1 y S2 se convierte en enlace troncal porque los puertos F0/1 en los switches S1 y S2 se configuran para ignorar todas las notificaciones del DTP y aparecen y permanecen en modo de puerto de enlace troncal. Los puertos F0/3 en los switches S1 y S3 se establecen en automático, entonces negocian para estar en estado predeterminado, el estado de modo de acceso (sin enlace troncal). Esto da por resultado un enlace troncal inactivo. Cuando configura un puerto de enlace troncal para que esté en modo de puerto de enlace troncal, no existe ambigüedad sobre en qué estado se encuentra el enlace troncal: está siempre activo. Además, es fácil recordar en qué estado están los puertos de enlaces troncales: si se supone que el puerto es un enlace troncal, el modo de enlace troncal es activo..

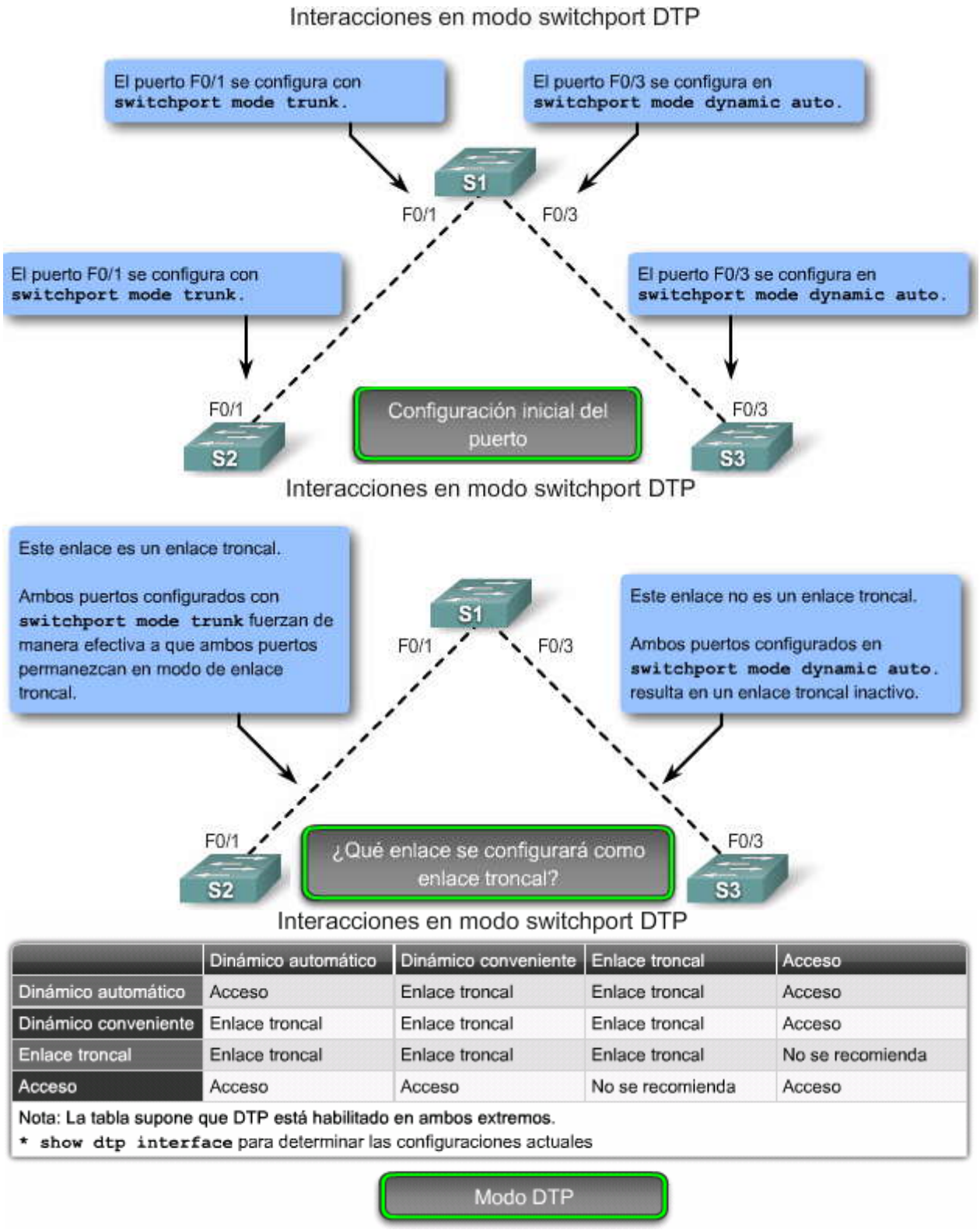
Nota: El modo switchport predeterminado para una interfaz en un switch Catalyst 2950 es conveniente y dinámico, pero el modo switchport predeterminado para una interfaz en un switch Catalyst 2960 es automático y dinámico. Si S1 y S3 fueran

switches Catalyst 2950 con interfaz F0/3 en modo switchport predeterminado, el enlace entre S1 y S3 se convertiría en un enlace troncal activo.

Haga clic en el botón Modo DTP en la figura para revisar las interacciones de los modos.

Para obtener más información acerca de qué switches Cisco admiten 802.1Q, ISL y DTP, visite: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a008017f86a.shtml#topic1.

Para obtener más información acerca de cómo admitir ISL en redes antiguas, visite: http://www.cisco.com/en/US/tech/tk389/tk689/tsd_technology_support_troubleshooting_technotes_list.html.



	Dinámico automático	Dinámico conveniente	Enlace troncal	Acceso
Dinámico automático	Acceso	Enlace troncal	Enlace troncal	Acceso
Dinámico conveniente	Enlace troncal	Enlace troncal	Enlace troncal	Acceso
Enlace troncal	Enlace troncal	Enlace troncal	Enlace troncal	No se recomienda
Acceso	Acceso	Acceso	No se recomienda	Acceso

Nota: La tabla supone que DTP está habilitado en ambos extremos.
* `show dtp interface` para determinar las configuraciones actuales

Modo DTP

3.3 CONFIRUGACIÓN DE LAS VLAN Y ENLACES TRONCALES.-

3.3.1 DECRIPCIÓN GENERAL DE LA CONFIGURACIÓN DE LAS VLAN Y DE LOS TRONCALES

En este capítulo, ha visto ejemplos de los comandos utilizados para configurar las VLAN y los enlaces troncales de las VLAN. En esta sección aprenderá sobre los comandos clave IOS de Cisco necesarios para crear, eliminar y verificar las VLAN y los enlaces troncales de las VLAN. Por lo general, estos comandos poseen muchos parámetros opcionales que extienden las capacidades de la tecnología de las VLAN y enlaces troncales de las VLAN. Estos comandos opcionales no se presentan; sin embargo, se suministran referencias en caso de que desee investigar estas opciones. Esta sección se enfoca en suministrarle las habilidades y conocimientos necesarios para configurar las VLAN y los enlaces troncales de la VLAN con sus características clave.

En esta sección, se muestra la sintaxis de configuración y verificación para un lado de la VLAN o del enlace troncal. En las prácticas de laboratorio y actividades configurará ambos lados y verificará que el enlace (VLAN o enlace troncal de VLAN) esté configurado correctamente.

Nota: Si desea mantener la configuración activa recién configurada, debe guardarla en la configuración de inicio.

Descripción general de la configuración de las VLAN y los enlaces troncales

Utilice los siguientes pasos para configurar y verificar las VLAN y los enlaces troncales en una red conmutada:

1. Crear las VLAN.
2. Asignar puertos de switch a las VLAN de manera estática
3. Verificar la configuración de la VLAN.
4. Activar el enlace troncal en las conexiones entre switches.
5. Verificar la configuración del enlace troncal.

3.3.2 CONFIGURACION DE UNA VLAN.-

Agregue una VLAN

En este tema, aprenderá a crear una VLAN estática en un switch Cisco Catalyst mediante el modo de configuración global de la VLAN. Existen dos modos diferentes para configurar las VLAN en un switch Cisco Catalyst: modo de configuración de base de datos y modo de configuración global. A pesar de que la documentación de Cisco menciona el modo de configuración de base de datos de la VLAN, se elimina a favor del modo de configuración global de la VLAN.

El usuario configurará las VLAN con los ID en el rango normal. Recuerde que existen dos rangos de ID de la VLAN. El rango normal incluye los ID 1 a 1001 y el rango ampliado consiste de los ID 1006 a 4094. VLAN 1 y 1002 a 1005 son números de ID reservados. Cuando configura las VLAN de rango normal, los detalles de configuración se almacenan automáticamente en la memoria flash del switch en un archivo llamado vlan.dat. Debido a que el usuario configura frecuentemente otros aspectos de un switch Cisco al mismo tiempo, es una buena práctica guardar los cambios de la configuración activa en la configuración de inicio.

Haga clic en el botón Sintaxis del comando en la figura.

La figura revisa los comandos IOS de Cisco utilizados para agregar una VLAN a un switch.

Haga clic en el botón Ejemplo en la figura.

La figura muestra cómo se configura la VLAN estudiante, VLAN 20 en el switch S1. En el ejemplo de topología, la computadora del estudiante, la PC2, aún no es una VLAN, pero tiene una dirección IP de 172.17.20.22.

Haga clic en el botón Verificación en la figura.

La figura muestra un ejemplo de uso del comando show vlan brief para mostrar los contenidos del archivo vlan.dat. En la captura de pantalla se resalta la VLAN del estudiante, VLAN 20. Los ID de VLAN predeterminada 1 y 1002 a 1005 se muestran en los resultados que aparecen en pantalla.

Nota: Además de ingresar un ID simple de VLAN, el usuario puede ingresar una serie de ID de VLAN separada por comas o un rango de ID de VLAN separado por guiones, usando el comando vlan vlan-id, por ejemplo: switch(config)#vlan 100,102,105-107.

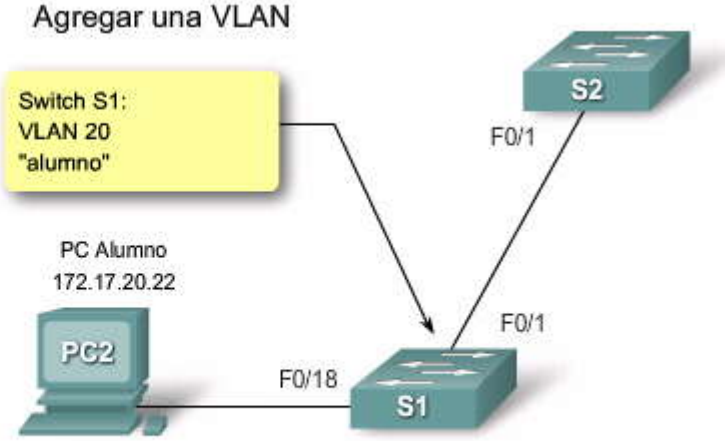
Agregar una VLAN

Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Crear una VLAN. El id de la VLAN es el número de VLAN que se creará. Switches para el modo de configuración de VLAN para el vlan id de la VLAN.	`S1(config)#vlan vlan id`
(Opcional) Especificar un único nombre de VLAN para identificar la misma. Si no se ingresa ningún nombre, el número de la VLAN, relleno con ceros, se anexa a la palabra 'VLAN', por ejemplo, VLAN0020.	`S1(config-vlan)#name Nombre de VLAN`
Volver a modo EXEC privilegiado. Debe finalizar su sesión de configuración para que la configuración se guarde en el archivo vlan.dat y para que la configuración entre en vigencia.	`S1(config-vlan)#end`

Sintaxis del comando

Agregar una VLAN

```
S1#configure terminal
S1(config)#vlan 20
S1(config-vlan)#name alumno
S1(config-vlan)#end
```



Ejemplo

Agregar una VLAN

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
20   student                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup


S1#conf t
```

Verificación

Asignación de un puerto de switch
Después de crear una VLAN, asígnele un puerto o más. Cuando asigna un puerto de switch a una VLAN en forma manual, se lo conoce como puerto de acceso estático. Un puerto de acceso estático puede pertenecer a sólo una VLAN por vez.

Haga clic en el botón Sintaxis del comando en la figura para revisar los comandos IOS de Cisco para asignar un puerto de acceso estático a la VLAN.

Haga clic en el botón Ejemplo en la figura para ver cómo la VLAN del estudiante, VLAN 20, se asigna estáticamente al puerto F0/18 en el switch S1. El puerto F0/18 se ha asignado a la VLAN 20, de manera que la computadora del estudiante, PC2, está en la VLAN 20. Cuando la VLAN 20 se configura en otros switches, el administrador de red sabe configurar las otras computadoras de estudiantes para encontrarse en la misma subred que PC2: 172.17.20.0 /24.

Haga clic en el botón Verificación en la figura para confirmar que el comando show vlan brief muestra los contenidos del archivo vlan.dat. En la captura de pantalla se resalta la VLAN del estudiante, VLAN 20.

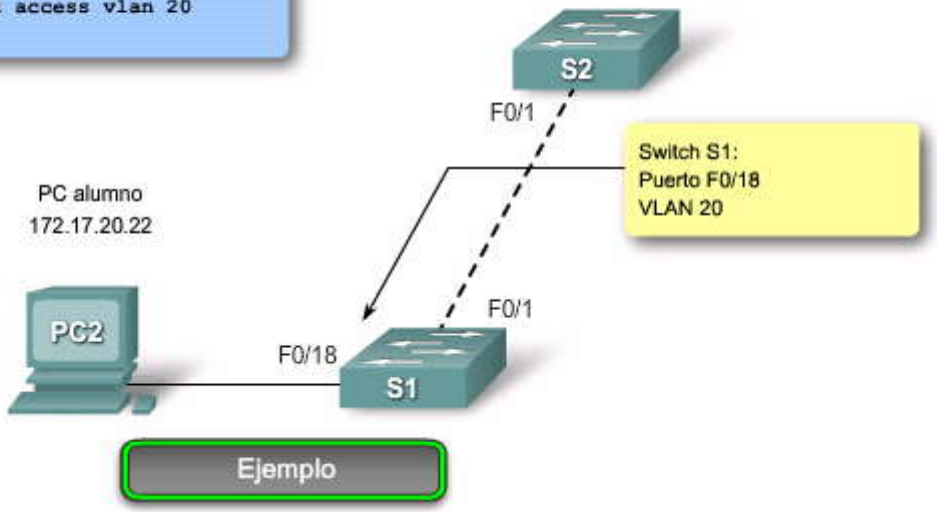
Asignar un puerto de switch

Sintaxis del comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	`S1#configure terminal`
Ingresar la interfaz para asignar la VLAN.	`S1(config)#interface` *interface id*
Definir el modo de asociación de VLAN para el puerto.	`S1(config-if)#switchport mode access`
Asignar el puerto a una VLAN.	`S1(config-if)#switchport access vlan` *vlan id*
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

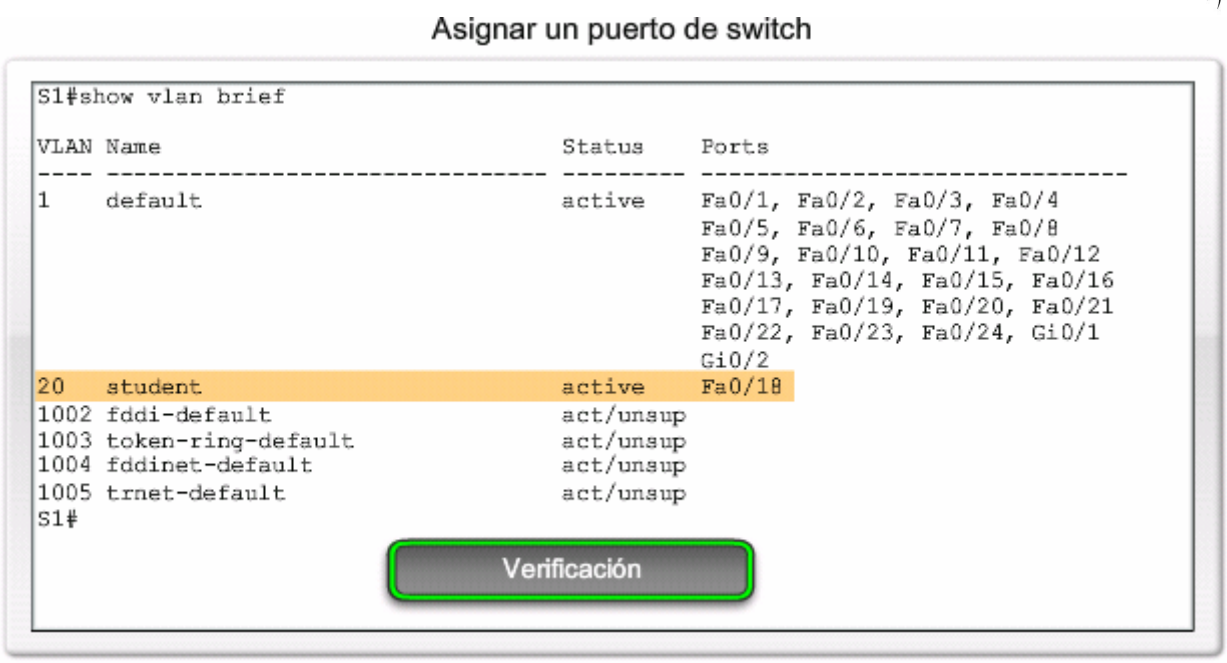
Sintaxis del comando

Asignar un puerto de switch

```
S1#configure terminal
S1(config)#interface F0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#end
```



Ejemplo



3.3.3 ADMINISTRACIÓN DE LAS VLAN.-

Verificación de las vinculaciones de puerto y de las VLAN

Después de configurar la VLAN, puede validar las configuraciones de la VLAN mediante la utilización de los comandos show del IOS de Cisco.

Haga clic en el botón Sintaxis del comando en la figura.

La sintaxis de comando para los diversos comandos show del IOS de Cisco debe conocerse bien. Ya ha utilizado el comando show vlan brief. Se pueden ver ejemplos de estos comandos haciendoclic en los botones de la figura.

Haga clic en el botón Mostrar VLAN en la figura.

En este ejemplo, el usuario puede ver que el comando show vlan name student no produce resultados muy legibles. Aquí se prefiere utilizar el comando show vlan brief. El comando show vlan summary muestra la cuenta de todas las VLAN configuradas. El resultado muestra seis VLAN: 1, 1002-1005 y la VLAN del estudiante, VLAN 20.

Haga clic en el botón Interfaces de VLAN en la figura.

Este comando muestra muchos detalles que exceden el alcance de este capítulo. La información clave aparece en la segunda línea de la captura de pantalla e indica que la VLAN 20 está activa.

Haga clic en el botón Puerto de switch de interfaces en la figura.

Este comando muestra información útil para el usuario. Puede determinar que el puerto F0/18 se asigna a la VLAN 20 y que la VLAN nativa es la VLAN 1. El usuario ha utilizado este comando para revisar la configuración de una VLAN de voz.

Para obtener más detalles acerca de los campos de resultados de los comandos show vlan y show interfaces, visite: http://www.cisco.com/en/US/products/ps6406/products_command_reference_chapter09186a008081874b.html#wp7730585.

Verificación de las vinculaciones de puerto y de las VLAN

Mostrar el comando VLAN

Sintaxis del comando de CLI IOS de Cisco	
show vlan [brief | id *vlan-id* **| name** *Nombre de VLAN* **| summary].**	
Mostrar una línea para cada VLAN con el nombre, estado y los puertos de la VLAN.	**brief**
Mostrar información sobre una sola VLAN identificada por el número de ID de la VLAN. Para la vlan-id, el intervalo es de 1 a 4094.	**id** *vlan-id*
Mostrar información sobre una sola VLAN identificada por el nombre de VLAN. El nombre de la VLAN es una cadena ASCII de 1 a 32 caracteres.	**name** *Nombre de VLAN*
Mostrar el resumen de información de la VLAN.	**resumen**

Mostrar el comando de interfaces

Sintaxis del comando de CLI IOS de Cisco	
show interfaces *[interface-id* **| vlan** *vlan-id]* **| switchport**	
Las interfaces válidas incluyen puertos físicos (incluidos tipo, módulo y número de puerto) y canales de puerto. El intervalo de canales de puerto es de 1 a 6.	*interface-id*
Identificación de VLAN. El intervalo es de 1 a 4094.	**vlan** *vlan-id*
Mostrar el estado de administración y operación de un puerto de conmutación, incluidas las configuraciones de bloqueo y protección del puerto.	**switchport**

Sintaxis del comando

Verificación de las vinculaciones de puerto y de las VLAN

```
S1#show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------
20   student                           active    Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Tr
---- ----- ---------- ----- ------ ------ -------- ---- -------- --
20   enet  100020     1500  -      -      -        -    -        0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------
```

Mostrar VLAN

Verificación de las vinculaciones de puerto y de las VLAN

```
S1#show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia 001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
```

Interfaces de VLAN

Verificación de las vinculaciones de puerto y de las VLAN

```
S1#show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
```

Puerto de switch de interfaces

Vínculos al puerto de administración

Existen varias formas de administrar las VLAN y los vínculos del puerto de VLAN. La figura muestra la sintaxis para el comando no switchport access vlan.

Haga clic en el botón Eliminar la VLAN en la figura.

Reasigne un puerto a la VLAN 1

Para reasignar un puerto a la VLAN 1, el usuario puede usar el comando no switchport access vlan en modo de configuración de interfaz. Examine la salida del comando show vlan brief que aparece inmediatamente a continuación. Note cómo VLAN 20 sigue activa. Sólo se la ha eliminado de la interfaz F0/18. En el comando show interfaces f0/18 switchport, se puede ver que la VLAN de acceso para interfaz F0/18 se ha reestablecido a la VLAN 1.

Haga clic en el botón Reasignar la VLAN en la figura.

Reasigne la VLAN a otro puerto

Un puerto de acceso estático sólo puede tener una VLAN. Con el software IOS de Cisco, no necesita quitar primero un puerto de una VLAN para cambiar su membresía de la VLAN. Cuando reasigna un puerto de acceso estático a una VLAN existente, la VLAN se elimina automáticamente del puerto anterior. En el ejemplo, el puerto F0/11 se reasigna a la VLAN 20.

Administrar la pertenencia al puerto

Sintaxis de comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	`S1#configure terminal`
Ingresar el modo de configuración de interfaz para que se configure la interfaz.	`S1(config)#interface` *interface id*
Eliminar la asignación de VLAN en esa interfaz de puerto de switch y cambiarla a la pertenencia de la VLAN predeterminada de VLAN 1.	`S1(config-if)#no switchport access vlan`
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

Sintaxis del comando

```
S1(config)#interface fa0/18
S1(config-if)#no switchport access vlan
S1(config-if)#end
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3
                                                 Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/9, Fa0/10, Fa0/
                                                 Fa0/13, Fa0/14, Fa0
                                                 Fa0/17, Fa0/18, Fa0
                                                 Fa0/21, Fa0/22, Fa0
                                                 Gi0/1, Gi0/2
20   student                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
```

Eliminar la VLAN

```
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/11
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#end
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
20   student                           active    Fa0/11
```

Reasignar la VLAN

Eliminación de las VLAN

La figura proporciona un ejemplo de uso del comando de configuración global no vlan vlan-id para eliminar la VLAN 20 del sistema. El comando show vlan brief verifica que la VLAN 20 ya no está en el archivo vlan.dat.

Alternativamente, el archivo completo vlan.dat puede eliminarse con el comando delete flash:vlan.dat del modo EXEC privilegiado. Después de que el switch se haya vuelto a cargar, las VLAN configuradas previamente ya no estarán presentes. Esto ubica al switch, en forma efectiva, en "de fábrica de manera predeterminada" con respecto a las configuraciones de la VLAN.

Nota: Antes de eliminar una VLAN, asegúrese de reasignar primero todos los puertos miembro a una VLANdiferente. Todo puerto que no se ha movido a una VLAN activa no puede comunicarse con otras estaciones luego de eliminar la VLAN.

Eliminación de las VLAN

```
S1#show vlan brief

VLAN Name                      Status    Ports
---- ------------------------- --------- -------------------------------
1    default                   active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                         Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                         Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                         Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                         Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                         Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                         Gi0/2
1002 fddi-default              act/unsup
1003 trcrf-default             act/unsup
1004 fddinet-default           act/unsup
1003 trbrf-default             act/unsup
S1#
```

3.3.4 CONFIGURACION DE UN ENLACE TRONCAL.-

Configuración de un enlace troncal 802.1Q

Para configurar un enlace troncal en un puerto de switch, utilice el comando switchport mode trunk. Cuando ingresa al modo enlace troncal, la interfaz cambia al modo permanente de enlace troncal y el puerto ingresa a una negociación de DTP para convertir el vínculo a un vínculo de enlace troncal, por más que la interfaz que la conecta no acepte cambiar. En este curso configurará un enlace troncal utilizando únicamente el comando switchport mode trunk. En la figura se muestra la sintaxis de comando IOS de Cisco para especificar una VLAN nativa diferente a la VLAN 1. En el ejemplo, el usuario configura la VLAN 99 como la VLAN nativa. Se muestra la sintaxis de comando utilizada para admitir una lista de las VLAN en el enlace troncal. En este puerto de enlace troncal, admita las VLAN 10, 20 y 30.

Haga clic en el botón Topología en la figura.

El usuario ya conoce esta topología. Las VLAN 10, 20 y 30 admitirán las computadoras del Cuerpo Docente, del Estudiante y del Invitado : PC1, PC2 y PC3. El puerto F0/1 en el switch S1 se configura como un puerto de enlace troncal para admitir las VLAN 10, 20 y 30. La VLAN 99 se configura como la VLAN nativa.

Haga clic en el botón Ejemplo en la figura.

El ejemplo configura al puerto F0/1 en el switch S1 como puerto de enlace troncal. Éste vuelve a configurar la VLAN nativa como VLAN 99 y agrega las VLAN 10, 20 y 30 como las VLAN admitidas en el puerto F0/1.

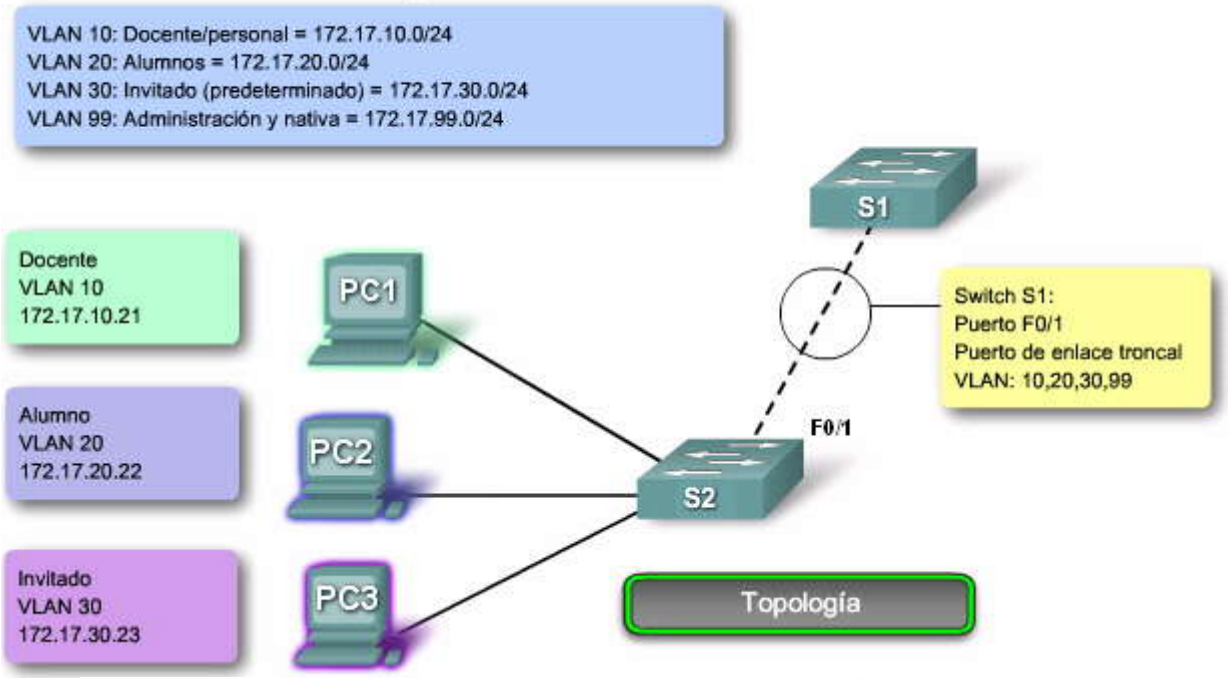
Un análisis sobre el DTP y los detalles de cómo trabaja cada opción de modo de acceso al puerto de switch supera el alcance del curso. Para más detalles sobre los parámetros asociados con el comando de interfaz switchport mode visite: http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_37_se/command/reference/cli3.html#wp1948171.

Configurar un enlace troncal 802.1Q

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global.	S1#configure terminal
Ingresar el modo de configuración de interfaz para la interfaz definida.	S1(config)#interface *interface id*
Hacer que el enlace que conecta los switches sea un enlace troncal.	S1(config-if)#switchport mode trunk
Especificar otra VLAN como la VLAN nativa para los enlaces troncales IEEE 802.1Q sin etiquetar.	S1(config-if)#switchport trunk native vlan *vlan id*
Volver al modo EXEC privilegiado.	S1(config-if)#end

Sintaxis de los comandos

Configurar un enlace troncal 802.1Q



Configurar un enlace troncal 802.1Q

```
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#end
```

Ejemplo

Verificación de la configuración del enlace troncal

La figura muestra la configuración del puerto de switch F0/1 en el switch S1. El comando utilizado es el comando show interfaces interface-ID switchport.

La primera área resaltada muestra que el puerto F0/1 tiene el modo administrativo establecido en Enlace Troncal. El puerto se encuentra en modo de enlace troncal. La siguiente área resaltada verifica que la VLAN nativa sea la VLAN 99, la VLAN de administración. En la parte inferior del resultado, la última área resaltada muestra que las VLAN del enlace troncal habilitadas son las VLAN 10, 20 y 30.

Configuración de un enlace troncal 802.1Q

```
S1#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Administración de una configuración de enlace troncal

En la figura, se muestran los comandos para reestablecer las VLAN admitidas y la VLAN nativa del enlace troncal al estado predeterminado. También se muestra el comando para reestablecer el puerto de switch a un puerto de acceso y, en efecto, eliminar el puerto de enlace troncal.

Haga clic en el botón Restablecer Ejemplo en la figura.

En la figura, los comandos utilizados para reestablecer todas las características de enlace troncal de una interfaz de enlace troncal a las configuraciones predeterminadas, están resaltados en el resultado de muestra. El comando show interfaces f0/1 switchport revela que el enlace troncal se ha reconfigurado a un estado predeterminado.

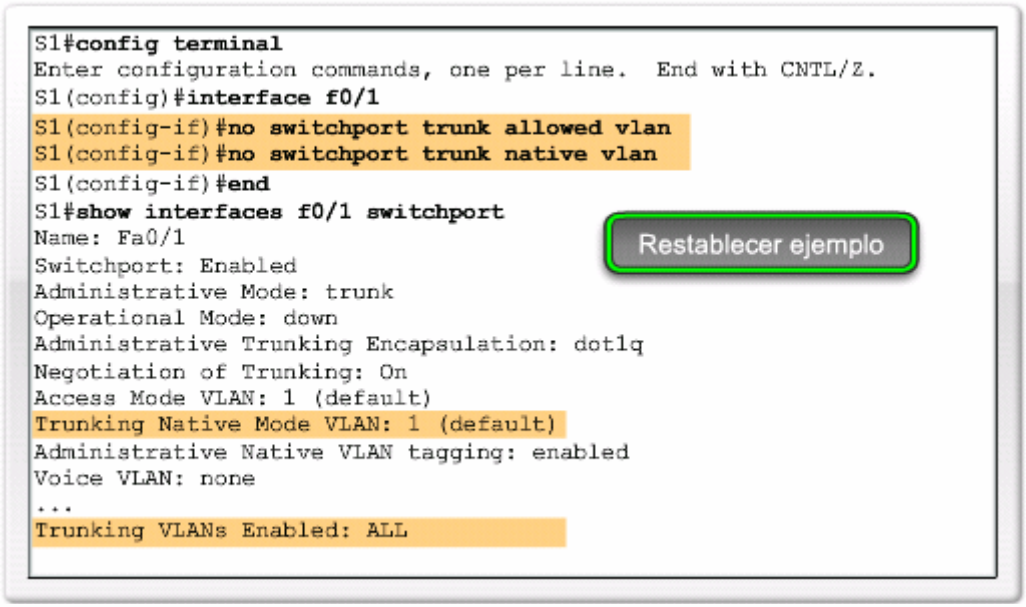
Haga clic en el botón Eliminar Ejemplo en la figura.

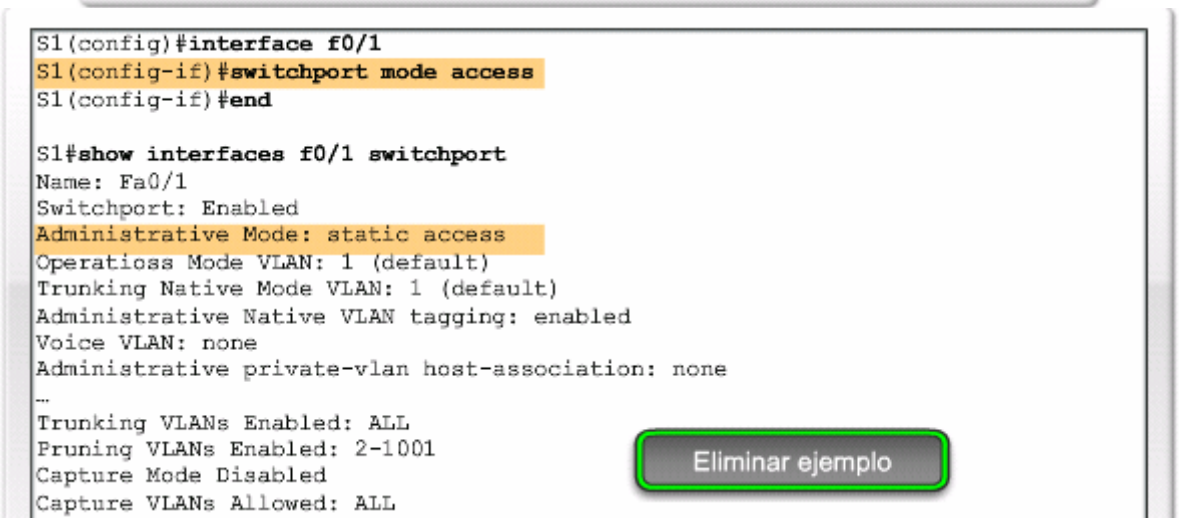
El resultado de la figura muestra los comandos utilizados para eliminar la característica de enlace troncal del puerto de switch F0/1 en el switch S1. El comando show interfaces f0/1 switchport revela que la interfaz F0/1 está ahora en modo de acceso estático.

Administración de una configuración de enlace troncal

Sintaxis de comando de la CLI del IOS de Cisco	
Utilice este comando en el modo de configuración de interfaz para restablecer todas las VLAN configuradas en la interfaz del enlace troncal.	`S1(config-if)#no switchport trunk allowed vlan`
Utilice este comando en el modo de configuración de interfaz para restablecer la VLAN nativa nuevamente a VLAN1.	`S1(config-if)#no switchport trunk native vlan`
Utilice este comando en el modo de configuración de interfaz para restablecer la interfaz de puerto de enlace troncal nuevamente a un puerto de modo de acceso estático.	`S1(config-if)#switchport mode access`

Sintaxis de los comandos





3.4 RESOLUCION DE PROBLEMAS DE LAS VLAN Y LOS ENLACES TRONCALES

3.4.1 PROBLEMAS COMUNES CON ENLACES TRONCALES.-

Problemas comunes con enlaces troncales

En este tema, el usuario aprende sobre los problemas comunes de la VLAN y el enlace troncal, que suelen asociarse a configuraciones incorrectas. Cuando configura la VLAN y los enlaces troncales en una infraestructura conmutada, estos tipos de errores de configuración son los más comunes,en el siguiente orden:

- **Faltas de concordancia de la VLAN nativa:** los puertos se configuran con diferentes VLAN nativas, por ejemplo si un puerto ha definido la VLAN 99 como VLAN nativa y el otro puerto de enlace troncal ha definido la VLAN 100 como VLAN nativa. Estos errores de configuración generan notificaciones de consola, hacen que el tráfico de administración y control se dirija erróneamente y, como ya ha aprendido, representan un riesgo para la seguridad.
- **Faltas de concordancia del modo de enlace troncal:** un puerto de enlace troncal se configura con el modo de enlace troncal "inactivo" y el otro con el modo de enlace troncal "activo". Estos errores de configuración hacen que el vínculo de enlace troncal deje de funcionar.
- **VLAN admitidas en enlaces troncales:** la lista de VLAN admitidas en un enlace troncal no se ha actualizado con los requerimientos de enlace troncal actuales de VLAN. En este caso, se envía tráfico inesperado o ningún tráfico al enlace troncal.

Si ha descubierto un problema con una VLAN o con un enlace troncal y no sabe cuál es, comience la resolución de problemas examinando los enlaces troncales para ver si existe una falta de concordancia de la VLAN nativa y luego vaya siguiendo los pasos de la lista. El resto de este tema examina cómo reparar los problemas comunes con enlaces troncales. El próximo tema presenta cómo identificar y resolver la configuración incorrecta de la VLAN y las subredes IP.

Problemas comunes con las VLAN y los enlaces troncales

Problema	Resultado	Ejemplo
Falta de concordancia en la VLAN nativa	Presenta un riesgo a la seguridad y crea resultados no deseados.	Por ejemplo, un puerto la ha definido como VLAN 99, el otro como VLAN 100.
Falta de concordancia en el modo de enlace troncal	Causa pérdida de la conectividad de la red.	Por ejemplo, en un puerto está configurado como "off" y en otro como modo de enlace troncal "on".
VLAN y Subredes IP	Causa pérdida de la conectividad de la red.	Por ejemplo, las computadoras de los usuarios pueden haber sido configuradas con las direcciones IP incorrectas.
VLAN permitidas en enlaces troncales	Provoca tráfico no deseado o no se envía el tráfico a través del enlace troncal.	La lista de las VLAN permitidas no admite los requisitos de enlace troncal de VLAN actuales.

Faltas de concordancia de la VLAN nativa

El usuario es un administrador de red y recibe un llamado que dice que la persona que utiliza la computadora PC4 no se puede conectar al servidor Web interno, servidor WEB/TFTP de la figura. Sabe que un técnico nuevo ha configurado recientemente el switch S3. El diagrama de topología parece correcto, entonces ¿por qué hay un problema? El usuario decide verificar la configuración en S3.

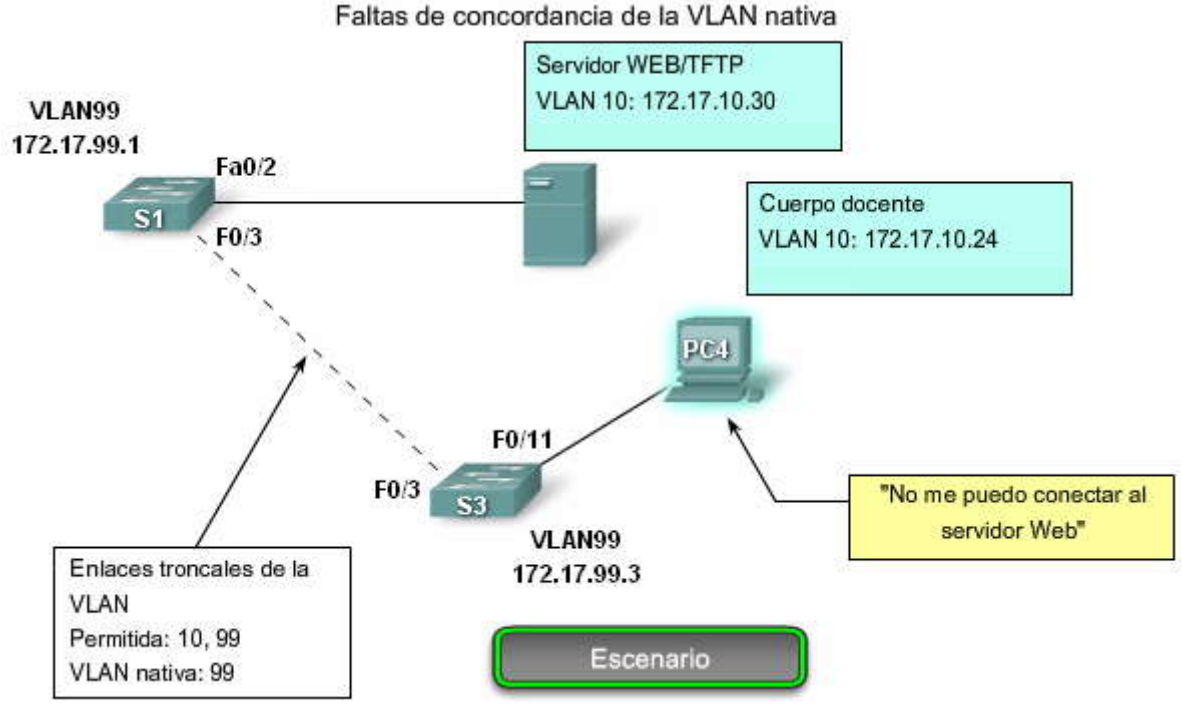
Haga clic en el botón Configuración en la figura.

Tan pronto como se conecta al switch S3, el mensaje de error que aparece en el área superior resaltada en la figuraaparece en la ventana de la consola. Observa la interfaz con el comando show interfaces f0/3 switchport. Nota que la VLAN nativa, la segunda área resaltada en la figura, se ha establecido como VLAN 100 y se encuentra inactiva. Sigue leyendo los resultados y observa que las VLAN permitidas son 10 y 99, como aparece en el área inferior resaltada.

Haga clic en el botón Solución en la figura.

Debe reconfigurar la VLAN nativa en el puerto de enlace troncal Fast Ethernet F0/3 para que sea VLAN 99. En la figura, el área superior resaltada muestra el comando para configurar la VLAN nativa en VLAN 99. Las dos áreas resaltadas siguientes confirman que el puerto de enlace troncal Fast Ethernet F0/3 ha reestablecido la VLAN nativa a VLAN 99.

Los resultados que aparecen en la pantalla para la computadora PC4 muestran que la conectividad se ha reestablecido para el servidor WEB/TFTP que se encuentra en la dirección IP 172.17.10.30.



Faltas de concordancia de la VLAN nativa

```
S3#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/3 (100), with S1 FastEthernet0/3 (99).
S3#show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 100 (Inactive)
…
Trunking VLANs Enabled: 10, 99
…
```

Configuración

Faltas de concordancia de la VLAN nativa

Resultado del switch S3

```
S3#config terminal
S3(config)#interface f0/3
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#end
S3#show interfaces f0/3 switchport
```

Resultado de la computadora PC4

```
Pc4>ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
…
```

Solución

Faltas de concordancia del modo de enlace troncal

En este curso ha aprendido que los vínculos de enlace troncal se configuran estáticamente con el comando switchport mode trunk. Ha aprendido que los puertos de enlace troncal utilizan publicaciones de DTP para negociar el estado del vínculo con el puerto remoto. Cuando un puerto en un vínculo de enlace troncal se configura con un modo de enlace troncal que no es compatible con el otro puerto de enlace troncal, no se puede formar un vínculo de enlace troncal entre los dos switches.

En este caso, surge el mismo problema: la persona que utiliza la computadora PC4 no puede conectarse al servidor Web interno. Una vez más, el diagrama de topología se ha mantenido y muestra una configuración correcta. ¿Por qué hay un problema?

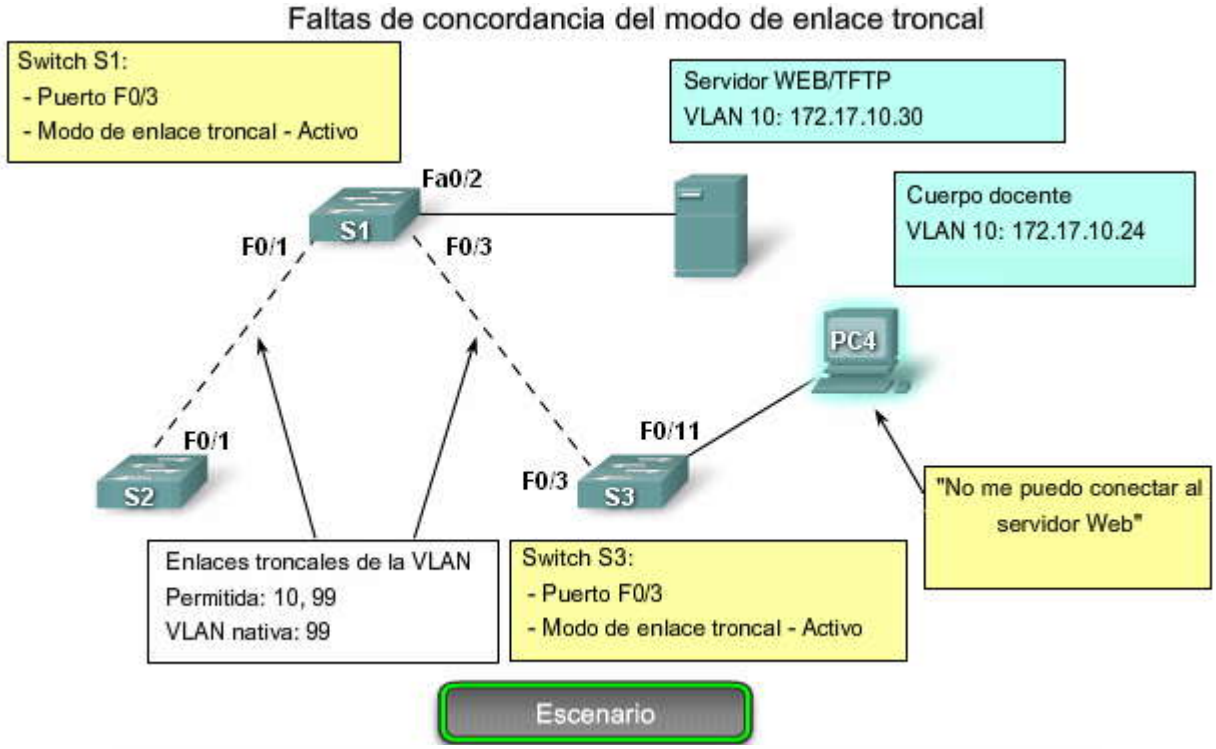
Haga clic en el botón Configuración en la figura.

Lo primero que hace es verificar el estado de los puertos de enlace troncal en el switch S1 con el comando show interfaces trunk. El comando revela en la figura que no hay enlace troncal en la interfaz F0/3 del switch S1. Examina la interfaz F0/3 para darse cuenta de que el puerto de switch está en modo dinámico automático, la primera área resaltada en la parte superior de la figura. Un examen de los enlaces troncales en el switch S3 revela que no hay puertos de enlace troncal activos. Más controles revelan que la interfaz F0/3 también se encuentra en modo dinámico automático, la primera área resaltada en la parte inferior de la figura. Ahora ya sabe por qué el enlace troncal está deshabilitado.

Haga clic en el botón Solución en la figura.

Debe reconfigurar el modo de enlace troncal de los puertos Fast Ethernet F0/3 en los switches S1 y S3. En la parte superior izquierda de la figura, el área resaltada muestra que el puerto se encuentra ahora en modo de enlazamiento troncal. La salida superior derecha del switch S3 muestra el comando utilizado para reconfigurar el puerto y los resultados del comando show interfaces trunk y revela que la interfaz F0/3 ha sido reconfigurada como modo de enlace troncal. El resultado de la

computadora PC4 indica que la PC4 ha recuperado la conectividad al servidor WEB/TFTP que se encuentra en la dirección IP 172.17.10.30.



Faltas de concordancia del modo de enlace troncal

Resultado del switch S1

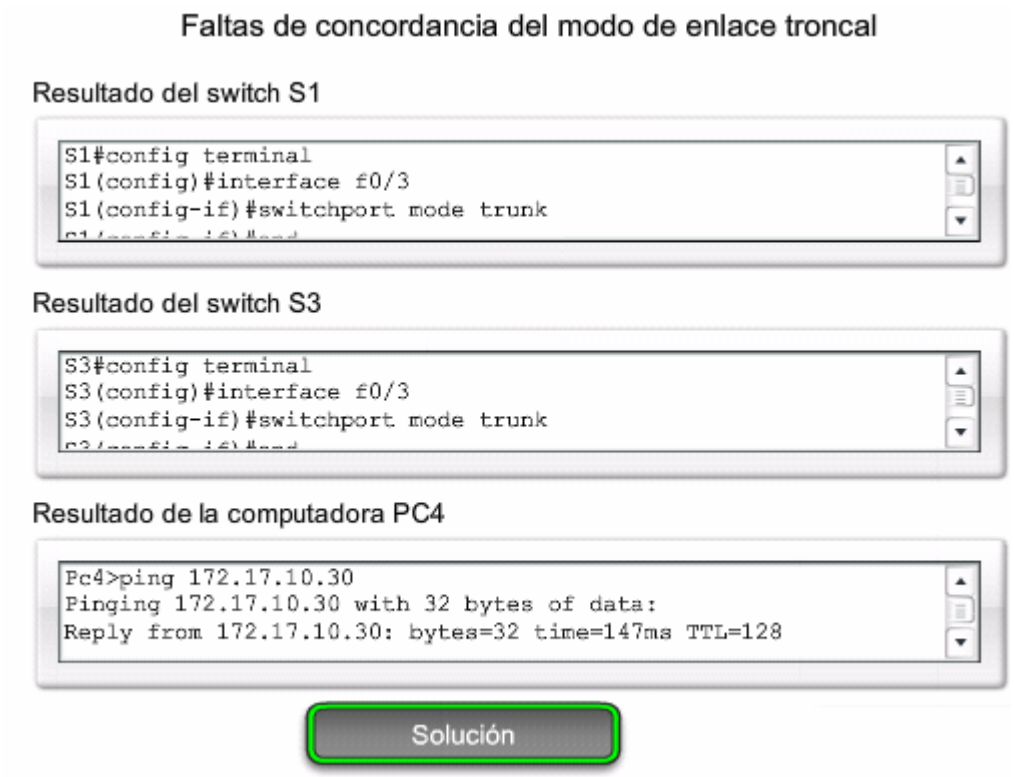
```
S1#show interfaces trunk
Port  Mode  Encapsulation  Status    Native vlan
Fa0/1 on    802.1q         trunking 99
Port  Vlans allowed on trunk
Fa0/1 10,99
```

Resultado del switch S3

```
S3# show interfaces trunk

S3#
S3# show interface f0/3 switchport
Name: Fa0/3
```

Configuración



Lista de VLAN incorrecta

Ha aprendido que para que el tráfico de una VLAN se transmita por un enlace troncal, debe haber acceso admitido en el enlace troncal. El comando utilizado para lograr esto es el comando switchport access trunk allowed vlan add vlan-id. En la figura, se han agregado la VLAN 20 (Estudiante) y la computadora PC5 a la red. La documentación se ha actualizado para mostrar que las VLAN admitidas en el enlace troncal son las 10, 20 y 99.

En este caso, la persona que utiliza la computadora PC5 no puede conectarse al servidor de correo electrónico del estudiante, que se muestra en la figura.

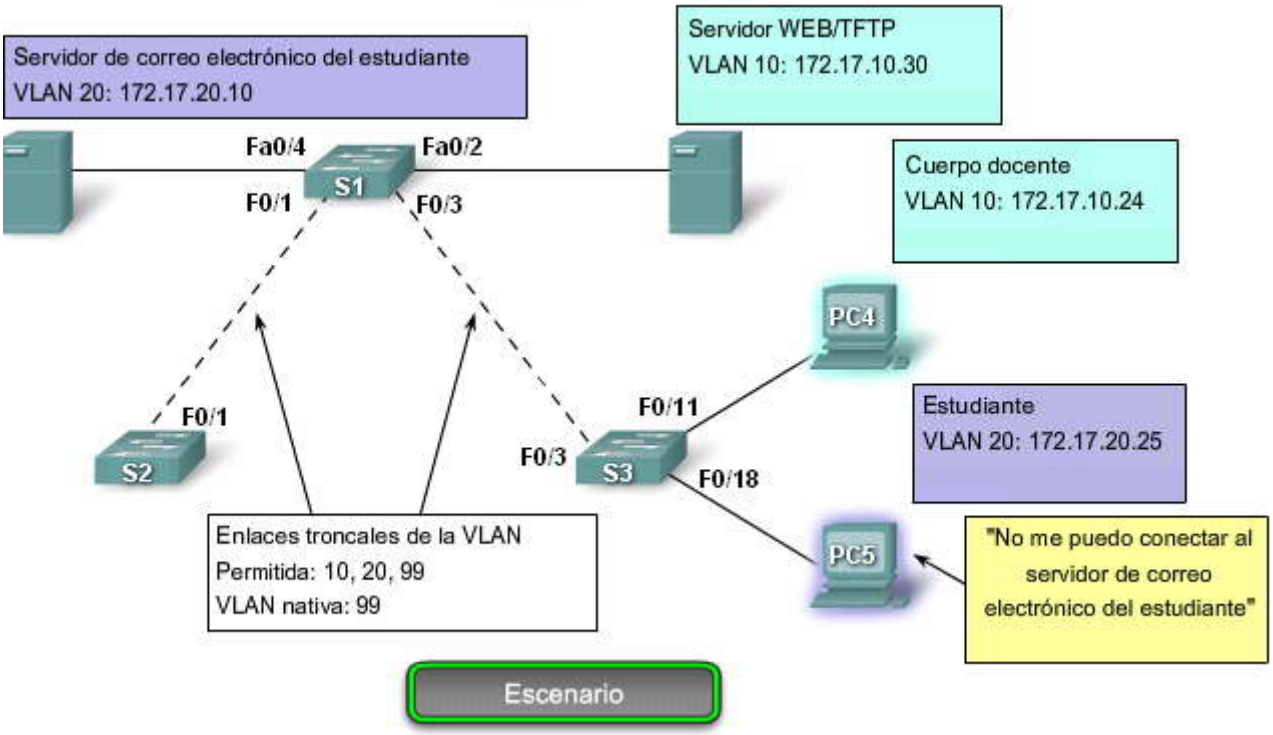
Haga clic en el botón Configuración en la figura.

Controle los puertos de enlace troncal en el switch S1 con el comando show interfaces trunk. El comando revela que la interfaz F0/3 en el switch S3 está correctamente configurada para admitir las VLAN 10, 20 y 99. Un examen de la interfaz F0/3 en el switch S1 revela que las interfaces F0/1 y F0/3 sólo admiten VLAN 10 y 99. Parece que alguien actualizó la documentación pero olvidó reconfigurar los puertos en el switch S1.

Haga clic en el botón Solución en la figura.

Debe reconfigurar los puertos F0/1 y F0/3 en el switch S1 con el comando switchport trunk allowed vlan 10,20,99. Los resultados que aparecen en la parte superior de la pantalla en la figura, muestran que las VLAN 10, 20 y 99 se agregan ahora a los puertos F0/1 y F0/3 en el switch S1. El comando show interfaces trunk es una excelente herramienta para revelar problemas comunes de enlace troncal. La parte inferior de la figura indica que la PC5 ha recuperado la conectividad con el servidor de correo electrónico del estudiante que se encuentra en la dirección IP 172.17.20.10.

Lista de VLAN incorrecta



Escenario

Lista de VLAN incorrecta

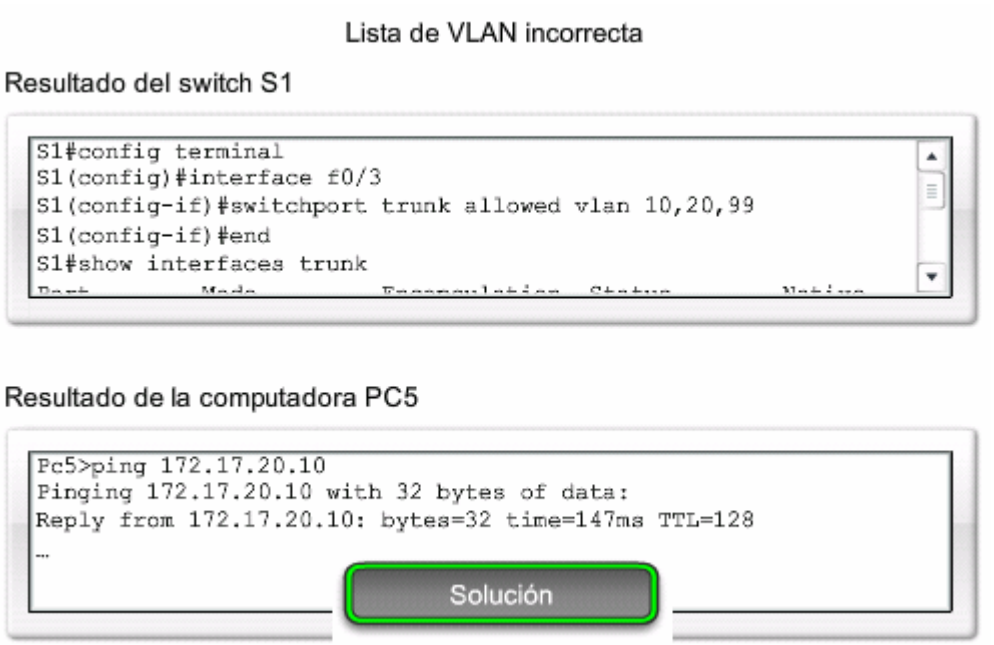
Resultado del switch S3

```
S3#show interfaces trunk
Port  Mode  Encapsulation  Status    Native vlan
Fa0/3 on    802.1q         trunking  99
Port  Vlans allowed on trunk
Fa0/3 10,20,99
```

Resultado del switch S1

```
S1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native
vlan
Fa0/1       on           802.1q         trunking      99
Fa0/3       on           802.1q         trunking      99
```

Configuración



3.4.2 UN PROBLEMA COMÚN CON CONFIGURACIONES DE VLAN.-

VLAN y subredes IP

Como ha aprendido, cada VLAN debe corresponder a una subred IP única. Si dos dispositivos en la misma VLAN tienen direcciones de subred diferentes, no se pueden comunicar. Este tipo de configuración incorrecta es un problema común y de fácil resolución al identificar el dispositivo en controversia y cambiar la dirección de subred por una dirección correcta.

En este caso, la persona que utiliza la computadora PC1 no puede conectarse al servidor Web del estudiante, que se muestra en la figura.

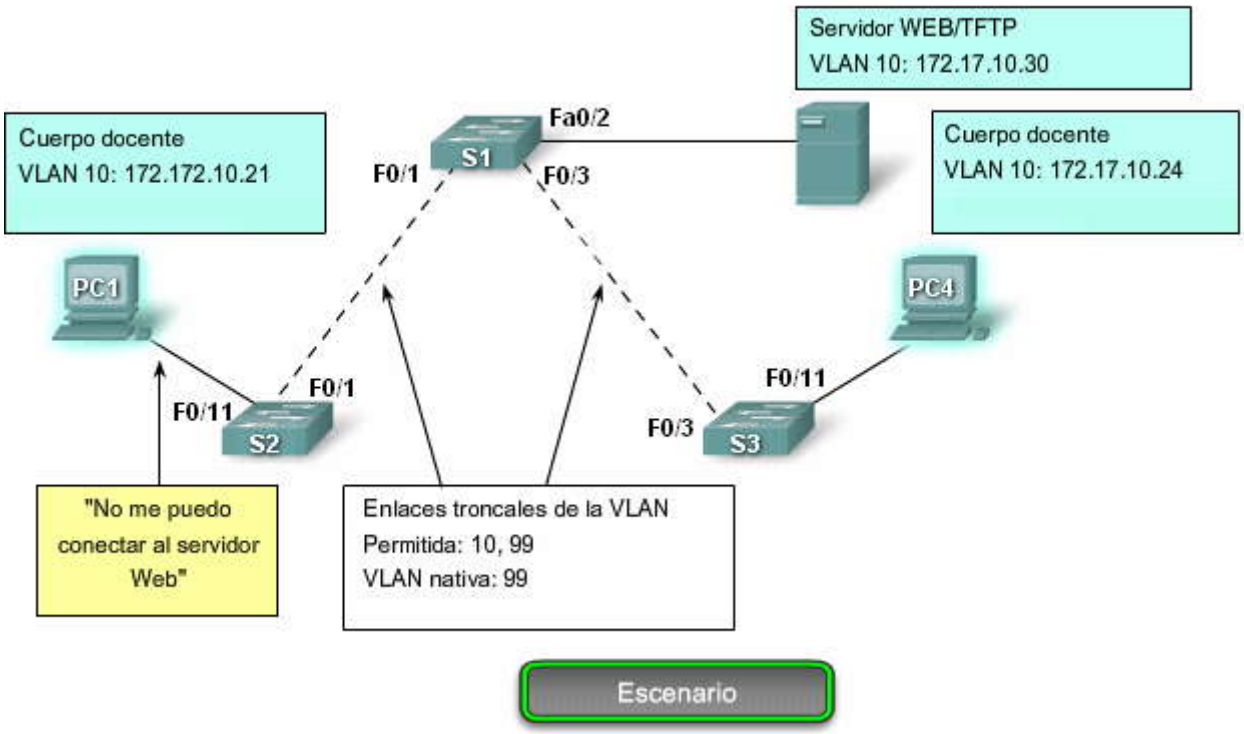
Haga clic en el botón Configuración en la figura.

En la figura, una verificación de los ajustes de configuración IP de la PC1 revela que el error más común al configurar las VLAN es: una dirección IP configurada incorrectamente. La computadora PC1 está configurada con una dirección IP de 172.172.10.21, pero debería haber estado configurada con la dirección 172.17.10.21.

Haga clic en el botón Solución en la figura.

La captura de pantalla del cuadro de diálogo de la configuración de Fast Ethernet de la PC1 muestra la dirección IP actualizada de 172.17.10.21. La captura de la parte inferior de la pantalla indica que la PC1 ha recuperado la conectividad al servidor WEB/TFTP que se encuentra en la dirección IP 172.17.10.30.

Problema común con configuraciones de VLAN



Problema común con configuraciones de VLAN

Resultado de la PC1

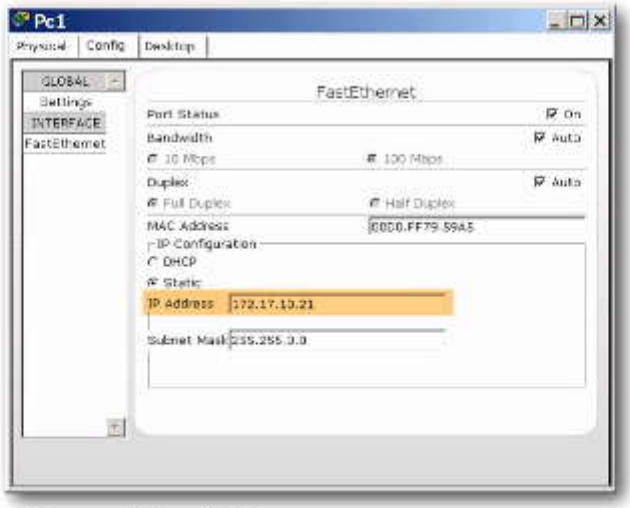
```
PC1>ipconfig

IP Address.....................: 172.172.10.21
Subnet Mask....................: 255.255.0.0
Default Gateway................: 0.0.0.0

PC1>
```

Configuración

Problema común con configuraciones de VLAN



Resultado de la Computadora PC1

```
PC1>ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
```

Solución

CAPITULO IV – "VTP"

4.0 INTRODUCCIÓN.-

4.0.1 INTRODUCCIÓN.-

A medida que crece el tamaño de la red de empresas pequeñas y medianas, también crece la administración involucrada en mantener la red. En el capítulo anterior aprendió cómo crear y manejar las VLAN y los enlaces troncales usando los comandos del IOS de Cisco. El tema era manejar la información de la VLAN en un solo switch. Pero ¿qué pasa si tiene muchos switches para administrar? ¿Cómo administrará la base de datos de la VLAN a través de muchos switches? En este capítulo, explorará cómo utilizar el protocolo de enlace troncal de la VLAN (VTP) de los switches Cisco Catalyst para simplificar la administración de la base de datos de la VLAN a través de switches múltiples.

En este capítulo aprenderá a:

- Explicar la función del VTP en una red switched convergente.
- Describir la operación del VTP incluidos dominios, modos, publicaciones y depuración.
- Configurar el VTP en los switches de una red convergente.

4.1 CONCEPTOS DE VTP.-

4.1.1 ¿QUÉ ES UN VTP?.-

El desafío de administrar la VLAN

A medida que aumenta el número de switches en una red de empresas pequeñas o medianas, la administración general requerida para administrar las VLAN y los enlaces troncales en una red se vuelve un desafío.

Haga clic para reproducir la visualización de una animación sobre el desafío de administrar la VLAN.

Administración de una VLAN de red pequeña

En la animación, la figura muestra una administración de red que agrega una nueva VLAN, VLAN30. El administrador de red necesita actualizar tres enlaces troncales que permitan a las VLAN 10, 20, 30 y 99. Debe recordar que un error común es olvidarse de actualizar la lista permitida de las VLAN en los enlaces troncales.

Haga clic en el botón Red grande que se muestra en la figura.

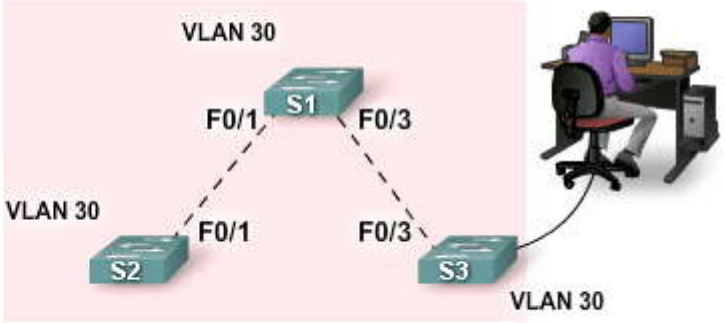
Administración de VLAN en la Red grande

Si considera la red más grande en la figura, se hace evidente el desafío de administrar la VLAN. Después de haber actualizado manualmente esta red unas pocas veces, puede desear conocer si existe una forma para que los switches sepan cuáles son las VLAN y los enlaces troncales, de modo que no tenga que configurarlos manualmente. Está listo para aprender sobre el protocolo de enlace troncal de la VLAN (VTP).

El desafío de administrar la VLAN

VLAN existentes:
- VLAN 10 - cuerpo docente/personal
- VLAN 20 - estudiantes
- VLAN 99 - VLAN de administración

Tarea de la VLAN de administración:
- Agregar VLAN 30 - Invitado

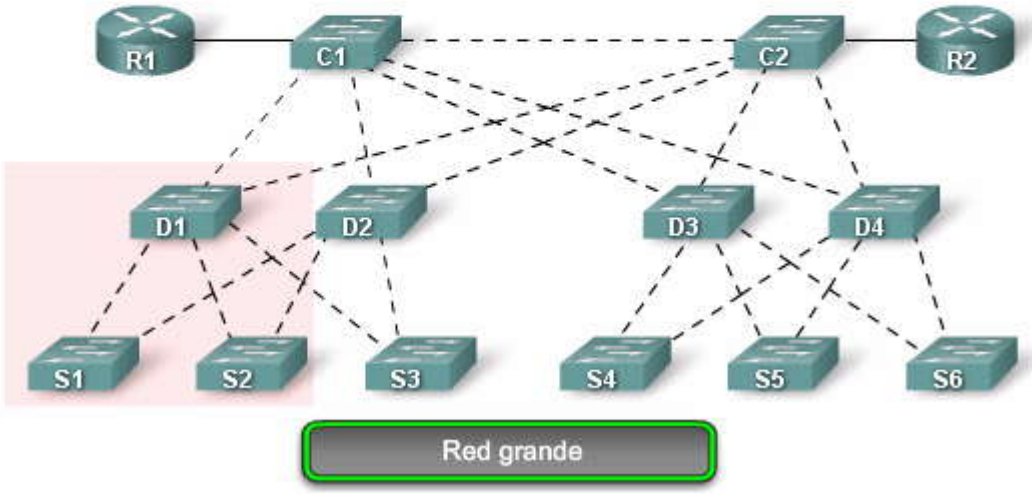


Red pequeña

El desafío de administrar la VLAN

VLAN existentes: 10 ,20 99

Tarea de administración de VLAN: Agregue la VLAN 30



¿Qué es el VTP?

El VTP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de cliente del VTP. El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP.

En la figura, haga clic en Reproducir para ver una animación general sobre cómo funciona el VTP.

Descripción general del VTP

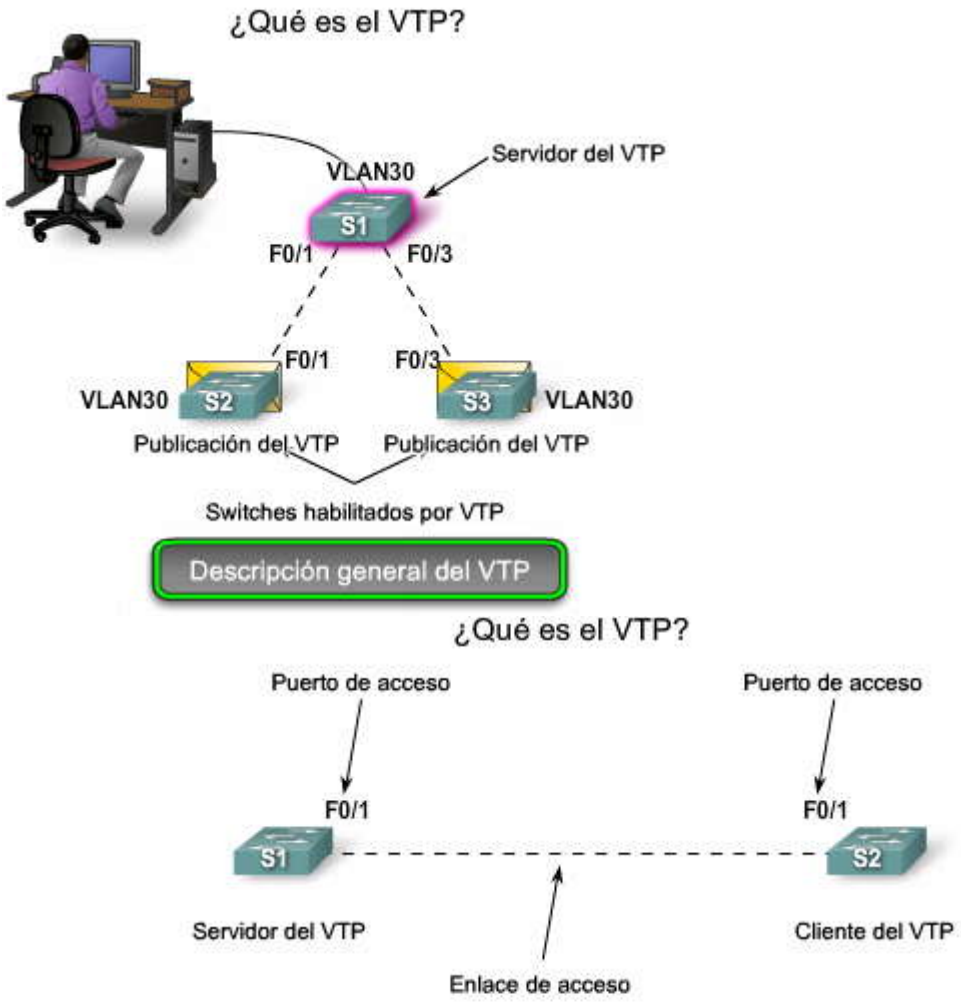
El VTP permite al administrador de red realizar cambios en un switch que está configurado como servidor del VTP. Básicamente, el servidor del VTP distribuye y sincroniza la información de la VLAN a los switches habilitados por el VTP a través de la red conmutada, lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias en las configuraciones. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN denominada vlan.dat.

Haga clic en el botón Dos switches que se muestra en la figura.

Dos switches

En la figura haga clic en Reproducir para ver una animación sobre la interacción básica del VTP entre un servidor del VTP y un cliente del VTP.

En la figura, se agrega un enlace troncal entre switch S1, un servidor del VTP y S2, un cliente del VTP. Después de establecer un enlace troncal entre los dos switches, las publicaciones del VTP se intercambian entre los switches. Tanto el servidor como el cliente intercambian las publicaciones entre ellos para asegurarse de que cada uno tieneun registro preciso de la información de la VLAN. Las publicaciones del VTP no se intercambiarán si el enlace troncal entre los switches está inactivo. En el resto de este capítulo se explican los detalles de cómo funciona el VTP.



El puerto F0/1 en el switch S1 y el puerto F0/1 en el switch S2 vuelven a acceder a los puertos de switch.

El enlace entre el switch S1 y el S2 se convierte en enlace de acceso.

Dos switches

Beneficios del VTP

Ya aprendió que el VTP mantiene la consistencia de configuración de la VLAN mediante la administración del agregado, la eliminación y la redenominación de las VLAN a través de los switches múltiples de Cisco en una red. El VTP ofrece un número de beneficios para los administradores de red, según se muestra en la figura.

Beneficios de VTP

- Consistencia en la configuración de la VLAN a través de la red
- Seguimiento y monitoreo preciso de las VLAN
- Informes dinámicos sobre las VLAN que se agregan a una red
- Configuración de enlace troncal dinámico cuando las VLAN se agregan a la red

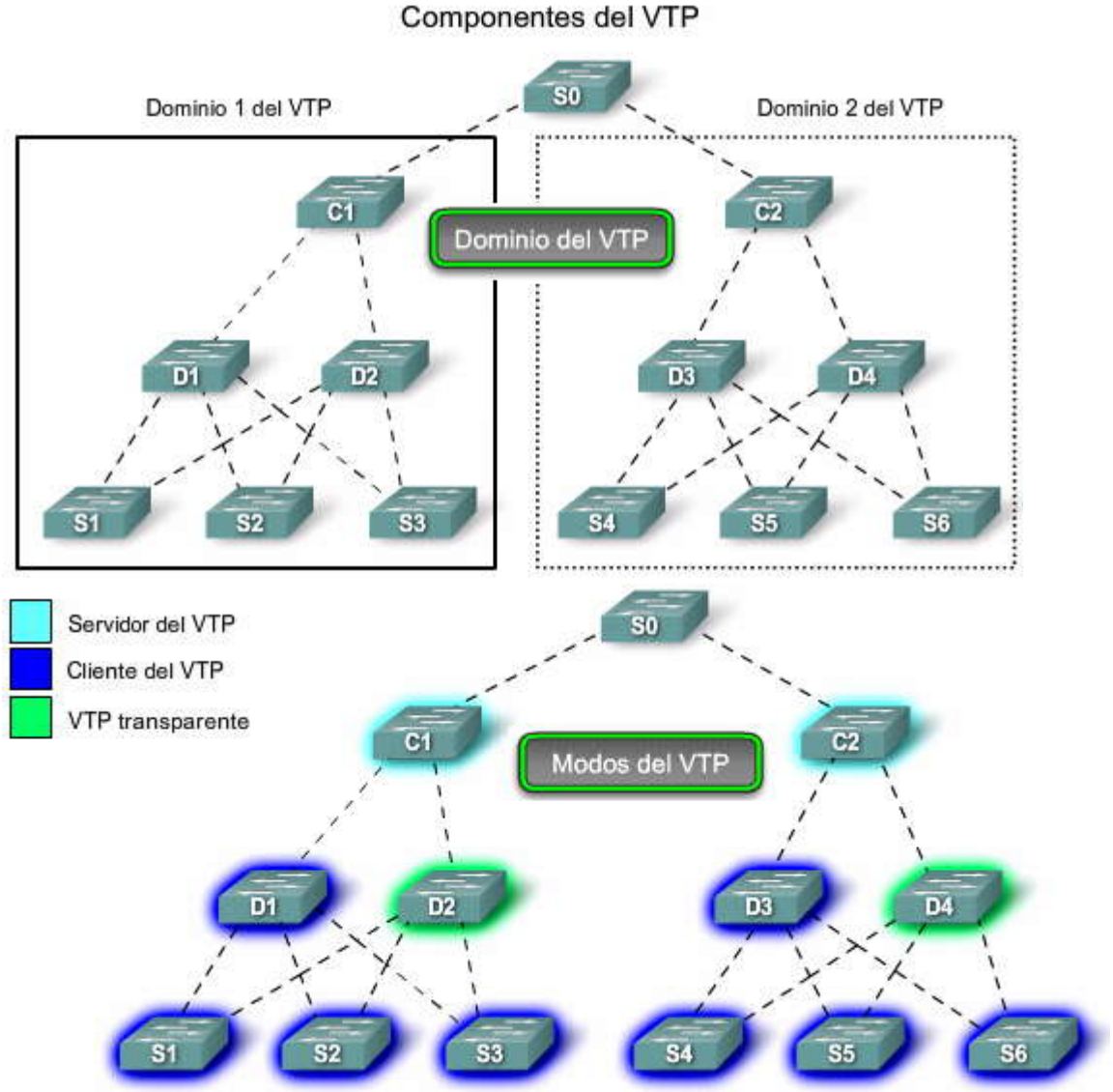
Componentes del VTP

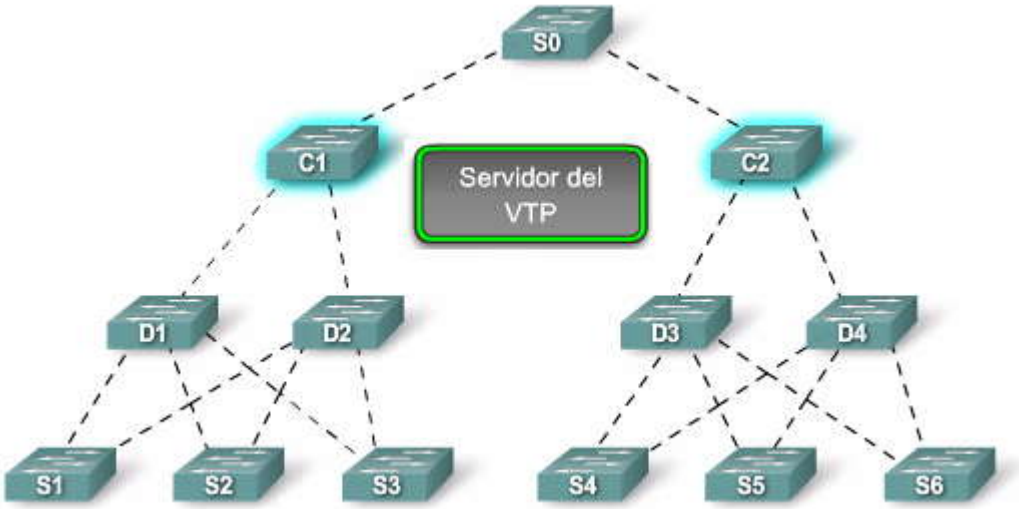
Existe un número de componentes clave con los que necesita familiarizarse al aprender sobre el VTP. Aquí se muestra una breve descripción de los componentes, que se explicarán más adelante a medida que se avance en el capítulo.

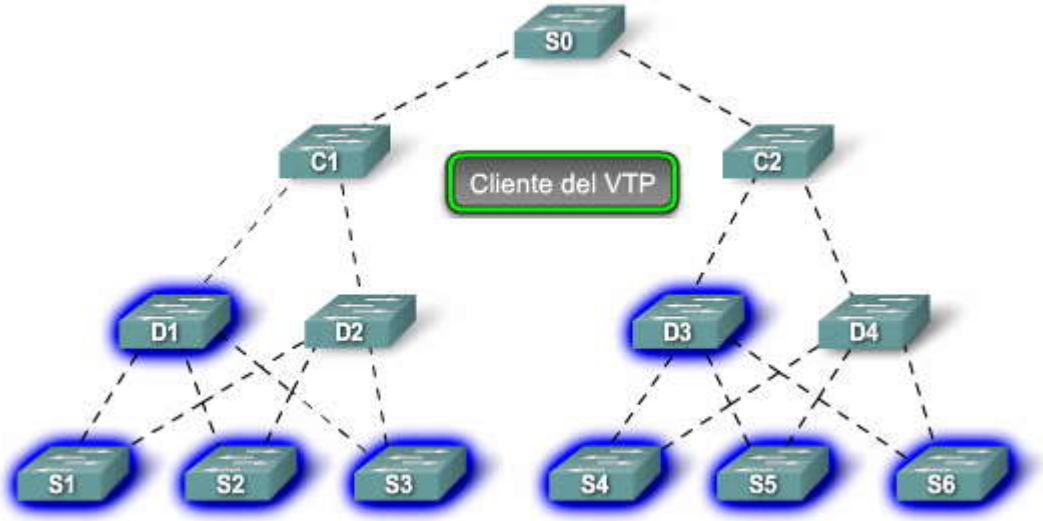
- **Dominio del VTP:** Consiste de uno o más switches interconectados. Todos los switches en un dominio comparten los detalles de configuración de la VLAN usando las publicaciones del VTP. Un router o switch de Capa 3 define el límite de cada dominio.
- **Publicaciones del VTP:** El VTP usa una jerarquía de publicaciones para distribuir y sincronizar las configuraciones de la VLAN a través de la red.
- Modos del VTP: Un switch se puede configurar en uno de tres modos: servidor, cliente o transparente.

- **Servidor del VTP:** los servidores del VTP publican la información VLAN del dominio del VTP a otros switches habilitados por el VTP en el mismo dominio del VTP. Los servidores del VTP guardan la información de la VLAN para el dominio completo en la NVRAM. El servidor es donde las VLAN se pueden crear, eliminar o redenominar para el dominio.
- **Cliente del VTP:** los clientes del VTP funcionan de la misma manera que los servidores del VTP pero no pueden crear, cambiar o eliminar las VLAN en un cliente del VTP. Un cliente del VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN. Debe configurar el modo de cliente del VTP en un switch.
- **VTP transparente:** los switches transparentes envían publicaciones del VTP a los clientes del VTP y servidores del VTP. Los switches transparentes no participan en el VTP. Las VLAN que se crean, redenominan o se eliminan en los switches transparentes son locales para ese switch solamente.
- **Depuración del VTP:** La depuración del VTP aumenta el ancho de banda disponible para la red mediante la restricción del tráfico saturado a esos enlaces troncales que el tráfico debe utilizar para alcanzar los dispositivos de destino. Sin la depuración del VTP, un switch satura el broadcast, el multicast y el tráfico desconocido de unicast a través de los enlaces troncales dentro de un dominio del VTP aunque los switches receptores podrían descartarlos.

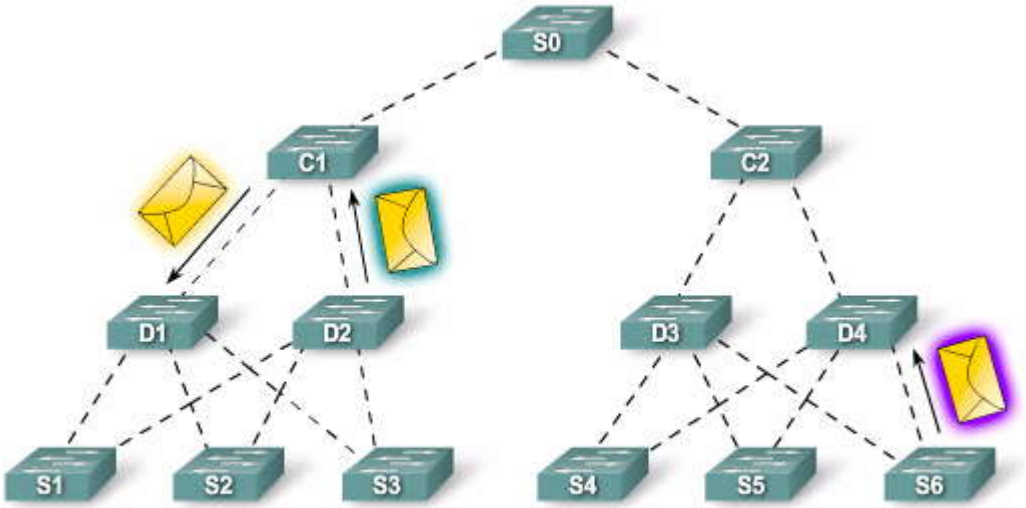
En la figura, pase el mouse sobre los componentes clave del VTP para ver dónde se encuentran en la red.

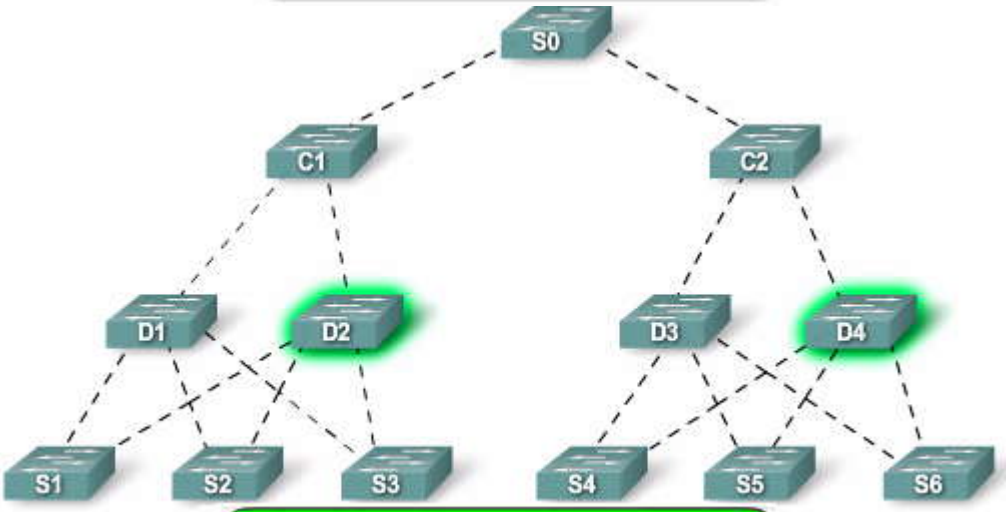






Componentes del VTP





VTP es el acrónimo de _____ .	✓	Protocolo de enlace troncal de VLAN
VTP es un _____ protocolo de mensajes que mantiene la consistencia de configuración de la VLAN mediante la administración del agregado, la eliminación y la redenominación de las VLAN a través de los switches múltiples de Cisco en una red.	✓	Capa 2
VTP es un protocolo _____ disponible sólo para switches Cisco.	✓	propiedad
En un VTP de modo _____ se puede crear, modificar y eliminar VLAN para el dominio completo del VTP.	✓	servidor
En un VTP de modo _____ , el switch no participa en el VTP. Sin embargo, el switch envía publicaciones del VTP a través de las interfaces de los enlaces troncales.	✓	transparente
En un VTP de modo _____ , no se puede crear, cambiar o eliminar las VLAN.	✓	cliente
En un VTP de modo _____ , las configuraciones de VLAN no se guardan en la NVRAM.	✓	cliente
El modo _____ del VTP le permite crear, modificar y eliminar las VLAN en un solo switch sin afectar al resto de los switches en su red.	✓	transparente
El modo _____ del VTP es el modo predeterminado del switch Cisco.	✓	servidor

4.2 OPERACIÓN DEL VTP.-

4.2.1 CONFIGURACION PRETERMINADA DEL VTP.-

En CCNA Exploration: Aspectos básicos de red, aprendió que un switch Cisco sale defábrica con configuraciones por defecto. La figura muestra las configuraciones predeterminadas del VTP. El beneficio del VTP es que automáticamente distribuye y sincroniza las configuraciones de dominio y VLAN a través de la red. Sin embargo, este beneficio viene con un costo: sólo se pueden agregar switches que están en la configuración predeterminada del VTP. Si se agrega un switch permitido por el VTP cuya configuración sustituye a las mismas del VTP de la red existente, los cambios que son difíciles de solucionar se propagan automáticamente a través de la red. Entonces asegúrese de agregar sólo switches que están en la configuración predeterminada del VTP Luego, en este capítulo, aprenderá cómo agregar switches a una red del VTP.

Versiones del VTP

El VTP tiene tres versiones: 1, 2 y 3. Sólo se permite una versión del VTP en un dominio del VTP. La versión predeterminada es la Versión 1 del VTP. Un switch Cisco 2960 admite la versión 2 del VTP pero está deshabilitada. Un debate de las versiones del VTP está más allá del ámbito de este curso.

Haga clic en el botón Resultado del switch que se muestra en la figura para ver las configuraciones predeterminadas del VTP en el switch S1.

Visualización del estado del VTP

La figura muestra cómo ver las configuraciones del VTP para un switch Cisco 2960, S1. El comando del IOS de Cisco show VTP status visualiza el estado del VTP. La salida muestra que el switch S1 está en modo del servidor del VTP predeterminado y que no existe nombre de dominio del VTP asignado. La salida también muestra que la versión máxima del VTP disponible para el switch es la versión 2 y que la versión 2 del VTP está deshabilitada. Utilizará el comando show VTP status frecuentemente a medida que configure y administre el VTP en una red. A continuación, se describen brevemente los parámetros de show VTP status:

- **Versión del VTP:** muestra la versión del VTP que el switch puede ejecutar. De manera predeterminada, el switch implementa la versión 1, pero puede configurarse para la versión 2.
- Revisión de la configuración: el número de la revisión de la configuración actual está en el switch. Más adelante, en este capítulo, aprenderá más acerca de los números de revisiones.
- **VLAN máximas admitidas localmente:** Número máximo de VLAN admitidas localmente.
- **Número de VLAN existentes:** Número de VLAN existentes.
- **Modo operativo del VTP:** puede ser servidor, cliente o transparente.
- **Nombre de dominio del VTP:** nombre que identifica el dominio administrativo para el switch.
- **Modo de depuración del VTP:** muestra si la depuración está habilitada o deshabilitada.
- **Modo de la V2 del VTP:** muestra si la versión 2 del VTP está habilitada. La versión 2 del VTP está deshabilitada de manera predeterminada.
- **Generación de Traps del VTP:** muestra si las traps del VTP se envían hacia la estación de administración de red.
- **MD5 Digest:** una checksum de 16 bytes de la configuración del VTP.
- **Última configuración modificada:** fecha y hora de la última modificación de configuración. Muestra la dirección IP del switch que causó el cambio de configuración a la base de datos.

Configuración del VTP predeterminado

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x3F 0x37 0x45 0x9A 0x37 0x53 0xA6 0xDE
Configuration last modified by 0.0.0.0 at 3-1-93 00:14:07
S1#
```

Resultado del switch

4.2.2 DOMINIOS DEL VTP.-

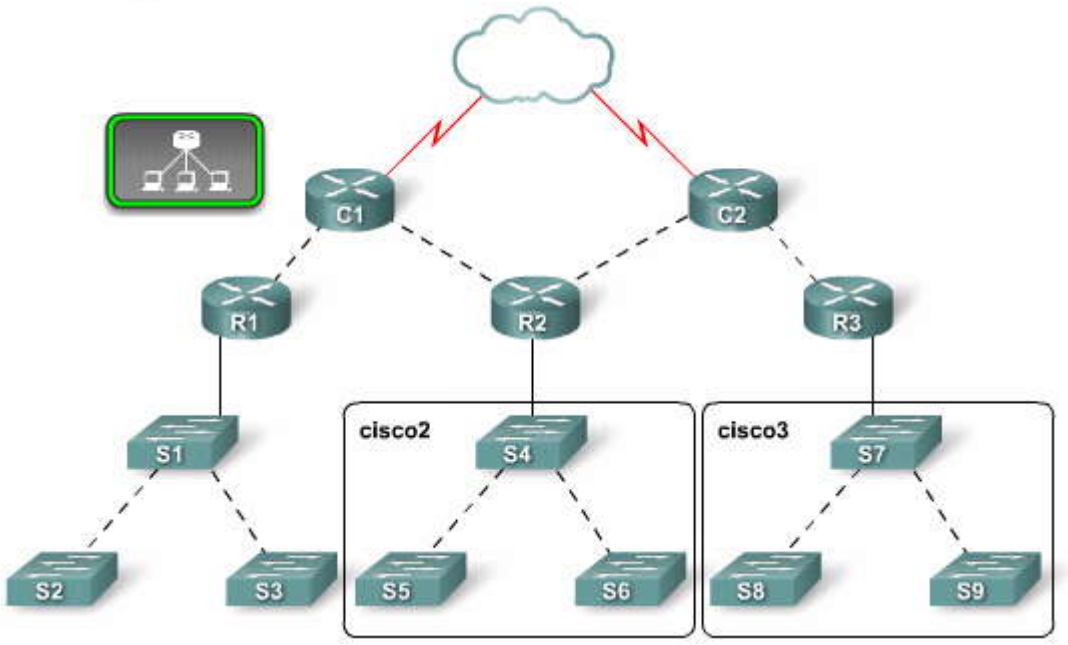
Dominios del VTP

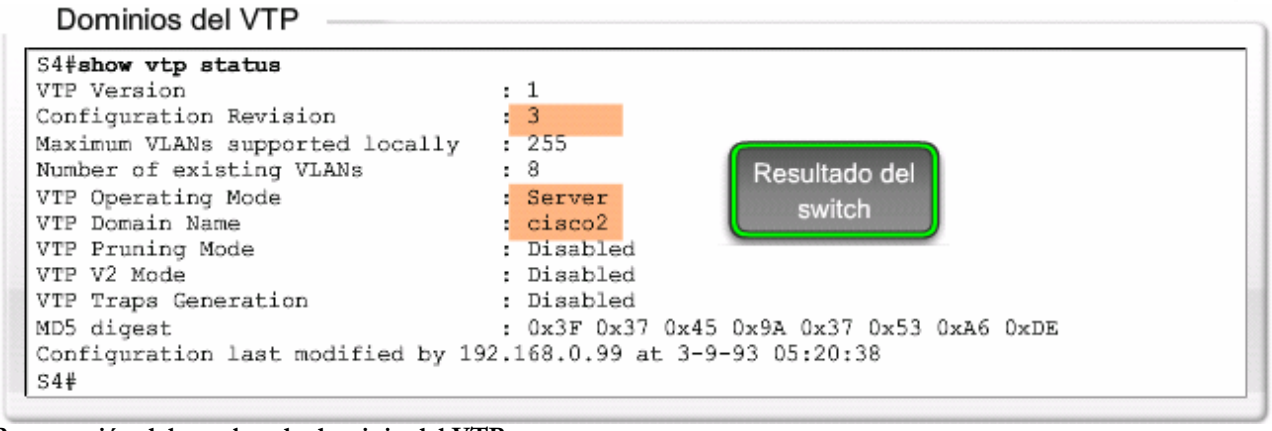
El VTP le permite separar su red en dominios de administración más pequeños para ayudarlo a reducir la administración de la VLAN. Un beneficio adicional de configurar los dominios del VTP es que limita hasta qué punto se propagan los cambios de configuración en la red si se produce un error. La figura muestra una red con dos dominios de VTP: Cisco2 y Cisco3. En este capítulo, se configurarán los tres switches: S1, S2 y S3 para el VTP.

Un dominio del VTP consiste en un switch o varios switches interconectados que comparten el mismo nombre de dominio del VTP. Más adelante en este capítulo aprenderá cómo los switches habilitados por el VTP adquieren un nombre común de dominio. Un switch puede ser parte de sólo un dominio del VTP a la vez. Hasta tanto especifique el nombre de dominio del VTP, no puede crear ni modificar las VLAN en un servidor del VTP, y la información de la VLAN no se propaga a través de la red.

Haga clic en el botón Resultado del switch que se muestra en la figura para ver la salida del switch S4.

Dominios del VTP





Propagación del nombre de dominio del VTP

Para que un switch de cliente o servidor del VTP participe en una red habilitada por el VTP, debe ser parte del mismo dominio. Cuando los switches están en diferentes dominios de VTP no intercambian los mensajes del VTP. Un servidor del VTP propaga el nombre de dominio del VTP a todos los switches. La propagación del nombre de dominio usa tres componentes del VTP: servidores, clientes y publicaciones.

En la figura, haga clic en Reproducir para ver cómo un servidor del VTP propaga el nombre de dominio del VTP en una red.

La red en la figura muestra tres switches: S1, S2 y S3 en su configuración predeterminada del VTP. Se configuran como servidores del VTP. Los nombres de dominio del VTP no han sido configurados en ninguno de los switches.

El administrador de la red configura el nombre de dominio del VTP como cisco1 en el switch S1 del servidor del VTP. El servidor del VTP envía una publicación de VTP con el nuevo nombre de dominio incluido. Los switches del servidor del VTP de S2 y S3 actualizan su configuración del VTP al nuevo nombre de dominio.

Nota: Cisco recomienda que el acceso a las funciones de configuración del nombre de dominio sea protegido por una contraseña. Los detalles de la configuración de la contraseña se presentarán más adelante en el curso.

¿Cómo se ubica el nombre de dominio en una publicación del VTP? ¿Qué información se intercambia entre los switches habilitados por el VTP? En el próximo punto, aprenderá sobre los detalles de las publicaciones del VTP y encontrará respuestas a estas preguntas.

4.2.3 PUBLICACIÓN DEL VTP.-

Estructura de trama del VTP

Las publicaciones (o mensajes) del VTP distribuyen nombre de dominio del VTP y cambios en la configuración de la VLAN a los switches habilitados por el VTP. En este punto, aprenderá sobre la estructura de la trama del VTP y cómo los tres tipos de publicaciones permiten al VTP distribuir y sincronizar las configuraciones de VLAN a través de toda la red.

Haga clic en el botón Descripción general en la figura y, luego haga clic en Reproducir para ver una animación sobre la estructura de una trama del VTP.

Encapsulación de la trama del VTP

Una trama del VTP consiste en un campo de encabezado y un campo de mensaje. La información del VTP se inserta en el campo de datos de una trama de Ethernet. La trama de Ethernet luego se encapsula como una trama troncal de 802.1Q (o trama ISL). Cada switch en el dominio envía publicaciones periódicas de cada puerto de enlace troncal a una dirección multicast reservada. Los switches vecinos reciben estas publicaciones que actualizan las configuraciones de sus VTP y VLAN si es necesario.

Haga clic en el botón Detalles de trama del VTP que se muestra en la figura.

Detalles de trama del VTP

En la figura, se puede ver la estructura de la trama del VTP en más detalle. Tenga presente que una trama del VTP encapsulada como una trama 802.1Q no es estática. El contenido del mensaje delVTP determina qué campos están presentes. El switch receptor habilitado por el VTP busca campos y valores específicos en la trama 802.1Q para saber qué procesar. Los siguientes campos clave están presentes cuando una trama del VTP está encapsulada como una trama 802.1Q:

Dirección MAC destino: esta dirección se configura a 01-00-0C-CC-CC-CC, que es la dirección multicast reservada para todos los mensajes del VTP.

Campo LLC: campo de Control de enlace lógico (LLC) contiene un punto de acceso al servicio destino (DSAP) y un punto de acceso al servicio de origen (SSAP) establecidos al valor de AA.

Campo SNAP: campo del Protocolo de acceso a la subred (SNAP) tiene un OUI establecido a AAAA y tipo establecido a 2003.

Campo del encabezado del VTP: el contenido varía según el tipo de resumen del mensaje del VTP, subconjunto o solicitud pero siempre contiene estos campos del VTP:

Nombre de dominio: identifica el dominio administrativo para el switch.
Longitud de nombre de dominio: la longitud del nombre de dominio.
Versión establecida ya sea para VTP 1, VTP 2 o VTP 3. El switch Cisco 2960 sólo admite a VTP 1 y VTP 2.
Número de revisión de configuración: el número de revisión de configuración actual en este switch.

Campo de mensaje del VTP: varía según el tipo de mensaje.

Haga clic en el botón Contenido del mensaje del VTP que se muestra en la figura.

Contenido del mensaje del VTP

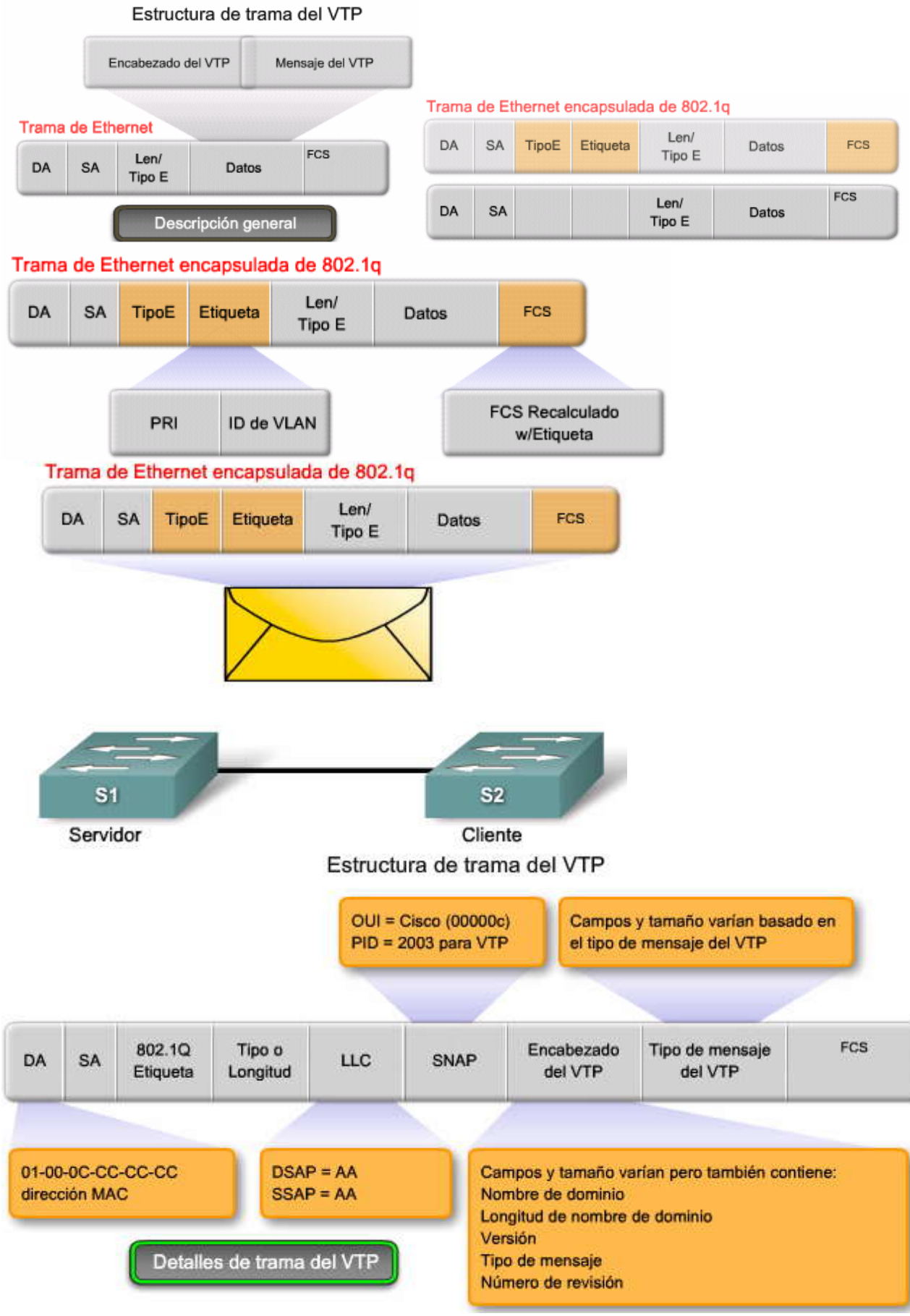
Las tramas del VTP contienen la siguiente información de dominio global de longitud fija:

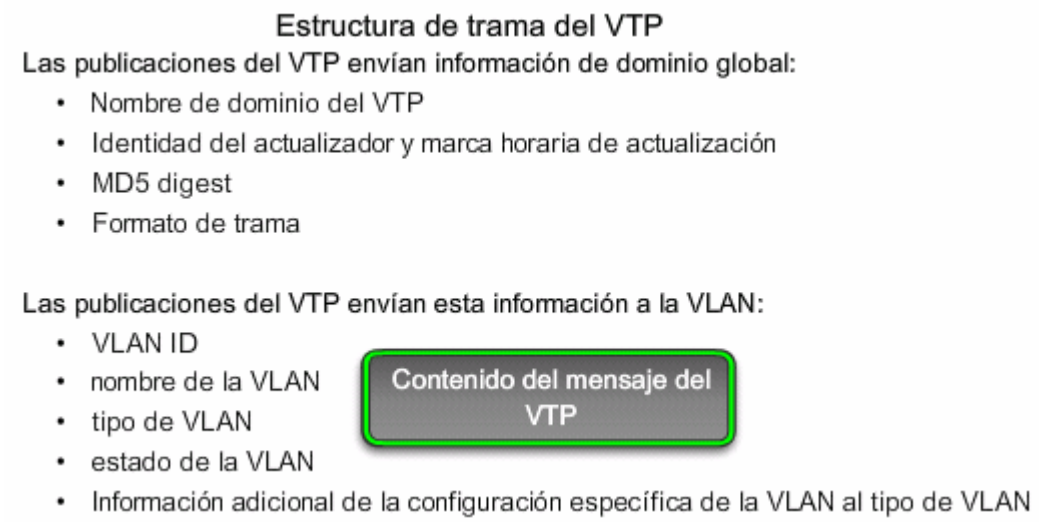
- Nombre de dominio del VTP
- Identidad del switch que envía el mensaje y la hora en que es enviado
- Configuración de VLAN del MD5 digest, incluido el tamaño de la unidad máxima de transmisión (MTU) para cada VLAN
- Formato de trama: ISL o 802.1Q

Las tramas del VTP contienen la siguiente información para cada VLAN configurada:

- ID de VLAN (IEEE 802.1Q)
- Nombre de VLAN
- Tipo de VLAN
- Estado de la VLAN
- Información adicional de la configuración específica de la VLAN al tipo de VLAN

Nota: Una trama de VTP está encapsulada en una trama de Ethernet 802.1Q. La trama de Ethernet completa de 802.1Q es la publicación del VTP llamado con frecuencia mensaje del VTP. Los términos trama, publicación y mensaje se suelen utilizar de modo intercambiable.





Número de revisión del VTP

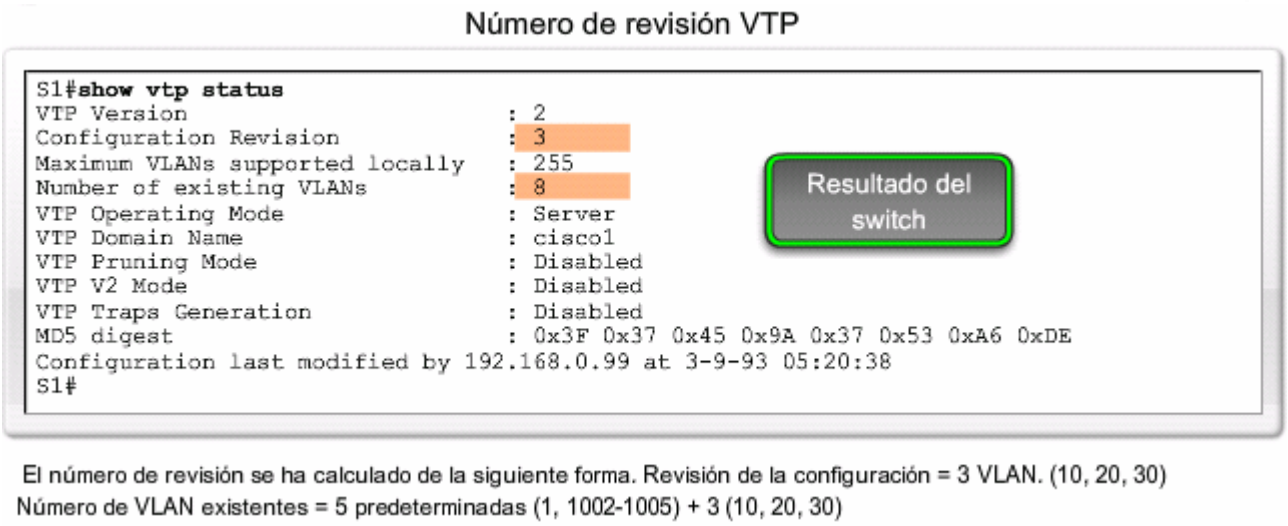
El número de revisión de la configuración es un número de 32 bits que incluye el nivel de revisión para una trama del VTP. El número de configuración predeterminado para un switch es cero. Cada vez que se agrega o elimina una VLAN, se aumenta el número de revisión de la configuración. Cada dispositivo de VTP rastrea el número de revisión de configuración del VTP que se le asigna.

Nota: Un cambio de nombre de dominio del VTP no aumenta el número de revisión. En su lugar, reestablece el número de revisión a cero.

El número de revisión de la configuración determina si la información de configuración recibida del otro switch habilitado por el VTP es más reciente que la versión guardada en el switch. La figura muestra un administrador de red que agrega tres VLAN al switch S1.

Haga clic en el botón Resultado de switch que se muestra en la figura para ver cómo se ha cambiado el número de revisión. El área resaltada muestra que el número de revisión en el switch S1 es 3, el número de VLAN es hasta ocho porque se han agregado tres VLAN a las cinco VLAN predeterminadas.

El número de revisión juega un rol importante y complejo al habilitar la VTP a distribuir y sincronizar el dominio del VTP y la información de configuración de la VLAN. Para comprender qué hace el número de revisión, primero necesita aprender los tres tipos de publicaciones del VTP y los tres modos del VTP.



Publicaciones del VTP

Publicaciones de resumen

La publicación del resumen contiene el nombre de dominio del VTP, el número actual de revisión y otros detales de la configuración del VTP.

Se envían publicaciones de resumen:

- Cada 5 minutos, por el servidor o cliente del VTP para informar a los switches vecinos habilitados por el VTP del número de revisión actual de la configuración del VTP para su dominio del VTP.
- Inmediatamente después de haber establecido una configuración

Haga clic en el botón Resumen y luego en el botón Reproducir que se muestran en la figura para ver una animación sobre las publicaciones del VTP del resumen.

Publicaciones de subconjunto

Una publicación de subconjunto contiene información de la VLAN. Los cambios que disparan una publicación de subconjunto incluyen:

- Creación o eliminación de una VLAN
- Suspensión o activación de una VLAN
- Cambio de nombre de una VLAN
- Cambio de MTU de una VLAN

Puede tomar publicaciones de subconjuntos múltiples para actualizar completamente la información de la VLAN.

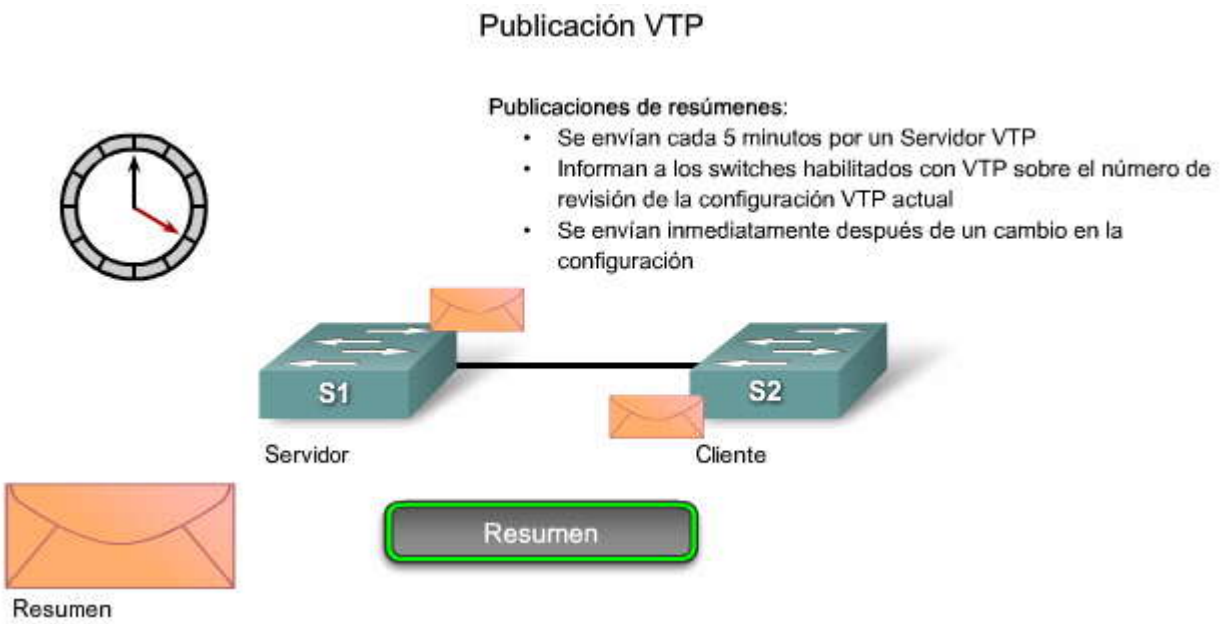
Haga clic en el botón Subconjunto y luego en el botón Reproducir que se muestran en la figura para ver una animación sobre las publicaciones del VTP de subconjuntos.

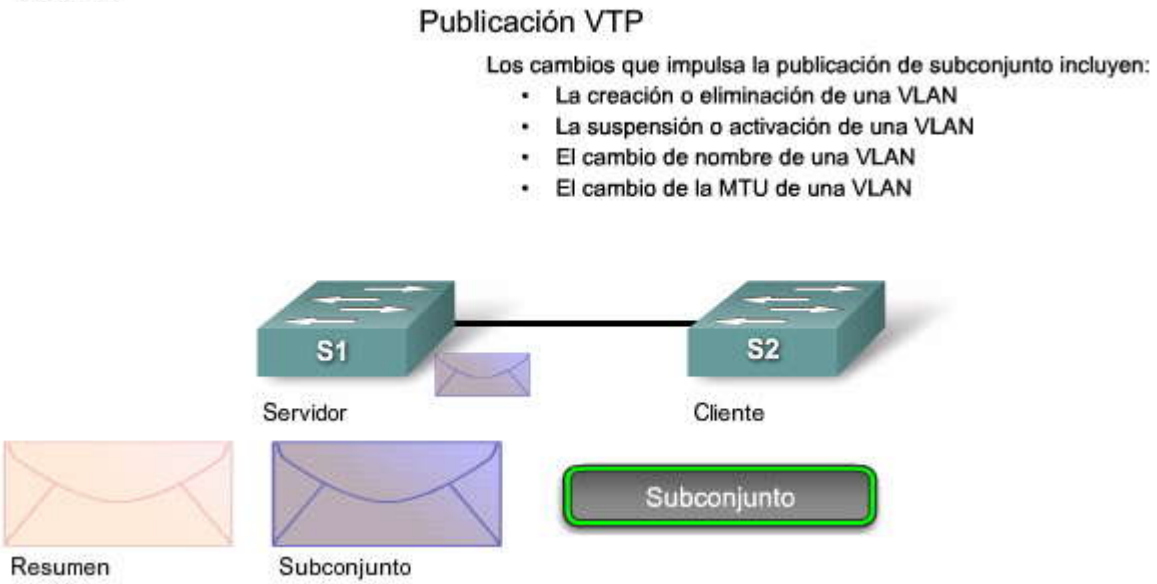
Publicaciones de solicitud

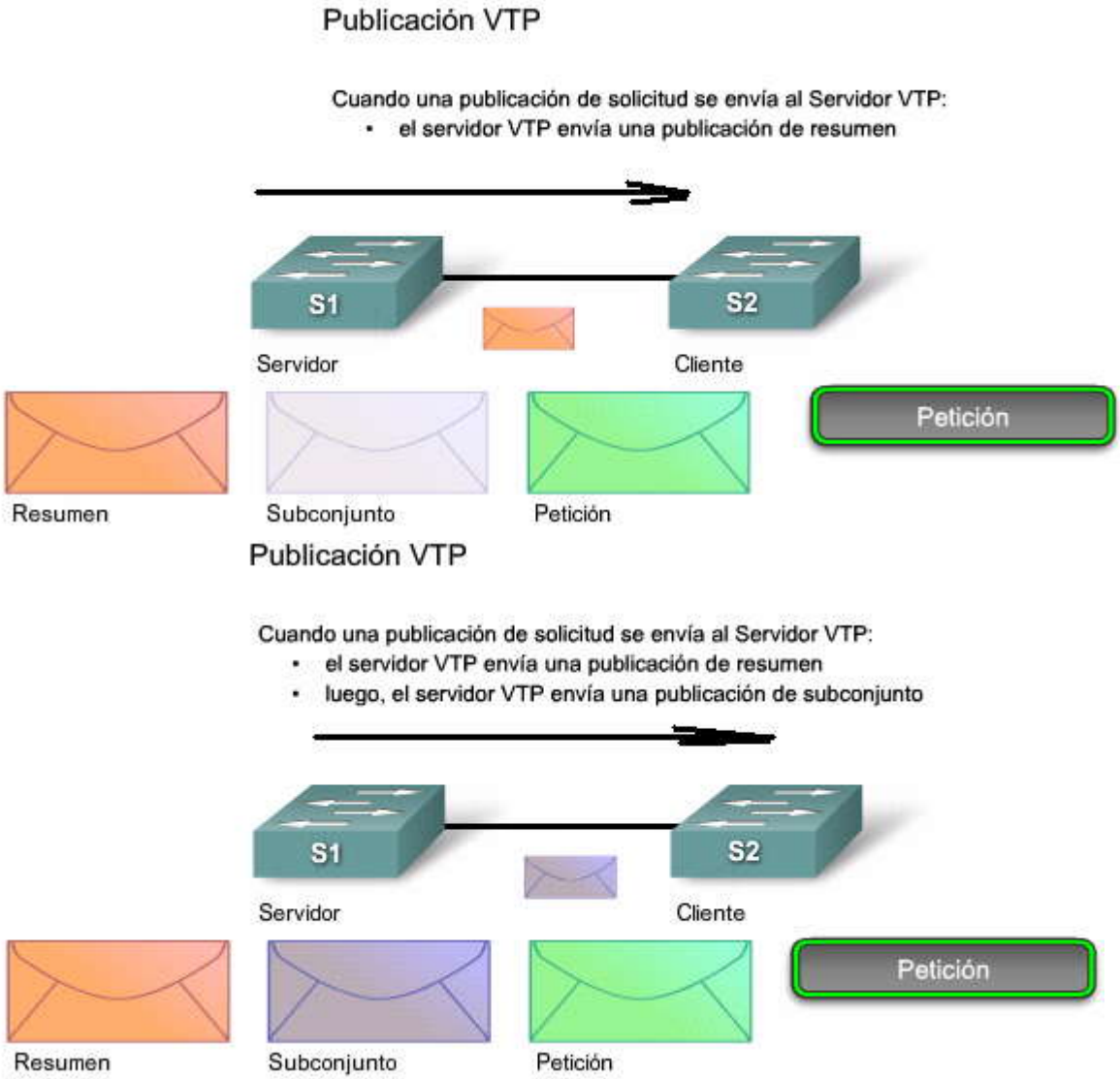
Cuando una publicación de solicitud se envía al servidor del VTP en el mismo dominio del VTP, el servidor del VTP responde enviando una publicación del resumen y luego una publicación de subconjunto. Las publicaciones de solicitud se envían si:

El nombre de dominio del VTP se ha cambiado.
El switch recibe una publicación de resumen con un número de revisión de configuración más alto que el suyo.
Un mensaje de publicación de subconjunto se pierde por alguna razón
El switch se ha reconfigurado

Haga clic en el botón Petición y, luego, en el botón Reproducir que se muestran en la figura para ver una animación sobre las publicaciones del VTP de solicitud.







Detalles de publicaciones del VTP

El VTP utiliza publicaciones para distribuir y sincronizar información sobre los dominios y configuraciones de VLAN. Existen tres publicaciones principales del VTP.

Cada tipo de publicación del VTP envía información sobre varios parámetros utilizados por el VTP. Se presenta una descripción de los campos en cada una de las publicaciones del VTP.

Haga clic en el botón Detalles del resumen que se muestra en la figura.

Publicaciones de resumen

Las publicaciones del resumen comprenden la mayoría del tráfico de publicaciones del VTP. Pase el mouse sobre los campos en la publicación del resumen para ver las descripciones.

Pase el mouse sobre los campos en la publicación del resumen para ver las descripciones.

Haga clic en el botón Detalles de subconjunto que se muestra en la figura.

Publicaciones de subconjunto

Los campos encontrados en una publicación de subconjunto se describen brevemente. No se describen los campos en la información de VLAN.

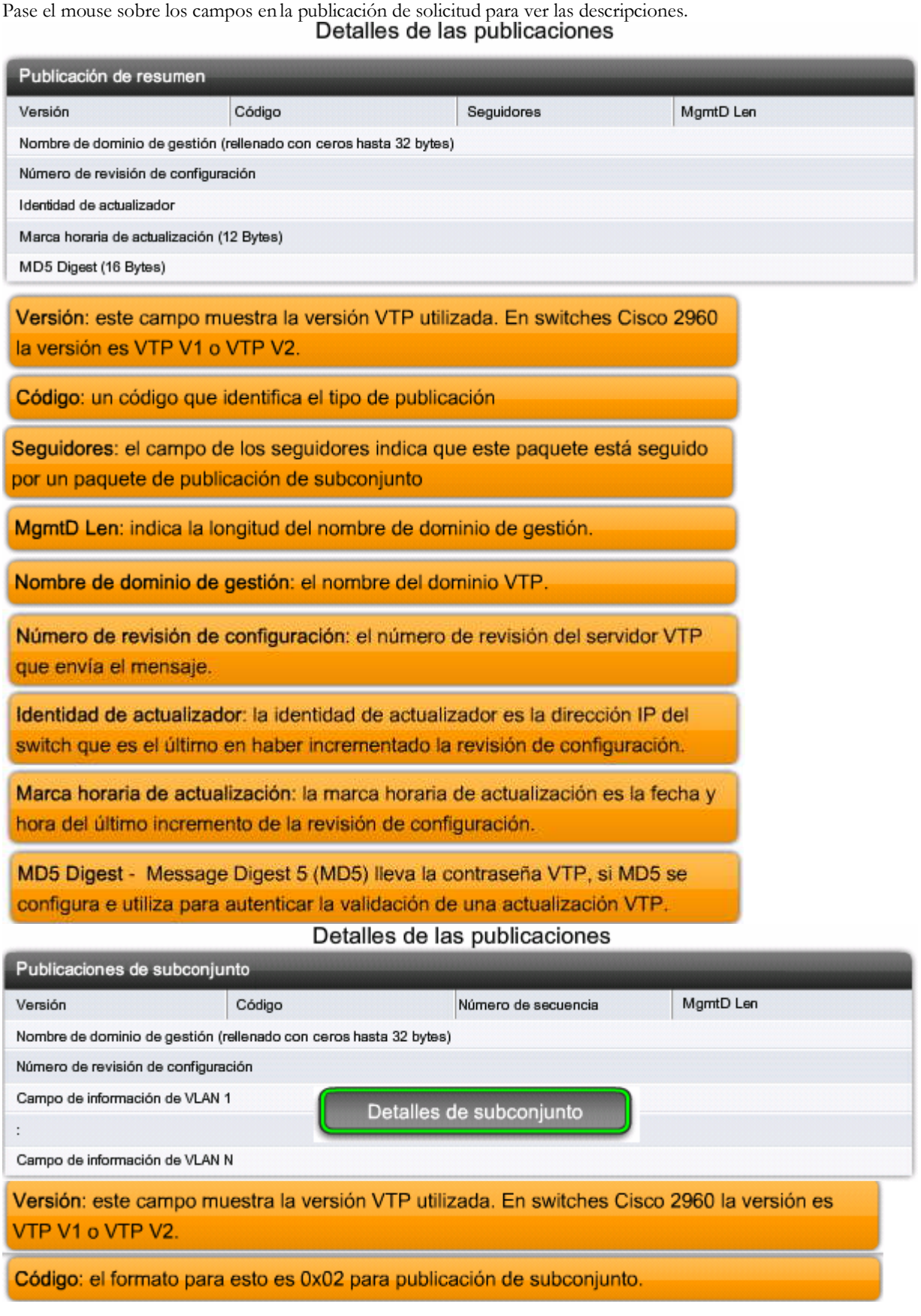
Pase el mouse sobre los campos en la publicación de subconjunto para ver las descripciones.

Haga clic en el botón Detalles de petición que se muestra en la figura.

Publicaciones de solicitud

Los campos encontrados en una publicación de solicitud se describen brevemente.

Pase el mouse sobre los campos en la publicación de solicitud para ver las descripciones.



Número de secuencia: es la secuencia del paquete en el flujo de paquetes que sigue a una publicación de resumen. La secuencia comienza con 1.

Longitud de nombre de dominio: indica la longitud del nombre de dominio de gestión.

Nombre de dominio de gestión: el nombre del dominio VTP.

Número de revisión de configuración: el número de revisión del servidor VTP que envía el mensaje.

El campo de información de VLAN contiene información para cada VLAN y se formatea de la siguiente manera:

Información de la VLAN			
Longitud de información	Estado	Tipo de VLAN	Longitud de nombre de VLAN
ID de VLAN en ISL		Tamaño de MTU	
Índice 802.10			
Nombre de VLAN (relleno con 0 hasta múltiplos de 4 bytes)			

Detalles de las publicaciones

Petición de publicación			
Versión	Código	Rsvd	MgmtD Len
Nombre de dominio de gestión (rellenado con ceros hasta 32 bytes)		Detalles de petición	
Valor de inicio			

Versión: este campo muestra la versión VTP utilizada. En switches Cisco 2960 la versión es VTP V1 o VTP V2.

Código: el formato para esto es 0x03 para una publicación de petición.

Rsvd: un campo reservado

MgmtD Len: indica la longitud del nombre de dominio de gestión.

Nombre de dominio de gestión: el nombre del dominio VTP.

Inicio: Valor: este campo se utiliza cuando existen diferentes publicaciones de subconjunto. Si la primera (n) publicación de subconjunto se ha recibido y todavía no se recibió la subsiguiente (n+1), el switch con VTP activado sólo solicita publicaciones de la (n+1).

4.2.4 MODOS DEL VTP.-

Visión general de modos del VTP

Un switch Cisco, configurado con el software IOS de Cisco, se puede configurar ya sea en modo servidor, cliente o transparente. Estos modos difieren en cómo se utilizan para administrar y publicar los dominios del VTP y VLAN.

Modo servidor

En modo servidor, se pueden crear, modificar y eliminar las VLAN para el dominio completo del VTP. El modo servidor del VTP es el modo predeterminado del switch Cisco. Los servidores del VTP publican sus configuraciones de VLAN a otros switches en el mismo dominio del VTP y sincronizan sus configuraciones de VLAN con otros switches basados en las publicaciones recibidas sobre los enlaces troncales. Los servidores del VTP mantienen la pista de actualizaciones por medio del número de revisión de configuración. Otros switches en el mismo dominio del VTP comparan su número de revisión de configuración con el número de revisión recibido desde un servidor del VTP para ver si necesitan sincronizar su base de datos de VLAN.

Modo cliente

Si un switch está en modo cliente, no se pueden crear, cambiar o eliminar las VLAN. Además, la información de configuración de la VLAN que el switch del cliente del VTP recibe del switch del servidor del VTP se almacena en una base de datos de la VLAN, no en NVRAM. Consecuentemente, los clientes del VTP requieren menos memoria que los servidores del VTP. Cuando un cliente del VTP se desactiva y reinicia, envía una publicación de solicitud a un servidor del VTP para actualizar la información de configuración de la VLAN.

Los switches configurados como clientes del VTP se encuentran más generalmente en redes grandes, porque en una red que consiste de muchos cientos de switches es más difícil coordinar las actualizaciones de la red. A menudo existen muchos administradores de red que trabajan a diferentes horas del día. Si se dispone de sólo unos pocos switches que pueden físicamente mantener las configuraciones de la VLAN, es más fácil controlar las actualizaciones de la VLAN y rastrear qué administradores de red las realizaron.

Para redes grandes, tener switches cliente es también mucho más eficaz. De manera predeterminada, todos los switches están configurados para que sean servidores de VTP. Esta configuración es adecuada para redes de pequeña escala en las que el tamaño de la información de la VLAN es pequeño y la información se almacena más fácilmente en la NVRAM de los switches. En redes grandes de muchos cientos de switches, el administrador de red debe decidir si el costo de los switches que compra con suficiente NVRAM para almacenar la información de la VLAN duplicada es demasiado. Un administrador de red consciente del costo podría elegir configurar unos pocos switches bien equipados como servidores de VTP y luego utilizar esos switches con menos memoria como clientes de VTP. Aunque un debate sobre la redundancia de la red está más allá del ámbito de este curso, sepa que el número de servidores de VTP se podría elegir para proveer el grado de redundancia que se desea en la red.

Modo transparente

Los switches configurados en modo transparente envían publicaciones de VTP que reciben en sus puertos troncales hacia otros switches en la red. Los switches en modo transparente del VTP no publican su configuración de VLAN y no sincronizan su configuración de VLAN con ningún otro switch. Configure un switch en modo transparente cuando tiene las configuraciones de la VLAN que tienen importancia local y no deben compartirse con el resto de la red.

En modo transparente, las configuraciones de VLAN se guardan en la NVRAM (pero no se publican a otros switches). De esta manera, la configuración está disponible después de la recarga de un switch. Esto significa que cuando se reinicia un switch en modo transparente del VTP, no vuelve a modo servidor del VTP de manera predeterminada, pero permanece en modo transparente del VTP.

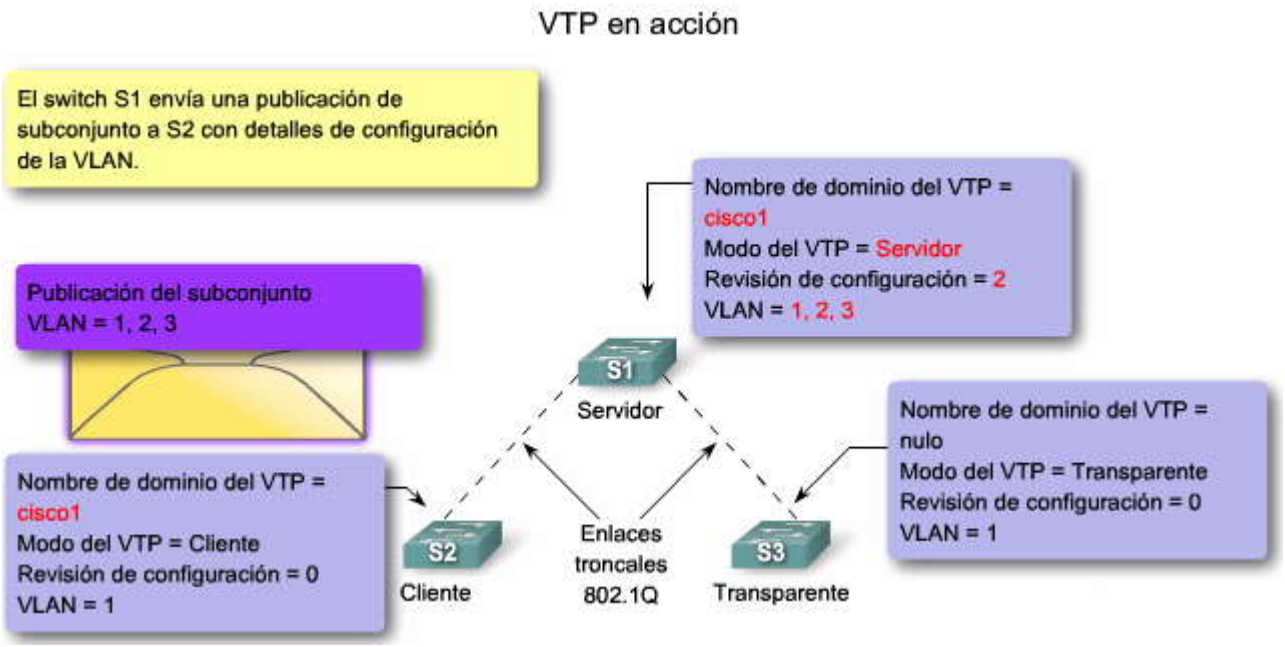
Modos VTP

	Servidor VTP	Cliente VTP	VTP transparente
Descripción	Configuraciones de VLAN y dominio de gestión.	Actualiza las configuraciones VTP, los switches cliente VTP no pueden cambiar las configuraciones VLAN.	Puede administrar configuraciones de VLAN locales. Configuraciones de VLAN locales, no compartidas con la red VTP.
¿Responder a publicaciones VTP?	Participa por completo.	Participa por completo.	Sólo reenvía publicaciones VTP.
¿Se preserva la configuración de VLAN global al reiniciar?	Sí, las configuraciones globales almacenadas en NVRAM.	No, las configuraciones globales almacenadas en RAM, no en NVRAM.	No, la configuración de VLAN local sólo se almacena en NVRAM.
¿Actualizar otros switches con VTP activado?	Sí	Sí	No

VTP en acción

Verá ahora cómo las diversas características del VTP se unen para distribuir y sincronizar el dominio y las configuraciones de VLAN en una red habilitada por el VTP. La animación comienza con tres switches nuevos: S1, S2 y S3 configurados de fábrica de manera predeterminada y finaliza con los tres switches configurados y participando en una red habilitada por el VTP.

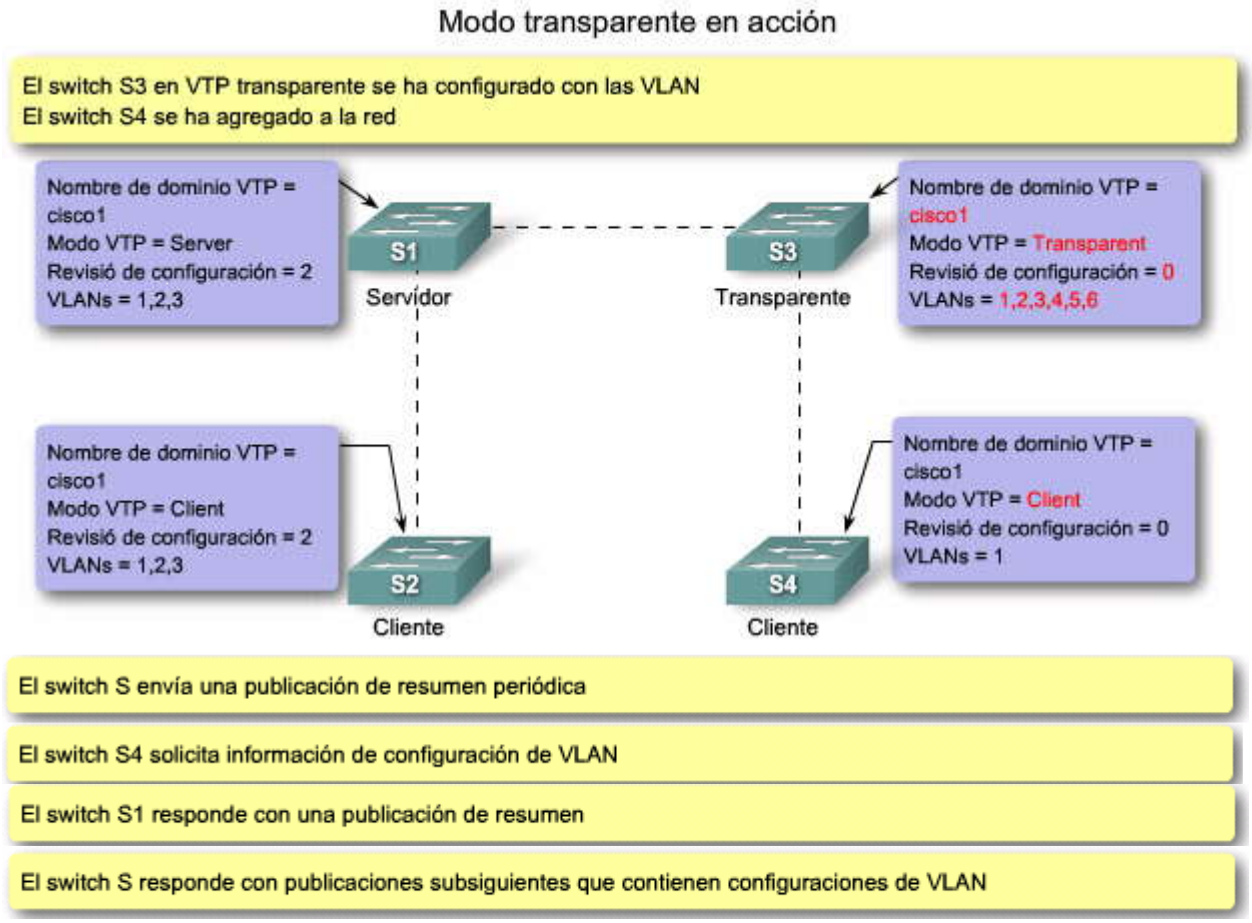
Puede pausar y rebobinar la animación para reflexionar y revisar este proceso.



Ha visto cómo funciona el VTP con tres switches. Esta animación examina en más detalle cómo un switch configurado en modo transparente de VTP admite la funcionalidad del VTP.

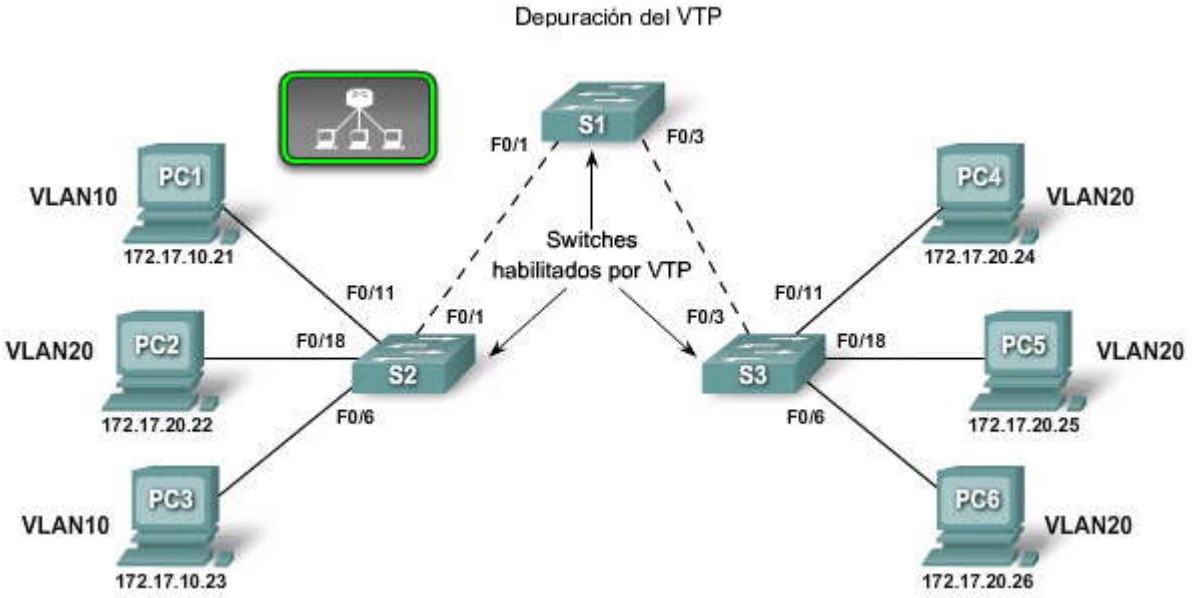
Haga clic en el botón Reproducir que se muestra en la figura.

Puede pausar y rebobinar la animación para reflexionar y revisar este proceso.



4.2.5 DEPURACION DEL VTP.-

La depuración del VTP evita flooding innecesaria de información de broadcast desde una VLAN a través de todos los enlaces troncales en un dominio de VTP. La depuración del VTP permite que los switches negocien qué VLAN están asignadas a puertos en otros extremos de un enlace troncal y, consiguientemente, depuren aquellas que no están asignadas a puertos en el switch remoto. La depuración se deshabilita de manera predeterminada. La depuración del VTP se habilita utilizando vtp pruning (comando de configuración local). Necesita habilitar la depuración en sólo un switch del servidor de VTP en el dominio. En la figura habilitaría la depuración del VTP en el switch S1. La figura muestra una red con VLAN 10 y VLAN 20 configuradas. El switch S3 tiene la VLAN 20 configurada y el switch S2 tiene la VLAN 10 y VLAN 20 configuradas. Examine la topología en la figura y, luego, haga clic para ver las configuraciones del switch.



Depuración del VTP

```
S1#show interfaces trunk
Port  Mode  Encapsulation  Status      Native vlan
Fa0/1 on    802.1q         trunking    1
Fa0/3 on    802.1q         trunking    1

Port  Vlans allowed on trunk
Fa0/1 1-1005
Fa0/3 1-1005

Port  Vlans allowed and active in management domain
Fa0/1 1,10,20,1002,1003,1004,1005
Fa0/3 1,10,20,1002,1003,1004,1005

Port  Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,20,1002,1003,1004,1005
Fa0/3 1,10,20,1002,1003,1004,1005
S1#
```

Resultados del switch

Switch S1

```
S2#show interfaces trunk
Port  Mode  Encapsulation  Status      Native vlan
Fa0/1 on    802.1q         trunking    1

Port  Vlans allowed on trunk
Fa0/1 1-1005

Port  Vlans allowed and active in management domain
Fa0/1 1,10,20,1002,1003,1004,1005

Port  Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,20,1002,1003,1004,1005
S2#
```

```
S3#show interfaces trunk
Port  Mode  Encapsulation  Status       Native vlan
Fa0/3 on    802.1q         trunking     1

Port  Vlans allowed on trunk
Fa0/3 1-1005

Port  Vlans allowed and active in management domain
Fa0/3 1,10,20,1002,1003,1004,1005

Port  Vlans in spanning tree forwarding state and not pruned
Fa0/3 1,10,20,1002,1003,1004,1005
S3#
```

Depuración del VTP en acción

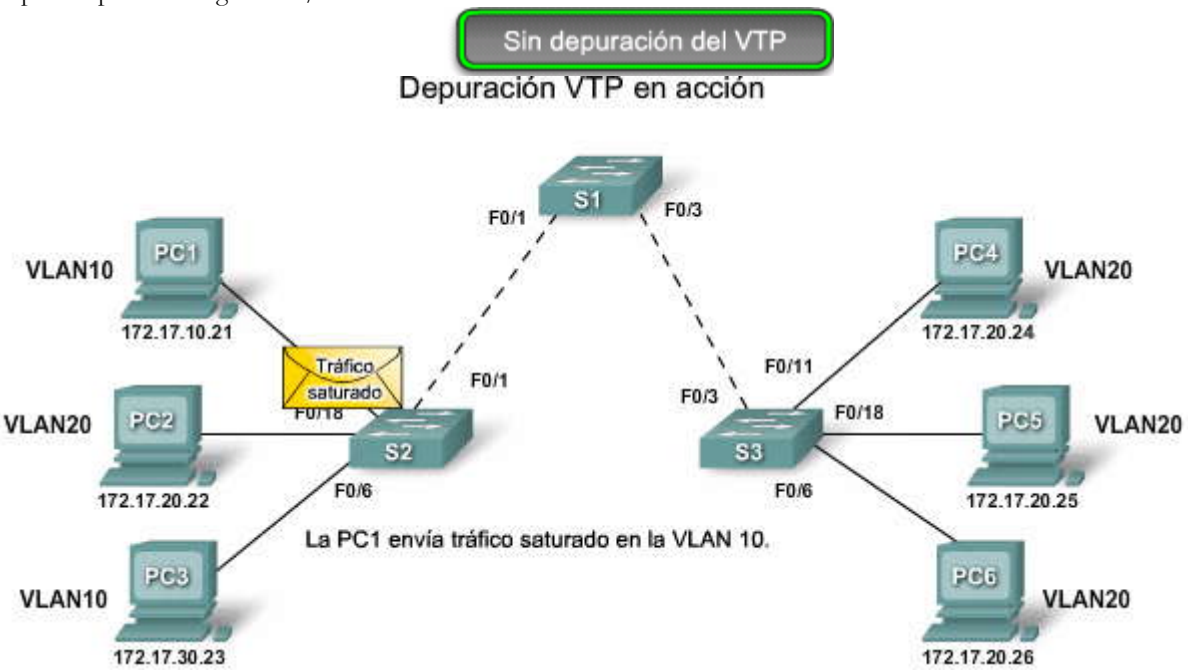
Recuerde que una VLAN crea un dominio de broadcast aislado. Un switch satura el tráfico de broadcast, multicast y unicast desconocido a través de los enlaces troncales dentro de un dominio VTP. Cuando una computadora o un dispositivo envía un broadcast por una VLAN, por ejemplo la VLAN 10 en la figura, el tráfico de broadcast recorre todos los enlaces troncales a través de la red hacia todos los puertos en todos los switches en la VLAN 10. En la figura todos los switches S1, S2 y S3 reciben tramas de broadcast desde la PC1. El tráfico de broadcast desde la PC1 consume el ancho de banda en el enlace troncal entre S1 y S3 y consume el tiempo del procesador en S1 y S2. El enlace entre los switches S1 y S3 no lleva tráfico de la VLAN 10, por lo tanto, es un candidato para la depuración del VTP.

Haga clic en el botón Reproducir que se muestra en la figura para ver cómo se maneja el tráfico de saturación de la VLAN en una red sin depuración del VTP.

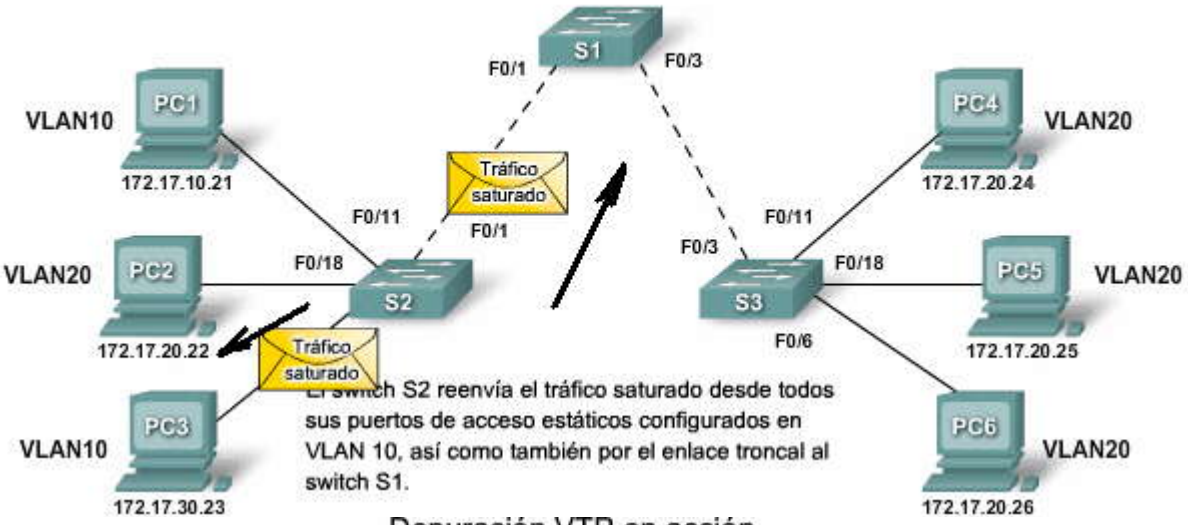
Depuración del VTP

Haga clic en el botón de Depuración del VTP y, luego, en Reproducir para ver la animación sobre cómo se maneja el tráfico de saturación de la VLAN en una red con depuración del VTP.

El tráfico de saturación es detenido al ingresar a la red troncal que conecta los switches S1 y S2. La depuración del VTP sólo depura el puerto de egreso F0/1 en el switch S2.

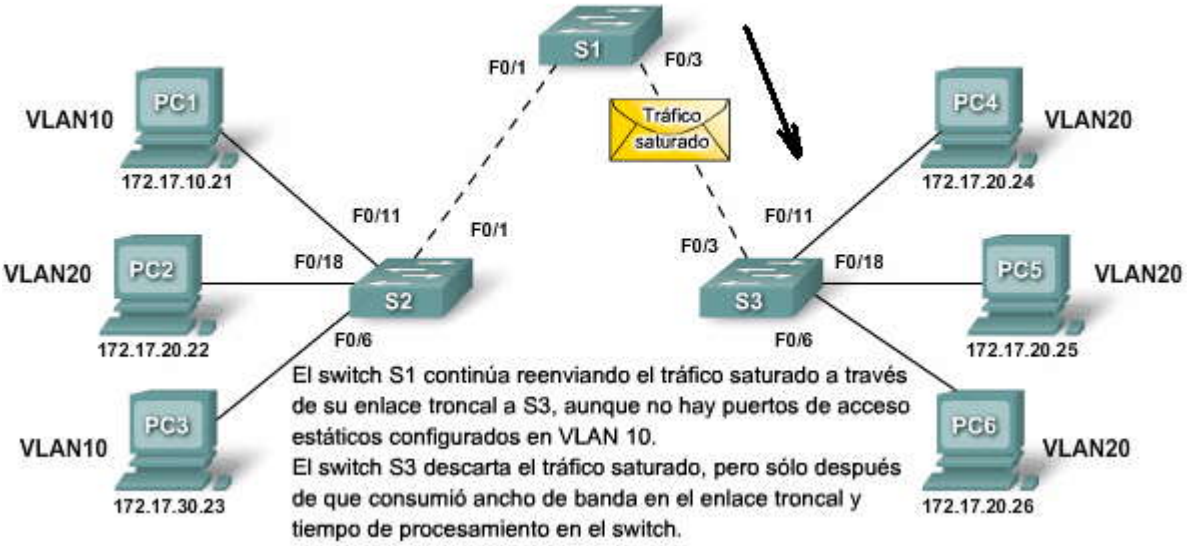


Depuración VTP en acción



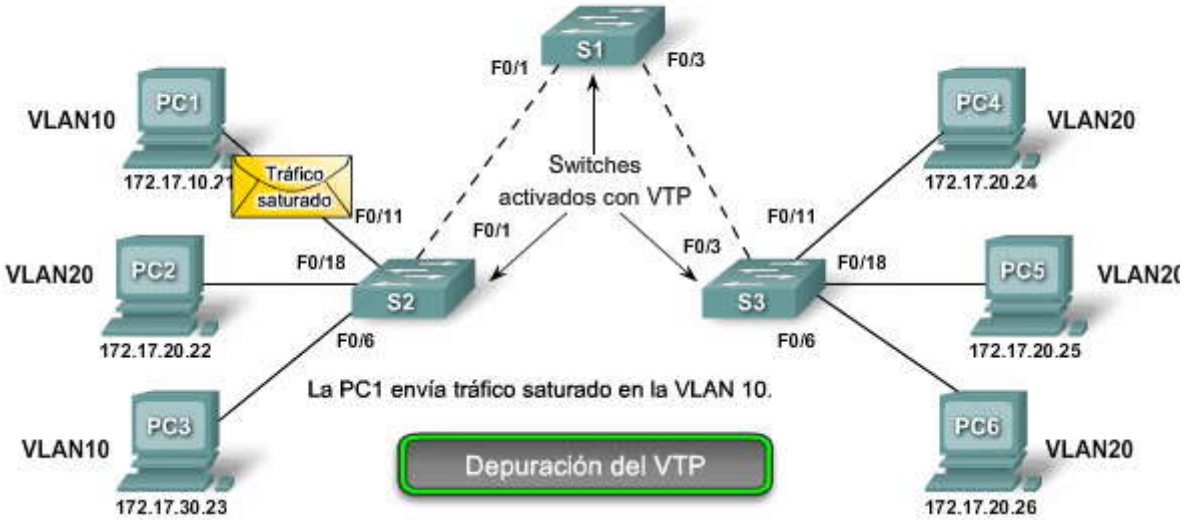
El switch S2 reenvía el tráfico saturado desde todos sus puertos de acceso estáticos configurados en VLAN 10, así como también por el enlace troncal al switch S1.

Depuración VTP en acción



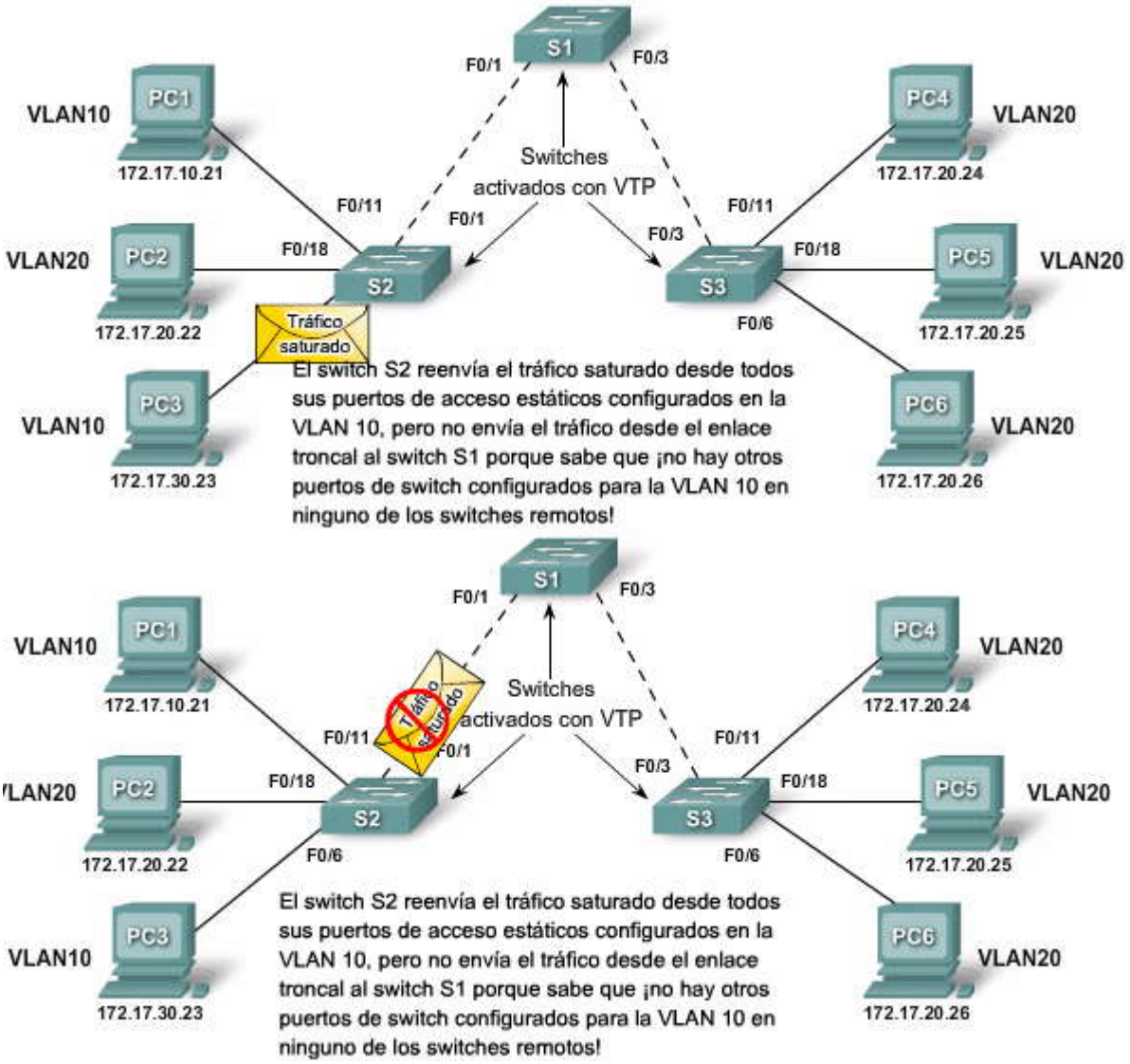
El switch S1 continúa reenviando el tráfico saturado a través de su enlace troncal a S3, aunque no hay puertos de acceso estáticos configurados en VLAN 10.
El switch S3 descarta el tráfico saturado, pero sólo después de que consumió ancho de banda en el enlace troncal y tiempo de procesamiento en el switch.

Depuración VTP en acción



La PC1 envía tráfico saturado en la VLAN 10.

Depuración del VTP



Depuración del VTP habilitada

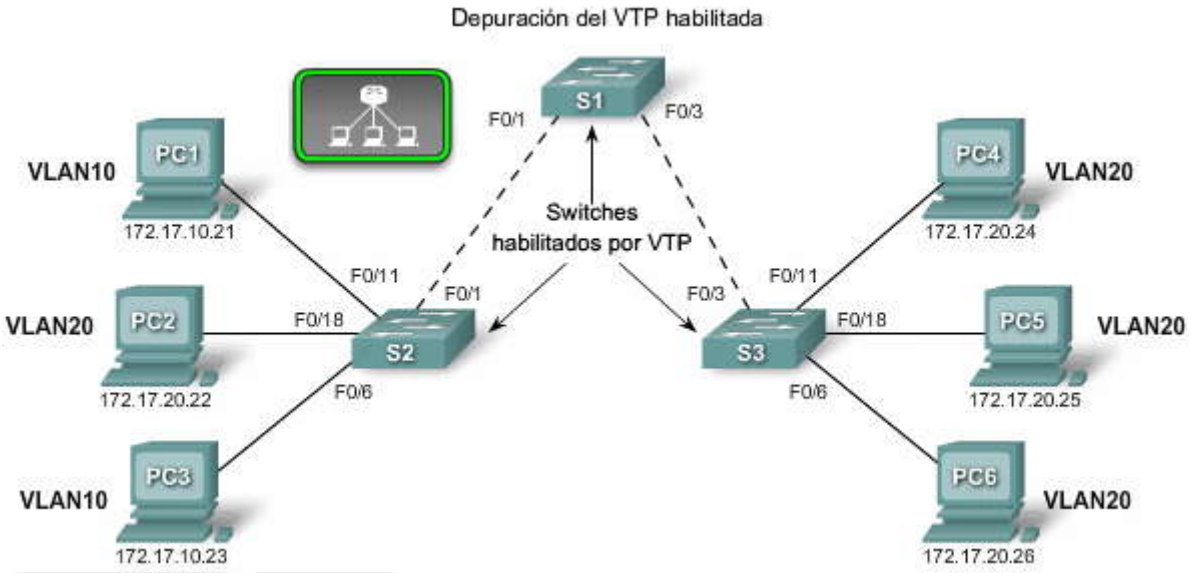
La figura muestra una topología de la red que tiene switches S1, S2 y S3 configurados con depuración de VTP. Cuando se habilita la depuración del VTP en una red, ésta reconfigura los enlaces troncales basados en qué puertos están configurados con cuáles VLAN.

Haga clic en el botón Switch S1 que se muestra en la figura.

El área resaltada muestra que el enlace troncal en el puerto F0/1 permite el tráfico de VLAN 10. La depuración del VTP sólo depura el puerto de egreso.

Haga clic en el botón Switch S2 que se muestra en la figura.

El área resaltada muestra que el enlace troncal en el puerto F0/1 no permite el tráfico de VLAN 10. VLAN 10 no está en la lista. Para más detalles sobre depuración del VTP, visite: http://www.cisco.com/en/US/products/ps6406/products_configuration_guide_chapter09186a008081d9ac.html#wp1035139.




```
S1#show interfaces trunk
Port  Mode   Encapsulation   Status      Native vlan
Fa0/1 on     802.1q          trunking    1
Fa0/3 on     802.1q          trunking    1

Port  Vlans allowed on trunk
Fa0/1 1-1005
Fa0/3 1-1005

Port  Vlans allowed and active in management domain
Fa0/1 1,10,20,1002,1003,1004,1005
Fa0/3 1,10,20,1002,1003,1004,1005

Port  Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,20,1002,1003,1004,1005
Fa0/3 1,10,20,1002,1003,1004,1005
S1#
```

Switch S1

```
S2#show interfaces trunk
Port  Mode  Encapsulation   Status      Native vlan
Fa0/1 on    802.1q          trunking    1

Port  Vlans allowed on trunk
Fa0/1 1-1005

Port  Vlans allowed and active in management domain
Fa0/1 1,10,20,1002,1003,1004,1005

Port  Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,20,1002,1003,1004,1005
S2#
```

Switch S2

4.3 CONFIGURAR EL VTP.-

4.3.1 CONFIGURACION DEL VTP.-

Guía de Configuración del VTP

Ahora que está familiarizado con la funcionalidad del VTP, está listo para aprender a configurar un switch de Cisco Catalyst que usa VTP. La topología muestra la topología de referencia para este capítulo. El VTP será configurado sobre esta topología.

Haga clic en el botón Tabla que se muestra en la figura.

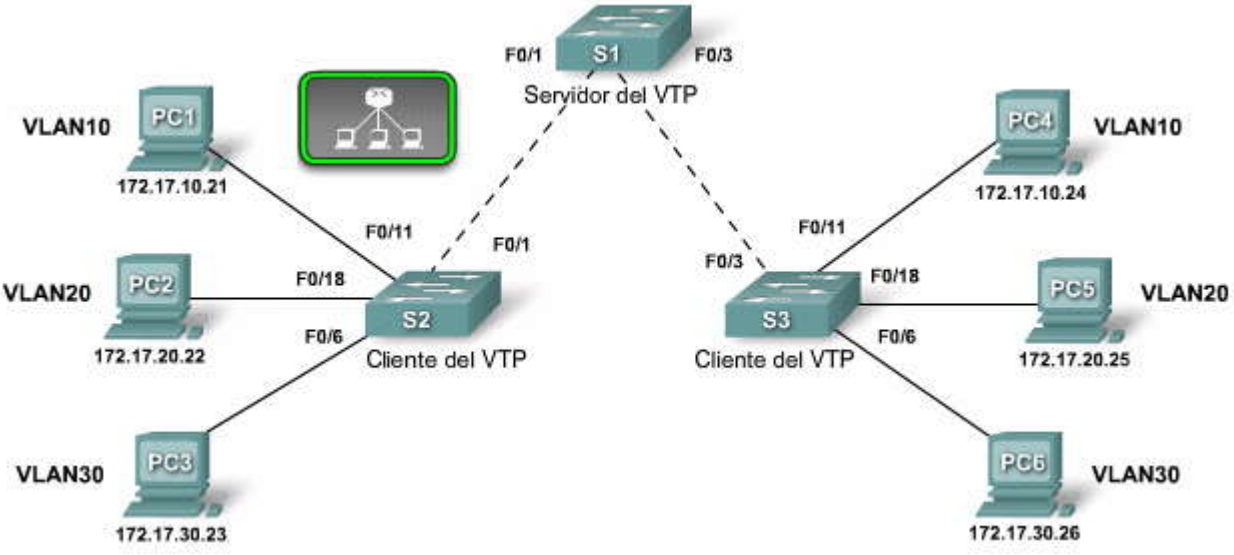
Switches del servidor del VTP

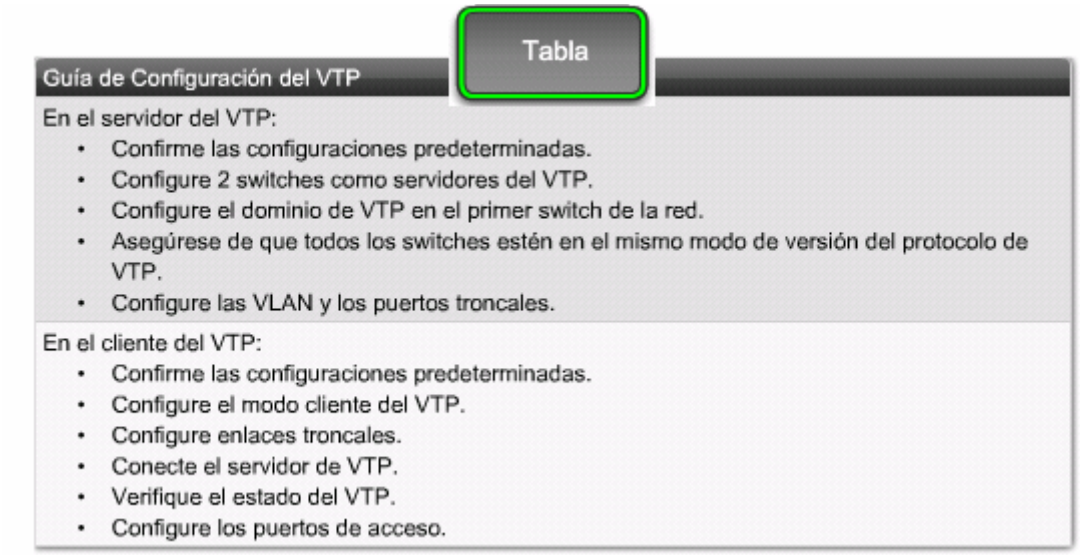
Siga estos pasos y guías asociadas para asegurarse de que configura el VTP con éxito:

- Confirme que todos los switches que va a configurar hayan sido previamente configurados de manera predeterminada.
- Siempre reconfigure el número de revisión de configuración antes de instalar un switch previamente configurado en un dominio del VTP. No reconfigurar el número de revisión de configuración permite la potencial discontinuidad en la configuración de la VLAN, a través del resto de los switches en el dominio del VTP.
- Configure al menos dos switches del servidor del VTP en su red. Como sólo los switches del servidor pueden crear, eliminar y modificar las VLAN, debe asegurarse de tener un servidor del VTP de respaldo en caso de que el servidor VTP principal se desactive. Si todos los switches en la red están configurados en modo cliente del VTP, no puede crear nuevas VLAN en la red.
- Configure un dominio de VTP en el servidor del VTP. La configuración del dominio del VTP en el primer switch habilita al VTP para comenzar la publicación de la información de la VLAN. Otros switches conectados a través de enlaces troncales reciben la información del dominio del VTP automáticamente a través de las publicaciones del VTP.
- Si hay un dominio de VTP existente, asegúrese de coincidir exactamente con el nombre. Los nombres de dominio del VTP distinguen entre mayúscula y minúscula.
- Si está configurando un contraseña para el VTP, asegúrese de que sea la misma contraseña configurada en todos los switches en el dominio que necesitan poder intercambiar información del VTP. Los switches sin contraseña o con contraseña incorrecta rechazan las publicaciones del VTP.
- Asegúrese de que todos los switches estén configurados para utilizar la misma versión de protocolo del VTP. La versión 1 del VTP no es compatible con la versión 2 del VTP. De manera predeterminada, los switches Cisco Catalyst 2960 ejecutan la versión 1 pero pueden ejecutar la versión 2. Cuando la versión del VTP se configura a versión 2, todos los switches con versión 2 en el dominio se autoconfiguran para utilizar la versión 2 a través del proceso de anuncio del VTP. Cualquier versión 1: sólo los switches no pueden participar en el dominio VTP después de ese punto.
- Cree la VLAN después de haber habilitado el VTP en el servidor del VTP. Se eliminan las VLAN creadas antes de habilitar el VTP. Siempre asegúrese de que los puertos troncales estén configurados para interconectar switches en el dominio del VTP. La información del VTP sólo se intercambia en los puertos troncales.

Switches del cliente de VTP

- Como en el switch del servidor del VTP, confirme que las configuraciones predeterminadas estén presentes.
- Configure el modo cliente del VTP. Recuerde que el switch no está en modo cliente del VTP de manera predeterminada. Tiene que configurar este modo.
- Configure los enlaces troncales. El VTP funciona sobre los enlaces troncales.
- Conecte al servidor del VTP. Cuando se conecta a un servidor del VTP u otro switch habilitado por el VTP, toma un momento para que las diversas publicaciones vayan y vuelvan al servidor del VTP.
- Verifique el estado del VTP Antes de comenzar a configurar los puertos de acceso, confirme que el modo revisión y número de VLAN hayan sido actualizados.
- Configure los puertos de acceso Cuando un switch es un modo cliente del VTP, no se pueden agregar VLAN nuevas. Solamente puede asignar puertos de acceso a las VLAN existentes.





Configuración del VTP: Paso 1 - Configure el servidor del VTP

Los próximos tres temas mostrarán cómo configurar el servidor del VTP y dos clientes del VTP.Inicialmente ninguno de los dispositivos está conectado.

La topología resalta el switch S1. Configurará este switch para que sea el servidor del VTP. Los comandos para configurar los puertos troncales se proveen en la interfaz F0/1.

Haga clic en el botón Confirmar detalles en la figura.

El resultado del comando show vtp status confirma que el switch es de manera predeterminada un servidor del VTP. Como todavía no se han configurado las VLAN, el número de revisión está aún configurado en 0, y el switchno pertenece al dominio del VTP.

Si el switch no fue todavía configurado como servidor del VTP, podría configurarlo utilizando el comando vtp mode {server}.

Haga clic en el botón Configurar nombre de dominio que se muestra en la figura.

El nombre de dominio está configurado usando el comando vtp domain domain-name. En la figura, el switch S1 ha sido configurado con el nombre de dominio cisco1.

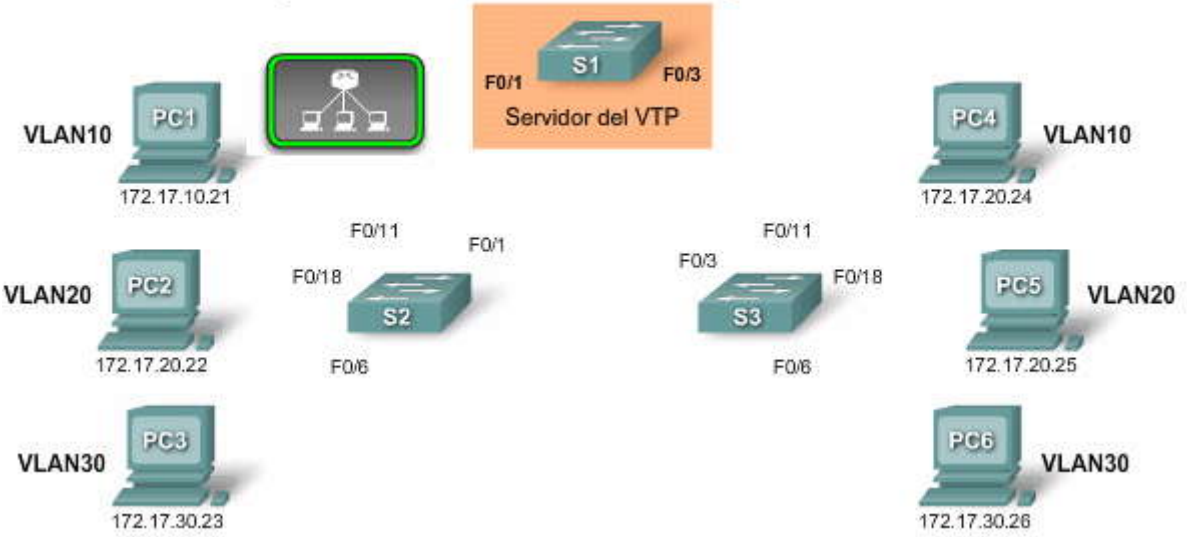
Por razones de seguridad, se podría configurar una contraseña con el comando vtp password password.

Haga clic en el botón Configurar versión que se muestra en la figura.

La mayoría de los switches puede admitir la versión 1 y 2 del VTP. Sin embargo, la configuración predeterminada para los switches Catalyst 2960 es la versión 1. Cuando el comando vtp version 1 es introducido al switch, nos informa que el switch ya está configurado para que esté en la versión 1.
Haga clic en el botón Agregar VLAN y enlaces troncales que se muestra en la figura.
Asuma que se han configurado tres VLAN y se les han asignado nombresde VLAN. La salida en la figura está mostrando el resultado de estos cambios.

Puede usar la versión no de los comandos.

Configuración del VTP: Paso 1 - Configure el sevidor del VTP




```
S1#show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name:
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest              : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
S1#
```

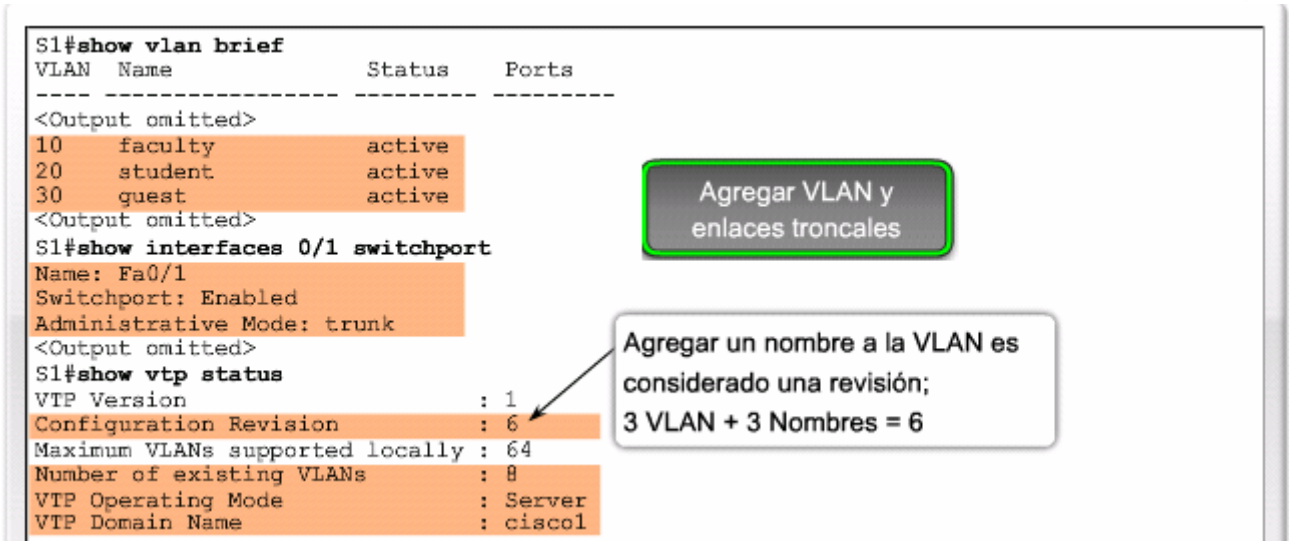
Confirmar detalles

```
S1#configure terminal
S1(config)#vtp domain cisco1
Changing VTP domain name from NULL to cisco1
S1(config)#exit
S1#show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : cisco1
<Output omitted>
S1#
```

Configurar nombre de dominio

```
S1(config)#vtp version 1
VTP mode already in V1.
S1(config)#exit
S1#
```

Configurar versión



La topología resalta los switches S2 y S3. Se le mostrará la configuración de cliente del VTP para S2. Para configurar el S3 como cliente de VTP, seguirá el mismo protocolo.

Haga clic en el botón Confirmar predeterminados para verificar el estado del switch.

Antes de configurar un switch como cliente de VTP, verifique su estado de VTP actual. Una vez que haya confirmado el estado, configurará el switch para que opere en modo cliente del VTP.

Haga clic en el botón Habilitar modo de cliente del VTP para ver cómo se configura un switch para modo cliente del VTP.

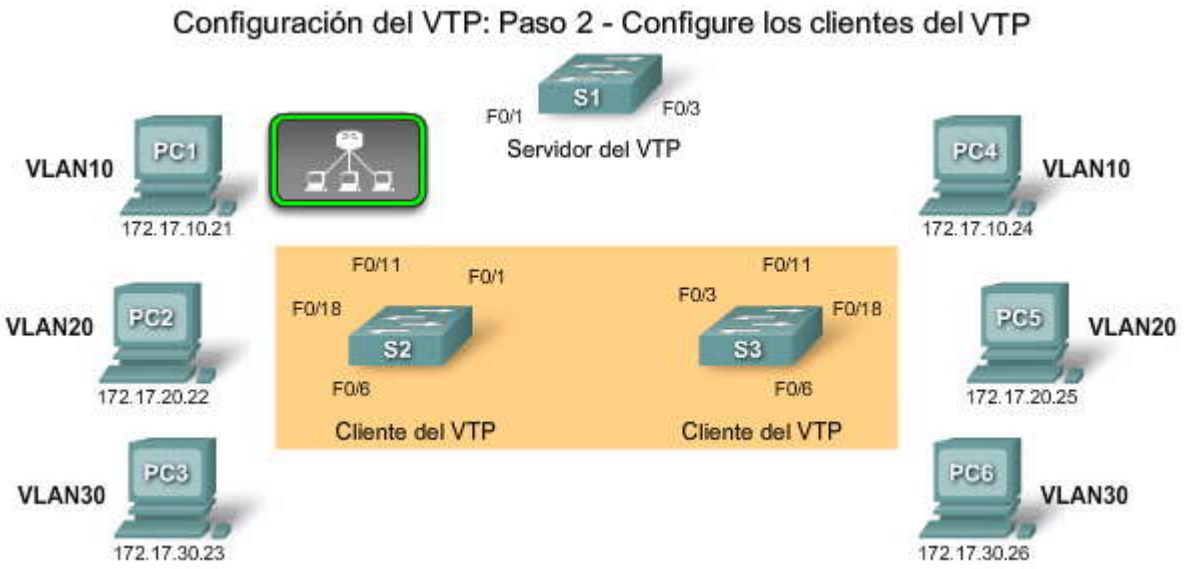
Configure el modo cliente del VTP usando la siguiente sintaxis del comando del IOS de Cisco:

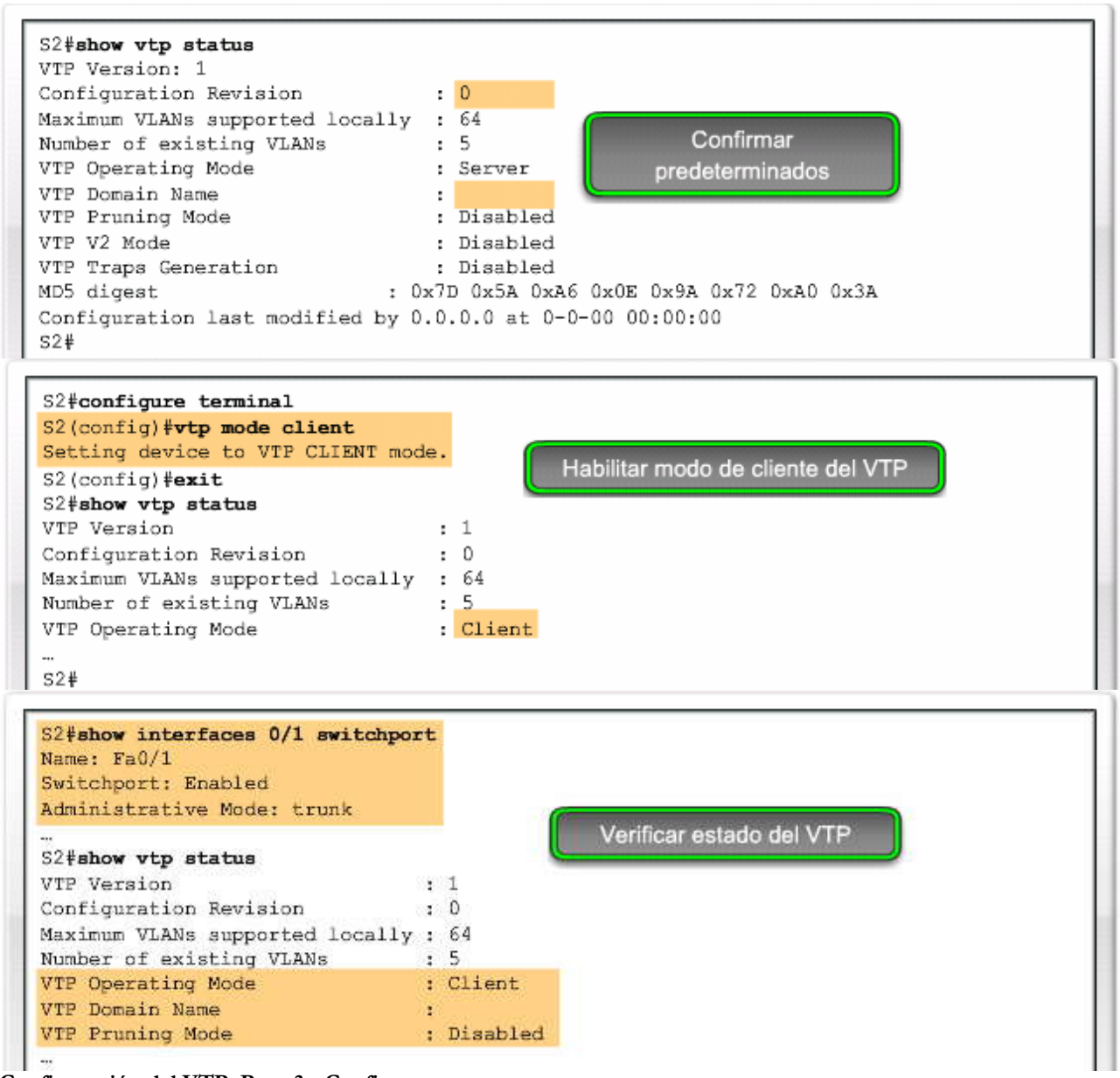
Ingrese al modo de configuración global mediante el comando configure terminal.

Configure el switch en modo cliente con el comando vtp mode {client}.

Si necesita volver a configurar el VTP a los valores predeterminados, puede utilizar la versión no de los comandos.

Haga clic en el botón Verificar estado del VTP para ver el resto de la configuración del cliente del VTP.





Configuración del VTP: Paso 3 - Confirmar y conectar

Después de configurar el servidor principal del VTP y los clientes del VTP, conectará el switch S2 del cliente del VTP al servidor del VTP del switch S1.

La topología resalta los enlaces troncales que se agregarán a esta topología. En la figura el switch S2 se conectará al switch S1. Luego se configurará el switch S2 para admitir a las computadoras PC1 hasta PC3. El mismo procedimiento se aplicará al switch S3, aunque los comandos para S3 no se muestren.

Confirmar la operación del VTP

Haga clic en el botón Confirmar operación del VTP en la figura.

Existen dos comandos del IOS de Cisco para confirmar que el dominio de VTP y las configuraciones de VLAN se han transferido al switch S2. Use el comando show VTP status para verificar lo siguiente:

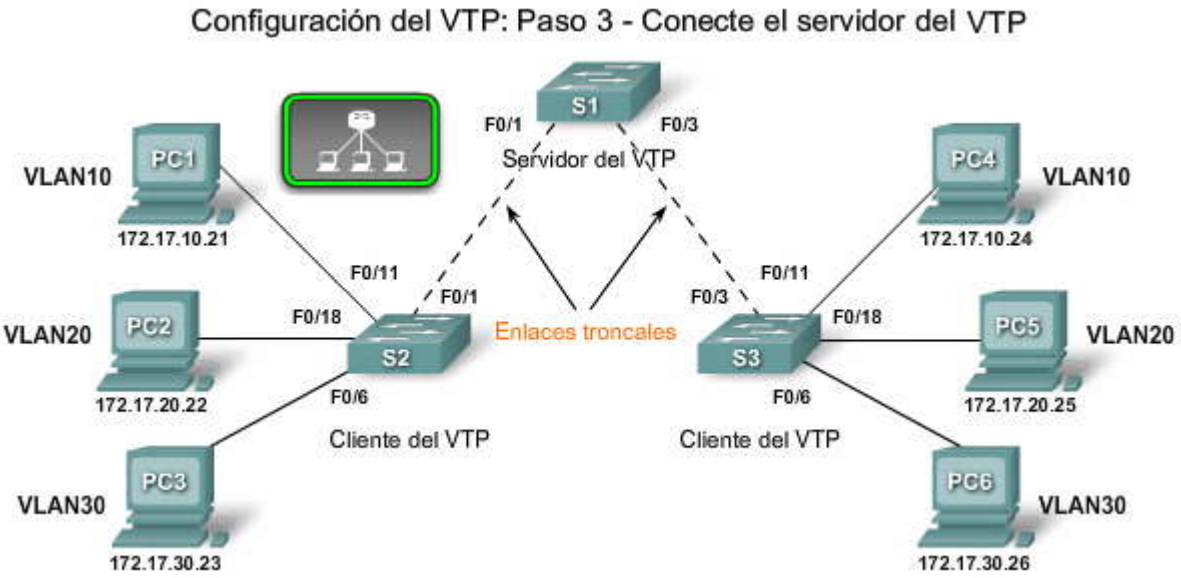
- El número de revisión de configuración se ha incrementado a 6.
- Existen ahora tres nuevas VLAN indicadas por el número existente de VLAN que muestra 8.
- El nombre de dominio se ha cambiado a cisco1.

Utilice el comando show vtp counters para confirmar que se realizaron las publicaciones.

Configure los puertos de acceso

Haga clic en el botón Configurar puertos de acceso que se muestra en la figura.

El resaltado superior en la salida de la pantalla confirma que el switch S2 está en modo cliente del VTP. La tarea ahora es configurar el puerto F0/18 en el switch S2 para que esté en la VLAN 20. El área inferior resaltada muestra el comando del IOS de Cisco utilizado para configurar el puerto F0/18 en el switch S2 para que esté en la VLAN 20.




```
S2#show vtp status
VTP Version                     : 1
Configuration Revision          : 6
Maximum VLANs supported locally : 64
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : cisco1
<output omitted>
S2#show vtp counters
VTP statistics                  :
Summary advertisements received : 1
Subset advertisements received  : 1
Request advertisements received : 0
Summary advertisements transmitted : 1
Subset advertisements transmitted : 1
<output omitted>
S2#
```

Confirmar operación del VTP

El área resaltada muestra que el switch S2 ha sido actualizado y ahora tiene tres nuevas VLAN.

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 20
%VTP VLAN configuration not allowed when device is in CLIENT mode.
S2(config)#interface fastEthernet 0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#exit
S2(config)#exit
S2#
```

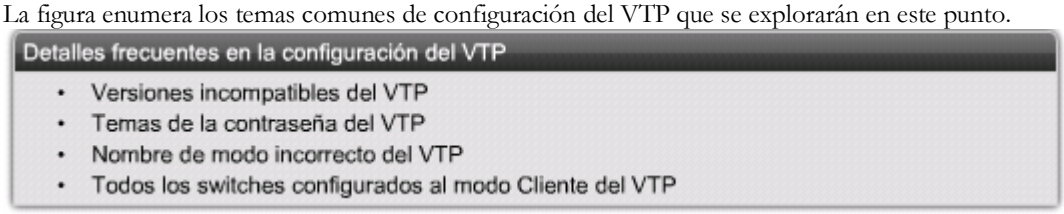
Configurar puertos de acceso

4.3.2 CONFIGURACION DEL VTP PARA SOLUCIONAR PROBLEMAS.-

Solución de problemas de las conexiones del VTP

Ha aprendido cómo se puede utilizar el VTP para simplificar la administración de una base de datos de VLAN a través de múltiples switches. En este punto, aprenderá sobre los problemas más comunes de configuración del VTP.Esta información, combinada con sus capacidades de configuración del VTP, le ayudará a solucionar los problemas de configuración del VTP.

La figura enumera los temas comunes de configuración del VTP que se explorarán en este punto.



Versiones incompatibles del VTP

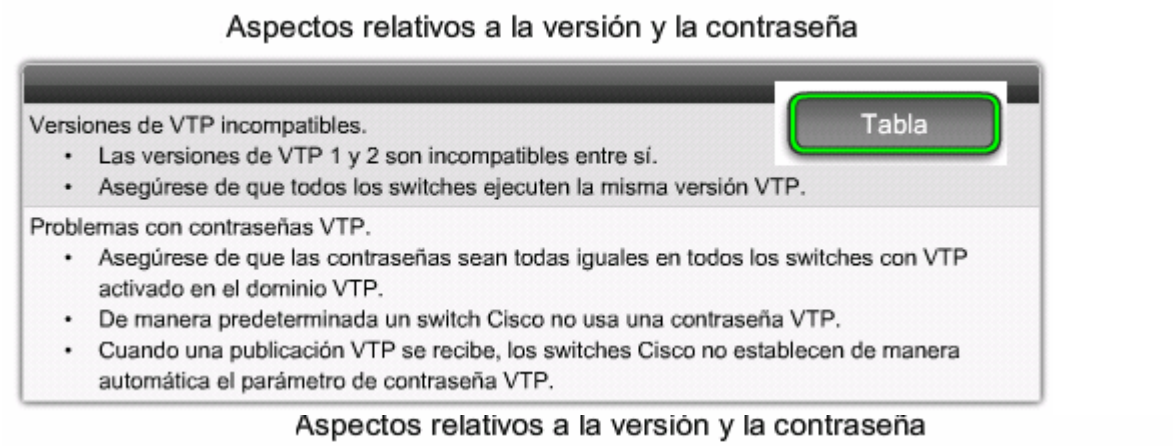
Las versiones 1 y 2 del VTP son incompatibles una con la otra. Los modernos switches de Cisco Catalyst, como el 2960, están configurados para usar la versión 1 del VTP de manera predeterminada. Sin embargo, switches más viejos pueden admitir la versión 1 del VTP. Los switches que sólo admiten la versión 1 no pueden participar en el dominio del VTP junto con los switches de la versión 2. Si su red contiene switches que admiten sólo los de la versión 1, necesita configurar manualmente los switches de la versión 2 para que operen en el modo de versión 1.

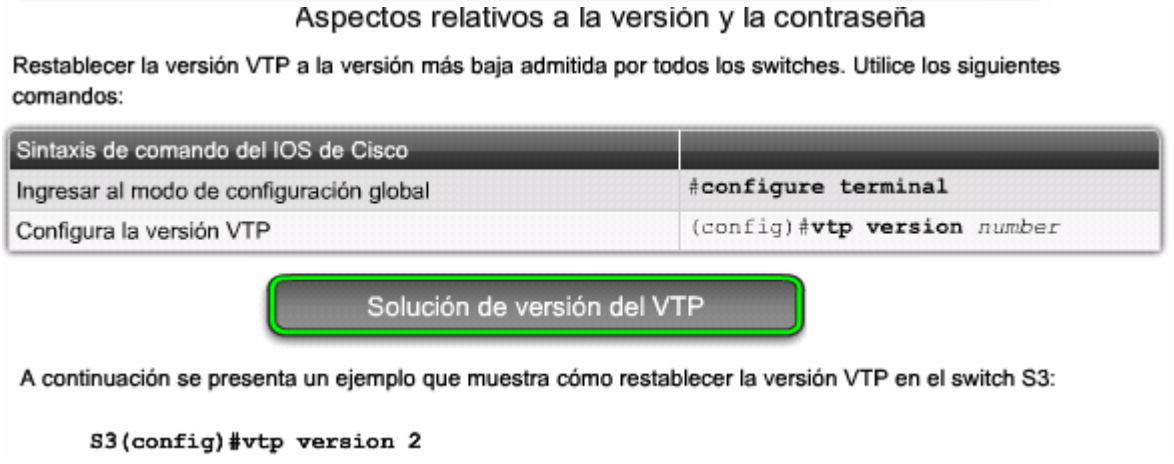
Haga clic en el botón Solución de versión del VTP que se muestra en la figura.

Temas de contraseña del VTP

Cuando utiliza una contraseña del VTP para controlar la participación en el dominio delVTP, asegúrese de que la contraseña esté correctamente configurada en todos los switches en el dominio del VTP. Olvidarse de configurar una contraseña del VTP es un problema muy común. Si se utiliza una contraseña, ésta debe ser configurada en cada switchen el dominio. De manera predeterminada, un switch Cisco no usa una contraseña de VTP. El switch no configura automáticamente el parámetro de contraseña, a diferencia de otros parámetros que se configuran automáticamente cuando se recibe una publicación del VTP.

Haga clic en el botón Solución de contraseña del VTP que se muestra en la figura.





Aspectos relativos a la versión y la contraseña

Configurar una contraseña VTP en cada switch con VTP activado mediante el uso de estos comandos:

Sintaxis de comando del IOS de Cisco	
Ingresar al modo de configuración global	`#configure terminal`
Configura la contraseña VTP	`(config)#vtp password password`

Solución de contraseña del VTP

A continuación se presenta un ejemplo que muestra cómo configurar la contraseña VTP en el switch S3:

```
S3(config)#vtp password cisco
```

Nombre incorrecto de dominio del VTP

El nombre de dominio del VTP es un parámetro clave que se configura en un switch. Un dominio del VTP configurado incorrectamente afecta la sincronización de la VLAN entre switches. Como aprendió anteriormente, si un switch recibe una publicación errónea de VTP, el switch descarta el mensaje. Si el mensaje descartado contiene la información legítima de la configuración, el switch no sincroniza su base de datos de VLAN como se espera.

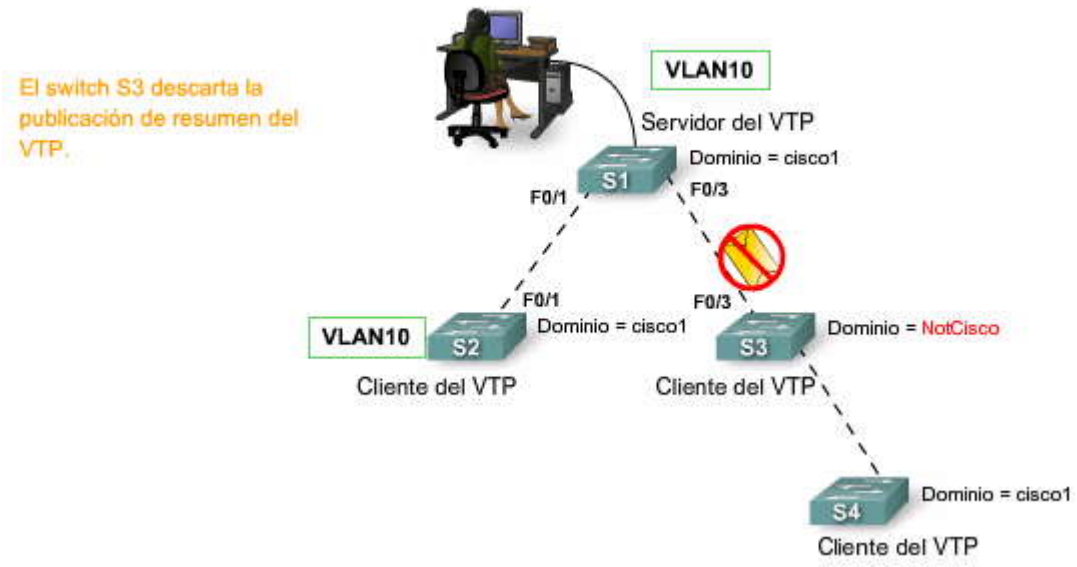
En la figura haga clic en Reproducir para ver una animación sobre este tema.

Haga clic en el botón Solución de dominio del VTP que se muestra en la figura.

Solución

Para evitar la configuración incorrecta de un nombre de dominio del VTP, sólo configure el nombre de dominio del VTP en un switch del servidor del VTP. Todos los otros switches en el mismo dominio del VTP aceptarán y automáticamente configurarán su nombre de dominio del VTP cuando reciba la primera publicación de resumen del VTP.

Nombre incorrecto de dominio del VTP



Nombre incorrecto de dominio del VTP

Cambie el nombre de dominio del VTP a un switch habilitado por el VTP por medio de estos comandos:

Sintaxis del comando del IOS de Cisco	
Ingrese al modo de configuración global	`#configure terminal`
Configura el nombre de dominio del VTP	`(config)#vtp domain` *domain-name*

Este ejemplo muestra cómo cambiar el nombre de dominio del VTP para el switch S3:

```
S3(config)#vtp domain cisco1
```

Solución de dominio del VTP

Switches configurados en modo Cliente del VTP

Es imposible cambiar el modo operativo de todos los switches a cliente del VTP. Al hacer esto, se pierde toda capacidad de crear, eliminar y administrar las VLAN dentro de un entorno de red. Como los switches del cliente de VTP no guardan la información de la VLAN en la NVRAM, necesitan actualizar la información de la VLAN después de una recarga.

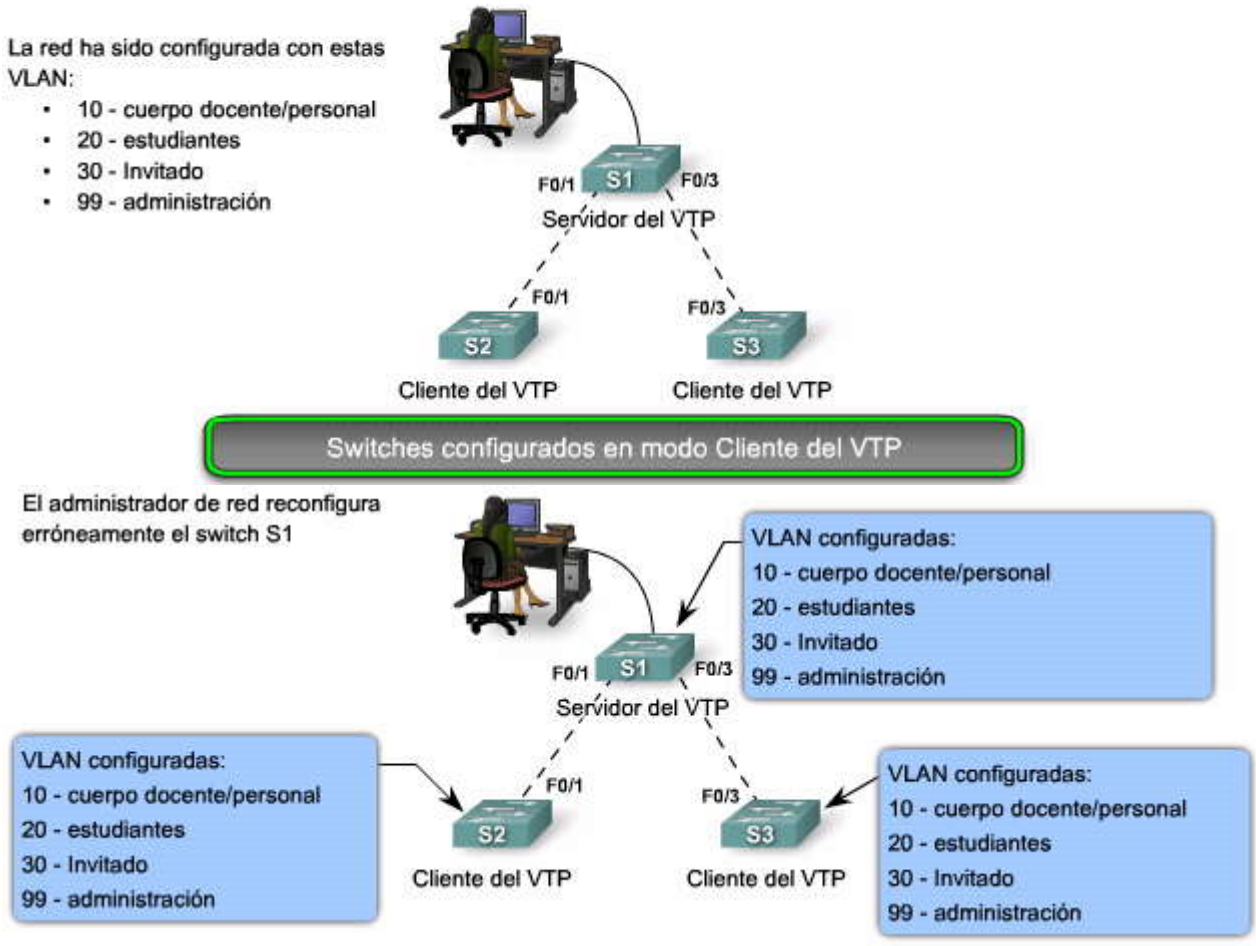
En la figura haga clic en Reproducir para ver una animación sobre este tema.

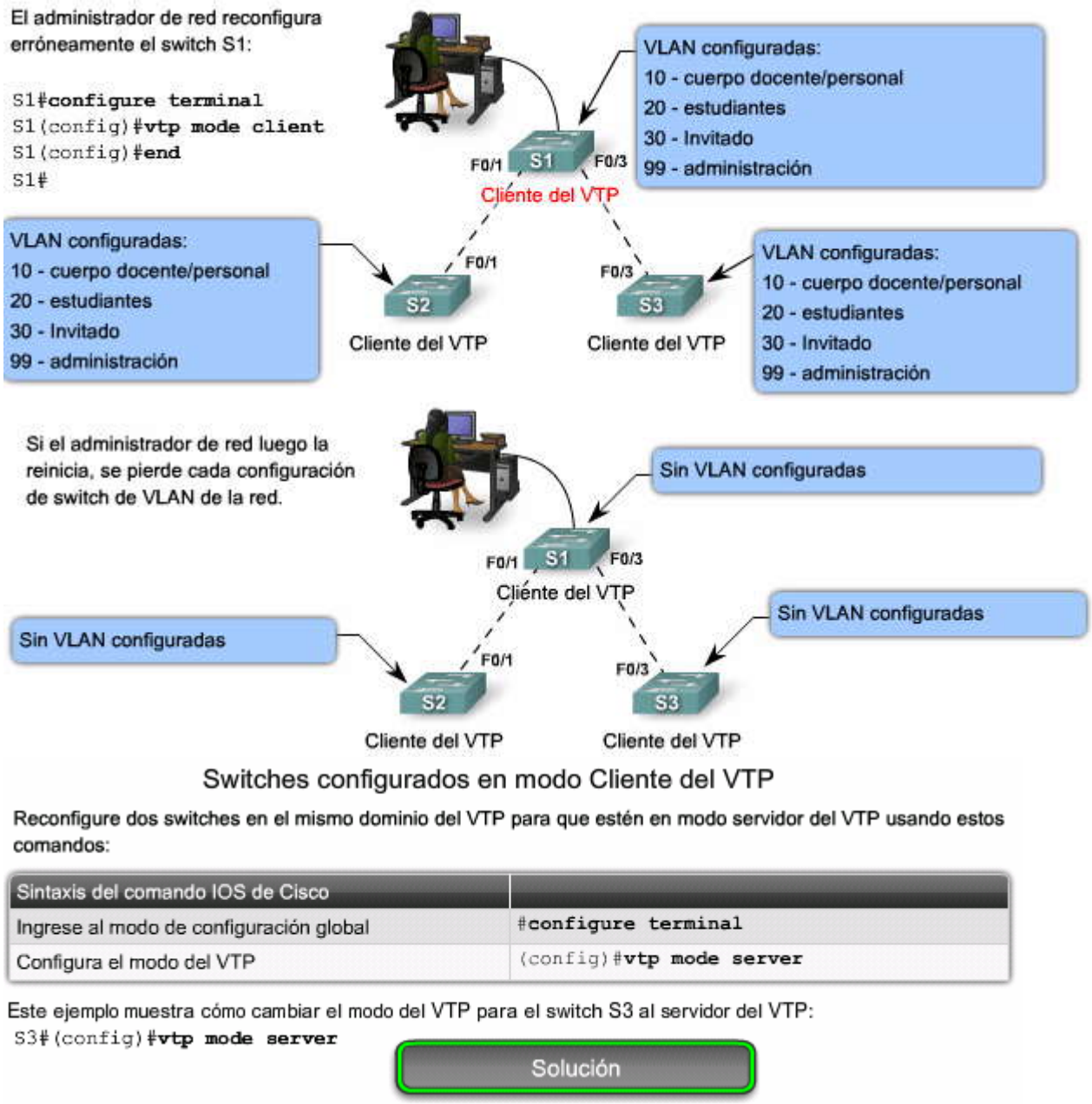
Haga clic en el botón Solución que se muestra en la figura.

Solución

Para evitar perder todas las configuraciones de VLAN en un dominio del VTP accidentalmente al reconfigurar el único servidor del VTP en el dominio como un cliente del VTP, puede configurar un segundo switch en el mismo dominio como servidor del VTP. Es común que redes pequeñas que usan VTP tengan todos los switches en modo servidor del VTP. Si la red está siendo administrada por un par de administradores de red, es poco probable que surjan conflictos de configuraciones de VLAN.

Switches configurados en modo Cliente del VTP





Switches configurados en modo Cliente del VTP

Reconfigure dos switches en el mismo dominio del VTP para que estén en modo servidor del VTP usando estos comandos:

Sintaxis del comando IOS de Cisco	
Ingrese al modo de configuración global	`#configure terminal`
Configura el modo del VTP	`(config)#vtp mode server`

Este ejemplo muestra cómo cambiar el modo del VTP para el switch S3 al servidor del VTP:

```
S3#(config)#vtp mode server
```

Solución

Número de revisión incorrecto

Incluso después de haber configurado los switches en el dominio de su VTP correctamente, existen otros factores que pueden afectar adversamente la funcionalidad del VTP.

Temas de Número incorrecto de revisión

La topología en la figura está configurada con VTP. Existe un switch del servidor del VTP, S1, y dos switches clientes del VTP, S2 y S3,

Haga clic en el botón de Número de revisión incorrecto que se muestra en la figura para reproducir la animación que muestra cómo el agregado de un switch con números mayores de revisión de configuración afecta al resto de los switches en el dominio del VTP.

S4, que ha sido anteriormente configurado como un cliente de VTP, se agrega a la red. El número de revisión del switch S4 es 35, que es mayor que el número de revisión de 17 en la red existente. S4 viene preconfigurado con las dos VLAN, 30 y 40, que no están configuradas en la red existente. La red existente tiene las VLAN 10 y 20.

Cuando se conecta el switch S4 al switch S3, las publicaciones de resumen del VTP anuncian la llegada de un switch habilitado por VTP con el número de revisión más alto en la red. La animación muestra cómo el switch S3, el switch S1 y

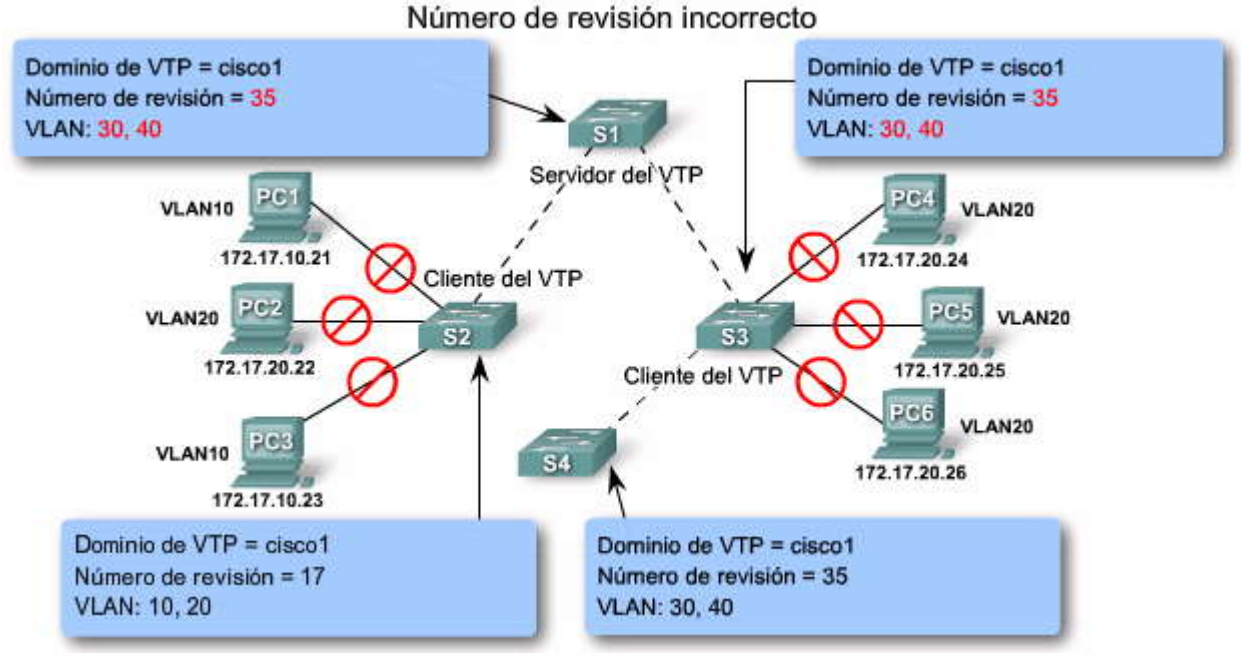
finalmente el switch S2 se reconfiguran a la configuración encontrada en el switch S4. Como cada switch se auto-reconfigura con las VLAN que no son admitidas en la red, los puertos no envían más tráfico desde las computadoras porque están configurados con las VLAN que no existen más en los switches nuevamente reconfigurados.

Haga clic en el botón Reconfigurar el número de revisión que se muestra en la figura.

Solución

La solución al problema es reestablecer a cada switch a su configuración anterior y luego reconfigurar las VLAN correctas, 10 y 20, en switch S1. En primer lugar, para evitar este problema, reestablezca el número de revisión de configuración en los switches previamente configurados que se agregaron a una red habilitada por el VTP. La figura muestra los comandos necesarios para reestablecer el switch S4 al número de revisión predeterminado.

Haga clic en el botón Verificar el número de revisión que se muestra en la figura para ver que al switch S4 se le ha reestablecido su número de revisión.



Número de revisión incorrecto

Antes de agregar un switch a una red habilitada por el VTP reconfigure el número de revisión en un switch mediante estos comandos:

Sintaxis del comando del IOS de Cisco	
Ingrese al modo de configuración global	`#configure terminal`
Configura el nombre de dominio del VTP	`(config)#vtp domain domain-name`

Este ejemplo muestra cómo restablecer el número de revisión en el switch S4:

```
S4(config)#vtp domain test
S4(config)#vtp domain cisco1
```

Reconfigurar el número de revisión

Número de revisión incorrecto

```
S4#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : cisco1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
S4#
```

Verificar el número de revisión

El área superior resaltada muestra el número de revisión reconfigurado a cero.

El área inferior resaltada muestra que las VLAN han sido eliminadas.

4.3.3 ADMINISTRACION DE VLAN EN UN SERVIDOR DEL VTP.-

Administración de VLAN en un servidor del VTP

Ya ha aprendido sobre el VTP y cómo puede utilizarse para simplificar la administración de las VLAN en una red habilitada por el VTP. Considere la topología en la figura. Cuando una VLAN nueva, por ejemplo la VLAN 10, es agregada a la red, el administrador de red agrega la VLAN al servidor de VTP, switch S1 en la figura. Como sabe, el VTP se encarga de propagar los detalles de configuración de la VLAN al resto de la red. No tiene ningún efecto sobre qué puertos están configurados en la VLAN 10 en los switches S1, S2 y S3.

Haga clic en el botón Configurar nuevas VLAN y puertos que se muestra en la figura.

La figura muestra los comandos utilizados para configurar la VLAN 10 y el puerto F0/11 en switch S1. Los comandos para configurar los puertos correctos para los switches S2 y S3 no se muestran.

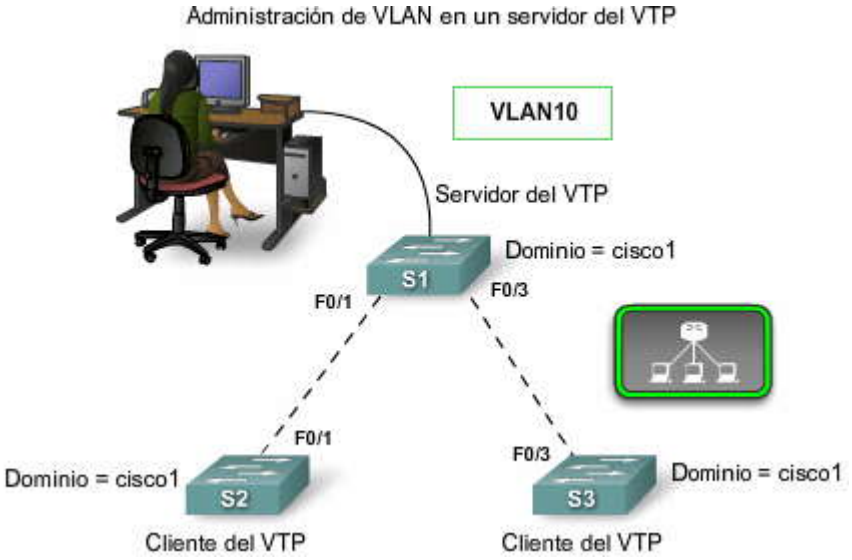
Después de haber configurado la nueva VLAN en el switch S1 y configurado los puertos en los switches S1, S2 yS3 para admitir la nueva VLAN, confirme que el VTP actualizó la base de datos de la VLAN en los switches S2 y S3.

Haga clic en el botón show vtp status que se muestra en la figura.

La salida del comando se usa para verificar la configuración en el switch S2. La verificación para S3 no se muestra.

Haga clic en el botón show interfaces trunk que se muestra en la figura.

La salida confirma que la nueva VLAN se ha agregado a F0/1 en el switch S2. El área resaltada muestra que la VLAN 10 está ahora activa en el dominio de administración del VTP.



```
S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name faculty
S1(config-vlan)#exit
S1(config)#interface FastEthernet 0/11
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#exit
S1#
```

Configurar nuevas VLAN y puertos

```
S2#show vtp status
VTP Version: 1
Configuration Revision: 4
Maximum VLANs supported locally: 64
Number of existing VLANs: 8
VTP Operating Mode: Client
VTP Domain Name: cisco1
VTP Pruning Mode: Disabled
VTP V2 Mode: Disabled
VTP Traps Generation: Disabled
MD5 digest: 0x59 0x67 0x4C 0xFD 0x8B 0xD9 0xA7 0x9A
Configuration last modified by 0.0.0.0 at 3-1-93 00:41:42
S2#
```

show vtp status

```
S2#show interfaces trunk
Port    Mode     Encapsulation     Status    Native vlan
Fa0/1   on       802.1q  trunking 1

Port    Vlans allowed on trunk
Fa0/1   1-1005

Port    Vlans allowed and active in management domain
Fa0/1   1,10,20,30,1002,1003,1004,1005

Port    Vlans in spanning tree forwarding state and not pruned
Fa0/1   1,10,20,30,1002,1003,1004,1005
S2#
```

show interfaces trunk

CAPITULO V – "STP"

5.0 INTRODUCCIÓN DEL CAPITULO.-

5.0.1 INTRODUCCIÓN.-

Es claro que las redes informáticas representan un componente fundamental para la mayoría de las pequeñas y medianas empresas. En consecuencia, los administradores de TI deben implementar la redundancia en sus redes jerárquicas. Sin embargo, cuando se agregan enlaces adicionales a switches y routers de la red, se generan bucles en el tráfico que deben ser administrados de manera dinámica. Cuando se pierde la conexión con un switch, otro enlace debe reemplazarlo rápidamente sin introducir nuevos bucles en el tráfico. En este capítulo aprenderá la forma en que el protocolo spanning-tree (STP) evita los inconvenientes relacionados con bucles en la red y la manera en que STP ha evolucionado en un protocolo que determina de forma rápida aquellos puertos que deben bloquearse, de forma que una red basada en red de área local virtual (VLAN, Virtual Local Area Network) no experimente bucles en el tráfico.

En este capítulo aprenderá a:

- Explicar la función de la redundancia en una red convergente.
- Resumir la forma en que funciona STP a la hora de eliminar los bucles de Capa 2 de una red convergente.
- Explicar la forma en que el algoritmo de STP utiliza tres pasos para converger en una topología sin bucles.
- Implementar PVST+ rápido en una LAN para evitar los bucles entre switches redundantes.

5.1 TOPOLOGÍAS REDUNDANTES DE CAPA 2.-

5.1.1 REDUNDANCIA.-

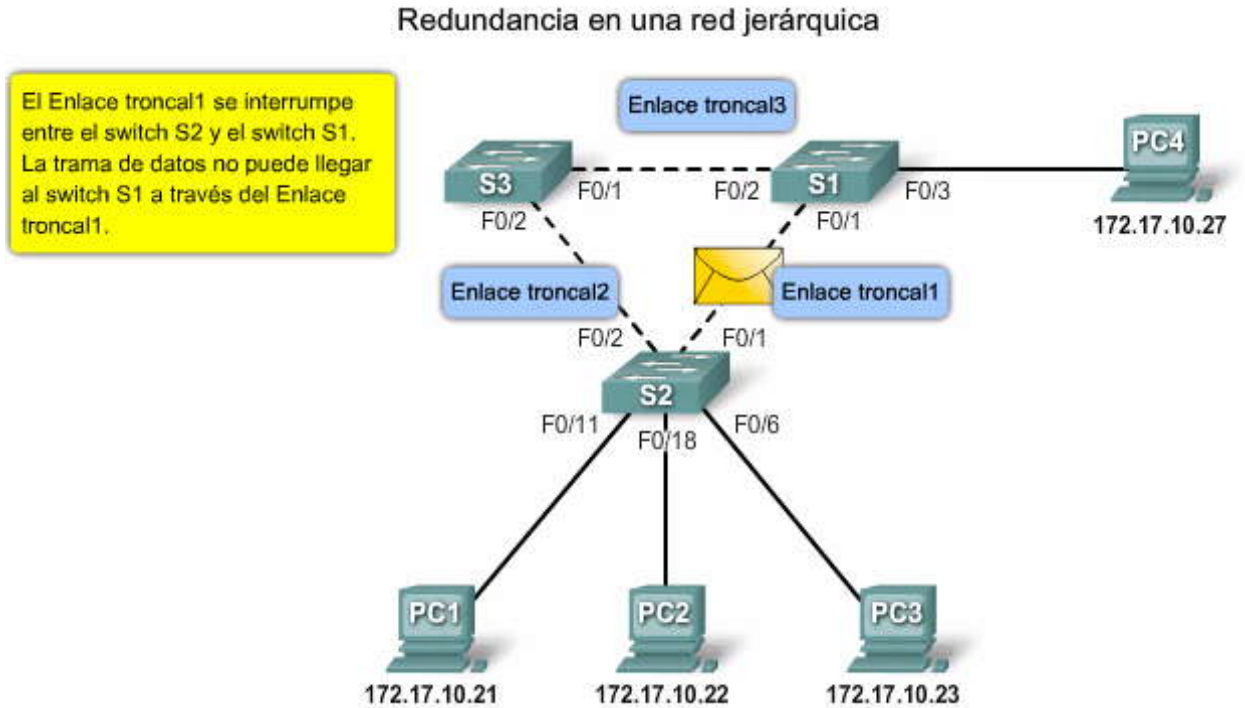
Redundancia en una red jerárquica

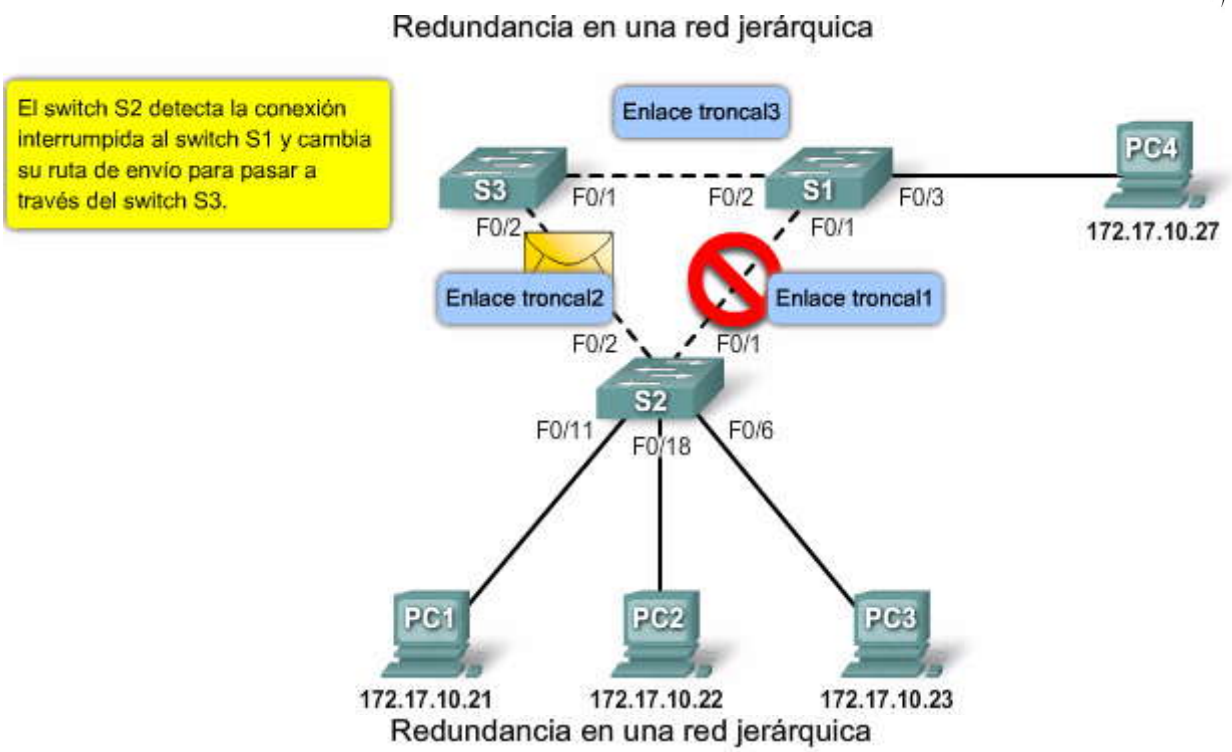
El modelo de diseño jerárquico fue presentado en el capítulo 1. El modelo de diseño jerárquico se enfoca en los temas encontrados en las topologías de red de modelo plano. Uno de esos temas es la redundancia. La redundancia de Capa 2 mejora la disponibilidad de la red implementando rutas de red alternas mediante el agregado de equipos y cables. Al contar con varias rutas para la transmisión de los datos en la red, la interrupción de una ruta simple no genera impacto en la conectividad de los dispositivos en la red.

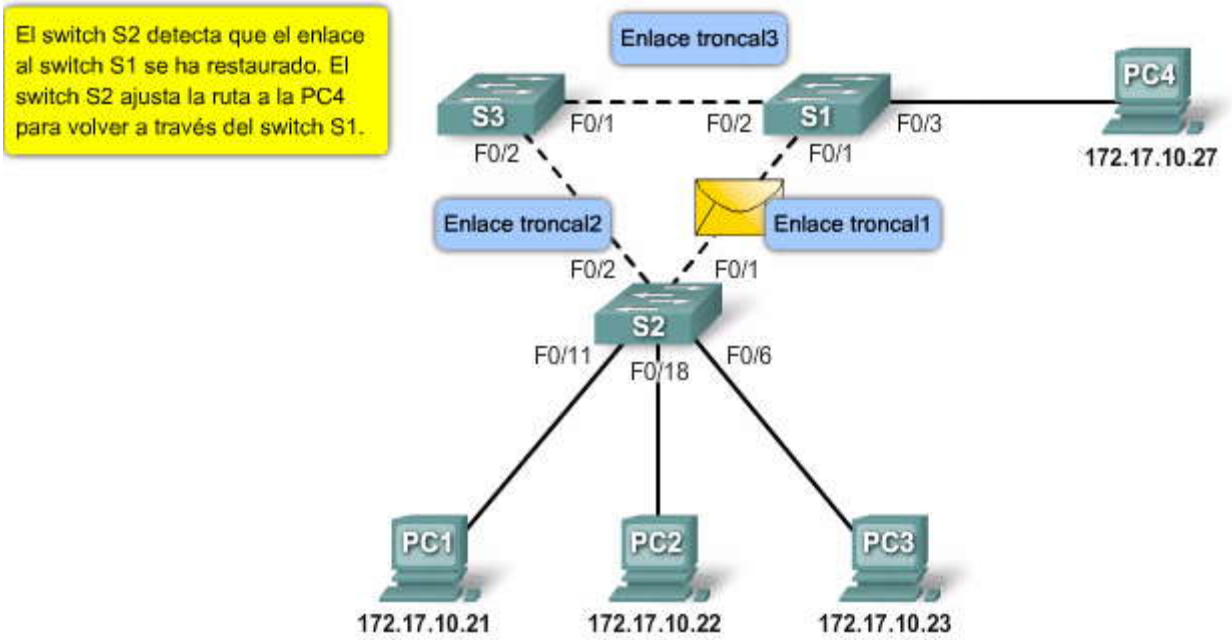
Como puede verse en la animación:

1. La PC1 se comunica con la PC4 a través de una topología de red configurada de forma redundante.
2. Cuando el enlace de red entre el switch S1 y el switch S2 se interrumpe, la ruta entre la PC1 y la PC4 se ajusta de manera automática para compensar la interrupción.
3. Cuando la conexión de red entre S1 y S2 se restablece, la ruta vuelve a ajustarse para enviar el tráfico directamente desde S2 a través de S1 para llegar a la PC4.

A medida que los negocios se vuelven cada vez más dependientes de la red, la disponibilidad de la infraestructura de red se transforma en una inquietud comercial fundamental que debe ser tenida en cuenta. La redundancia es la solución para lograr la disponibilidad necesaria.







Examinar un diseño redundante

En un diseño jerárquico, la redundancia se logra en las capas de distribución y núcleo a través de hardware adicional y rutas alternativas entre dicho hardware.

Haga clic en el botón Punto de partida: acceso a la capa de distribución de la figura.

En este ejemplo puede verse una red jerárquica con capas de acceso, distribución y núcleo. Cada switch de la capa de acceso se conecta a dos switches distintos de la capa de distribución. Además, cada switch de la capa de distribución se conecta a los dos switches de la capa núcleo. Al contar con varias rutas entre la PC1 y la PC4, existe redundancia que puede generar un único punto de falla entre las capas de acceso y de distribución y entre las capas de distribución y núcleo.

STP está habilitado en todos los switches. STP es el tema de este capítulo y será explicado de forma extensa. Por ahora, observe que STP ha colocado algunos puertos de switch en estado de enviar y otros en estado de bloqueo. Esto es para evitar bucles en la red de la Capa 2. STP sólo utilizará un enlace redundante si existe una falla en el enlace principal.

En el ejemplo, la PC1 puede comunicarse con la PC4 a través de la ruta identificada.

Haga clic en el botón Falla en la ruta: acceso a la capa de distribución de la figura.

El enlace entre el switch S1 y el switch D1 se ha interrumpido, lo que impide que los datos de la PC1 que tienen destino en la PC4 lleguen al switch D1 a través de su ruta original. Sin embargo, ya que el switch S1 cuenta con una segunda ruta a la PC4 a través del switch D2, la ruta se actualiza y los datos pueden llegar a la PC4.

Haga clic en el botón Falla en la ruta: distribución a la capa núcleo de la figura.

El enlace entre el switch D1 y el switch C2 se ha interrumpido, lo que impide que los datos de la PC1 que tienen destino en la PC4 lleguen al switch C2 a través de su ruta original. Sin embargo, ya que el switch D1 cuenta con una segunda ruta a la PC4 a través del switch C1, la ruta se actualiza y los datos pueden llegar a la PC4.

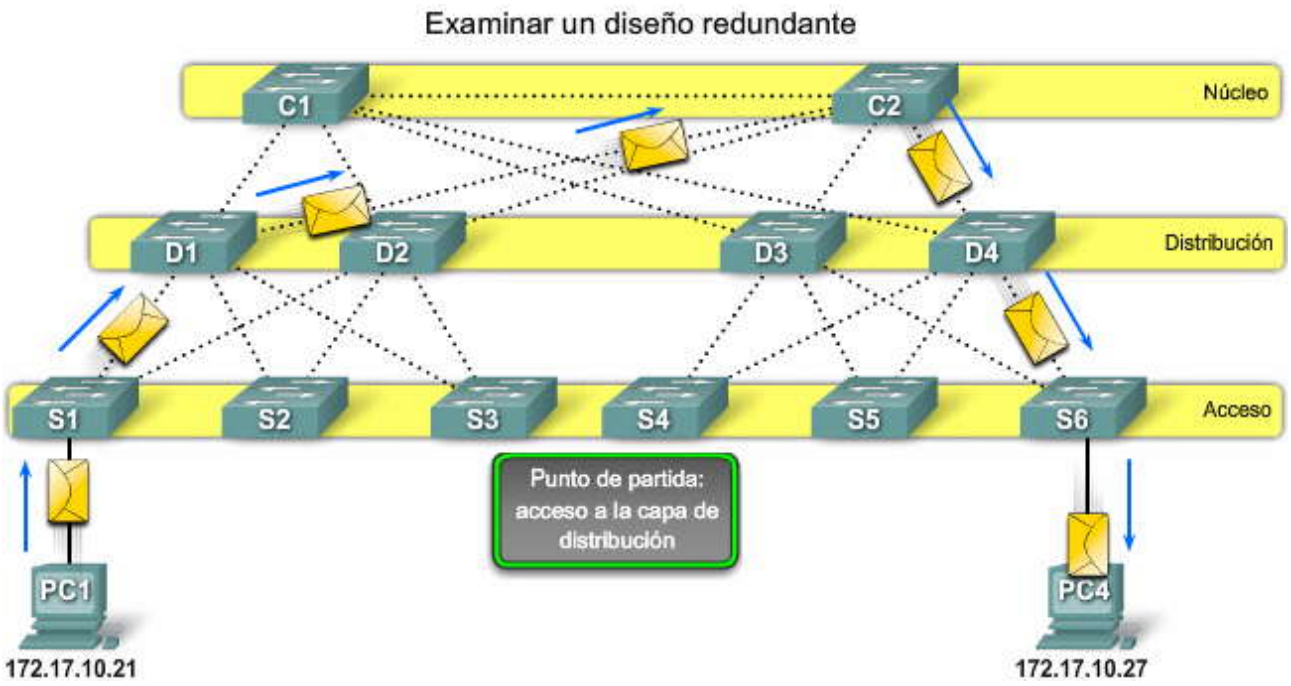
Haga clic en el botón Falla en el switch: capa de distribución de la figura.

El switch D1 ha fallado, lo que impide que los datos de la PC1 con destino a la PC4 lleguen al switch C2 a través de su ruta original. Sin embargo, ya que el switch S1 cuenta con una segunda ruta a la PC4 a través del switch D2, la ruta se actualiza y los datos pueden llegar a la PC4.

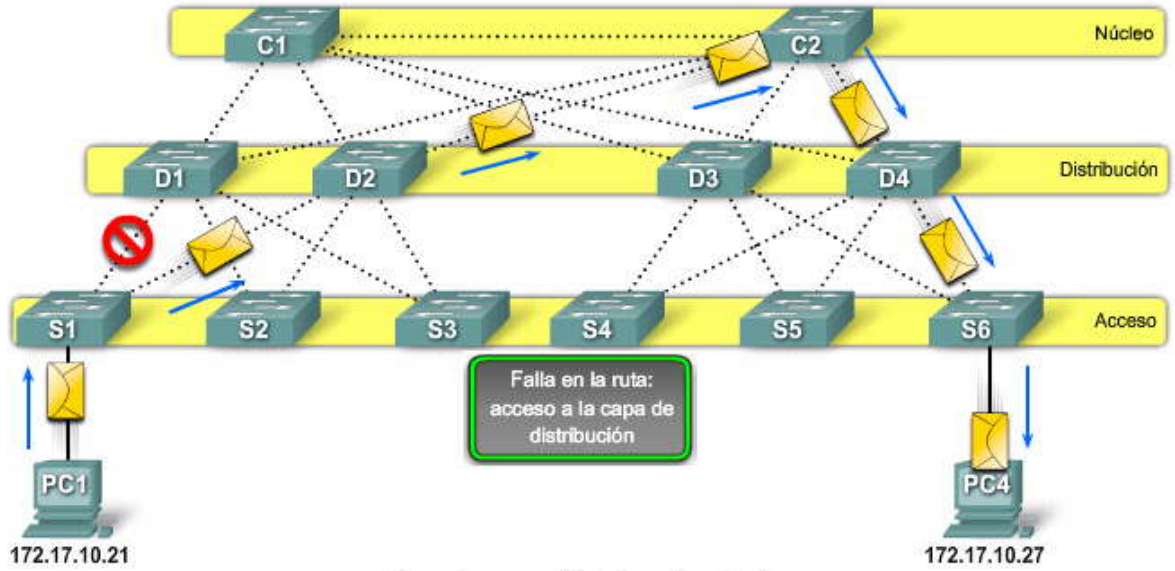
Haga clic en el botón Falla en el switch: capa núcleo de la figura.

El switch C2 ha fallado, lo que impide que los datos de la PC1 con destino a la PC4 lleguen al switch D4 a través de su ruta original. Sin embargo, ya que el switch D1 cuenta con una segunda ruta a la PC4 a través del switch C1, la ruta se actualiza y los datos pueden llegar a la PC4.

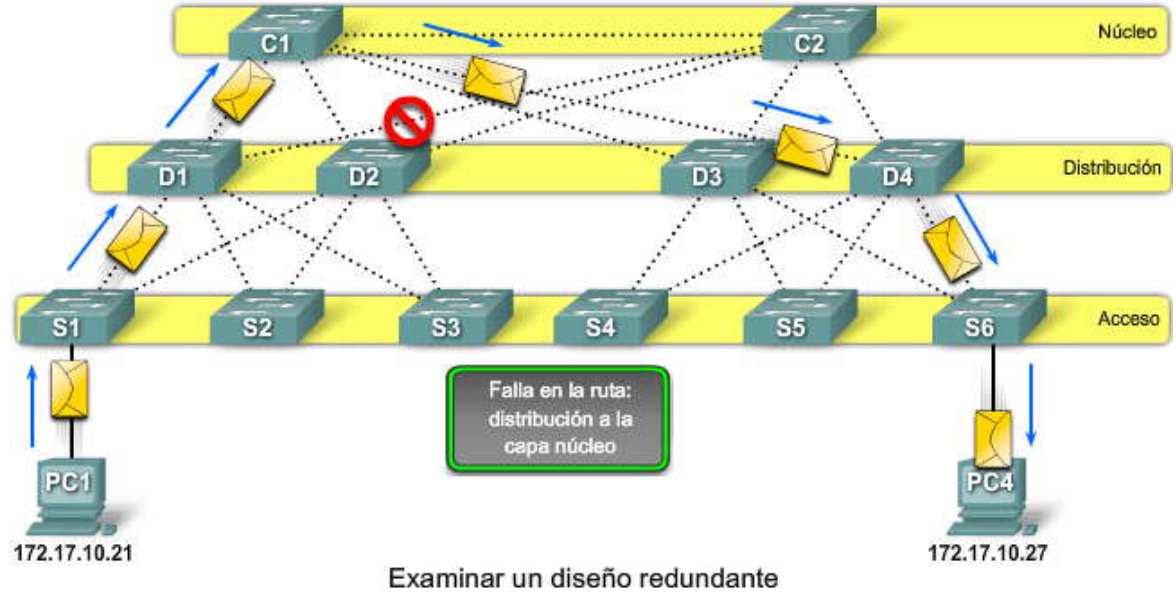
La redundancia proporciona una gran flexibilidad en la elección de rutas de la red y permite que los datos se transmitan independientemente de la existencia de fallas en una ruta simple o en un dispositivo en las capas de distribución o núcleo. La redundancia cuenta con algunas complicaciones que deben ser tenidas en cuenta antes de que se implemente de forma segura en una red jerárquica.



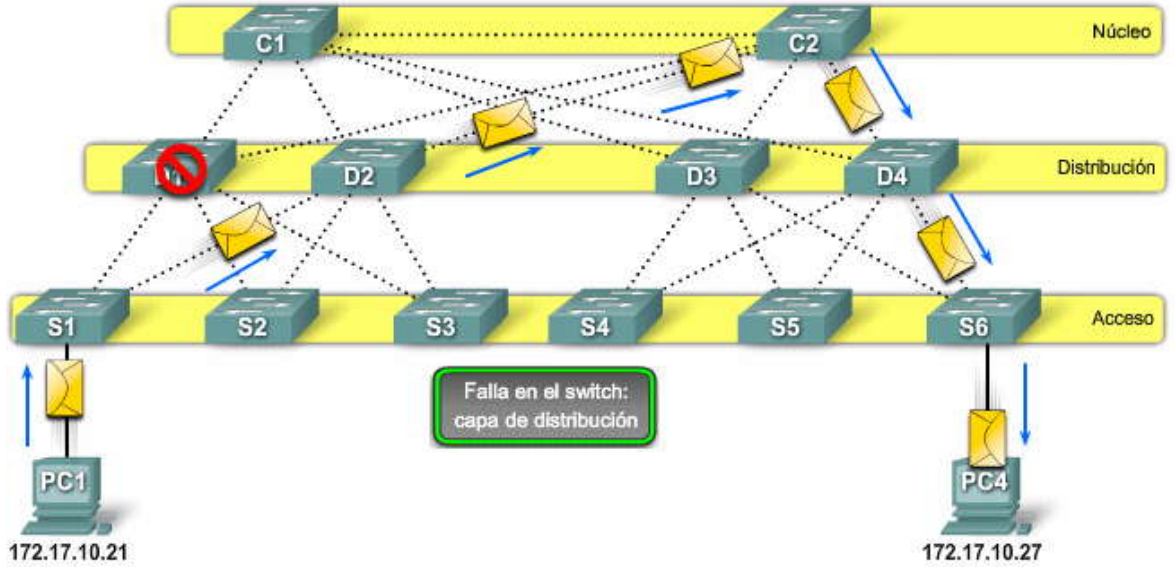
Examinar un diseño redundante

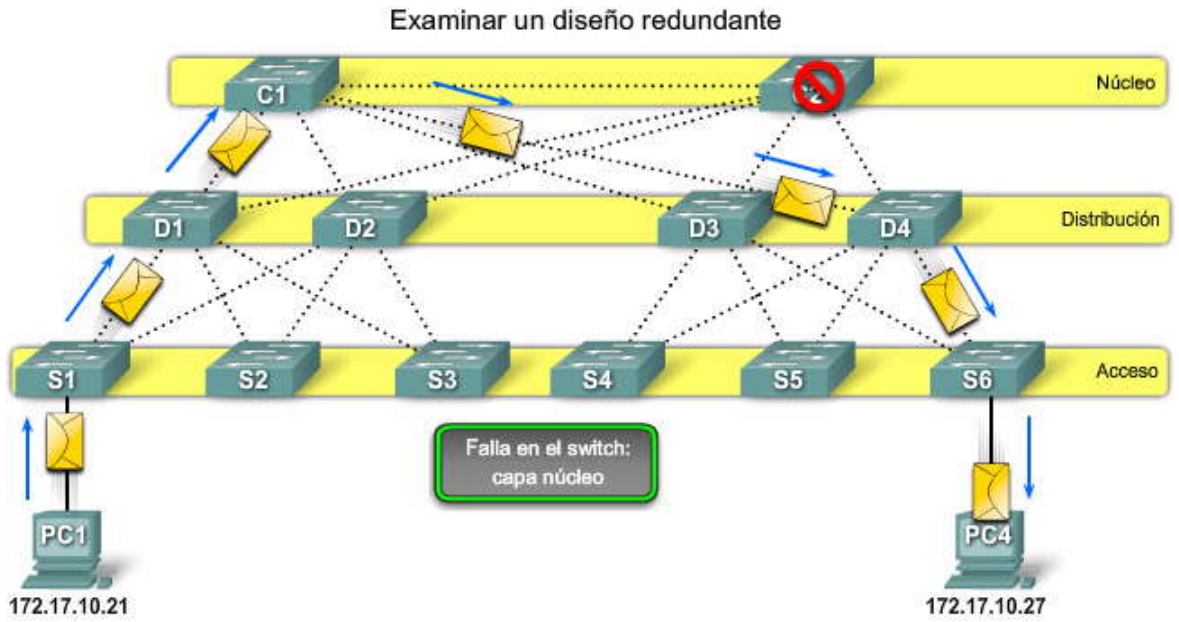


Examinar un diseño redundante



Examinar un diseño redundante





5.1.2 INCOVENIENTES DE LA REDUNDANCIA.-

Bucles de Capa 2

La redundancia es una parte importante del diseño jerárquico. Pese a que es importante para la disponibilidad, existen algunas consideraciones que deben atenderse antes de que la redundancia sea posible en una red.

Cuando existen varias rutas entre dos dispositivos en la red y STP se ha deshabilitado en los switches, puedegenerarse un bucle de Capa 2. Si STP está habilitado en estos switches, que es lo que que está predeterminado, el bucle de Capa 2 puede evitarse.

Las tramas de Ethernet no poseen un tiempo de existencia (TTL, Time to Live) como los paquetes IP que viajan por los routers. En consecuencia, si no finalizan de manera adecuada en una red conmutada, las mismas siguen rebotando de switch en switch indefinidamente o hasta que se interrumpa un enlace y elimine el bucle.

Las tramas de broadcast se envían a todos los puertos de switch, excepto el puerto de origen. Esto asegura que todos los dispositivos del dominio de broadcast puedan recibir la trama. Si existe más de una ruta para enviar la trama, se puede generar un bucle sin fin.

Haga clic en el botón Reproducir de la figura para iniciar la animación.

En la animación:

1. La PC1 envía una trama de broadcast al switch S2.

2. Cuando S2 recibe la trama de broadcast actualiza su tabla de direcciones MAC para registrar que la PC1 está disponible en el puerto F0/11.

3. Ya que es una trama de broadcast, S2 envía la trama a todos los puertos de switch, incluido el Enlace troncal1 y el Enlace troncal2.

4. Cuando la trama de broadcast llega a los switches S3 y S1, los mismos actualizan sus tablas de direcciones MACpara indicar que la PC1 está disponible en el puerto F0/1 para S1 y en el puerto F0/2 para S3.

5. Ya que es una trama de broadcast, S3 y S1 la envían a todos los puertos de switch, excepto el que envió la trama.

6. S3 envía entonces la trama a S1 y viceversa. Cada switch actualiza su tabla de direcciones MAC con el puerto incorrecto para la PC1.

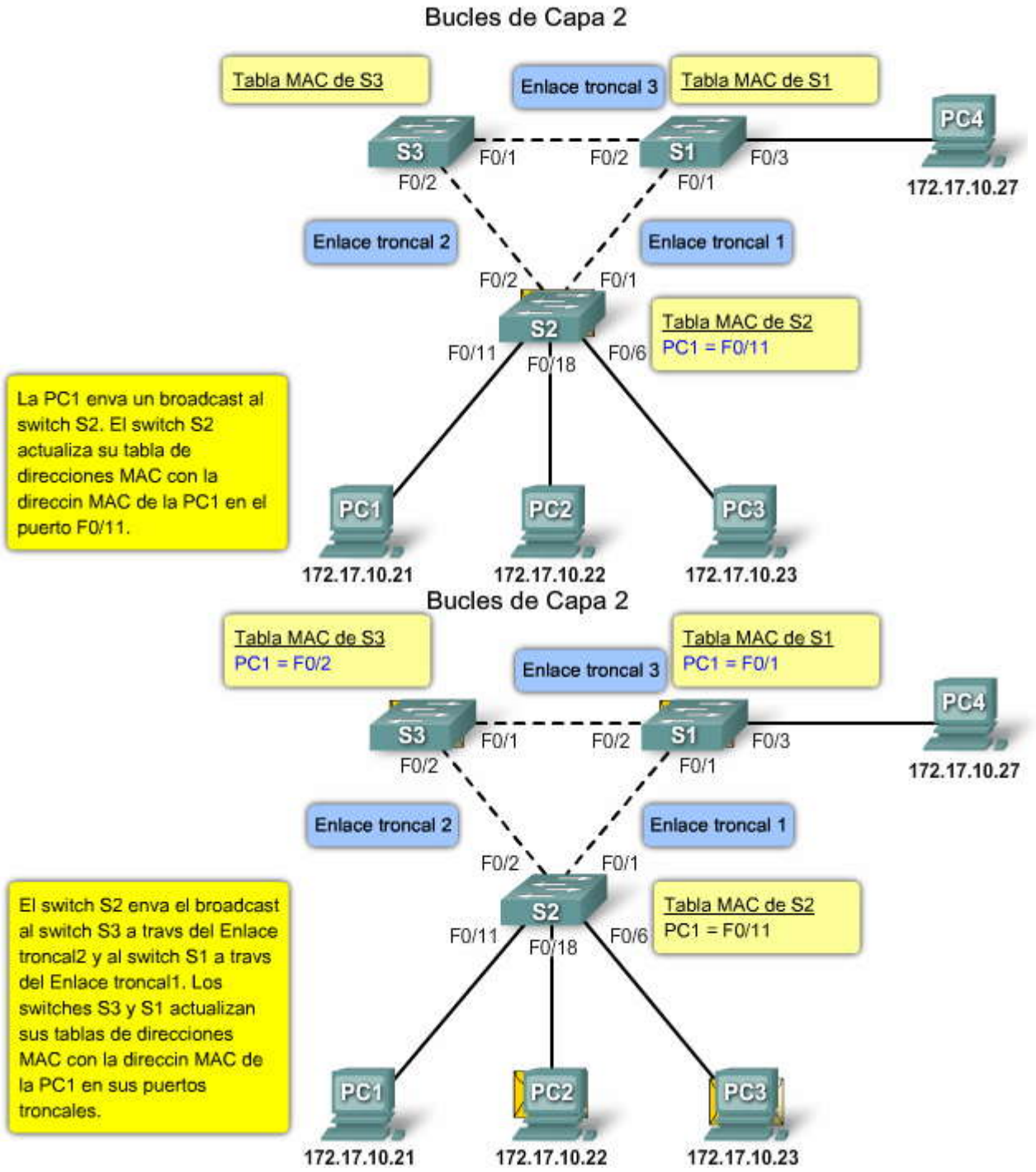
7. De nuevo, cada switch envía la trama de broadcast a todos sus puertos, excepto aquel que la envió, lo que produce que ambos switches envíen la trama a S2.

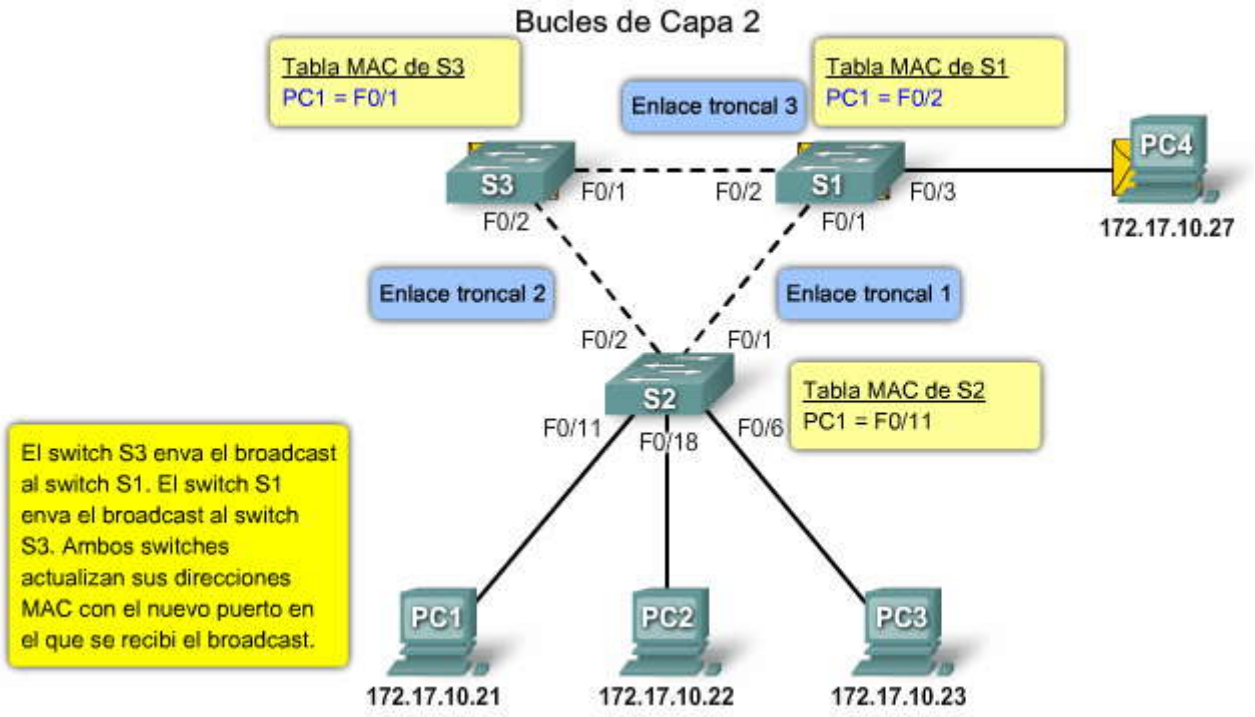
8. Cuando S2 recibe las tramas de broadcast de S3 y S1, la tabla de direcciones MAC vuelve a actualizarse, esta vez con la última entrada recibida de los otros dos switches.

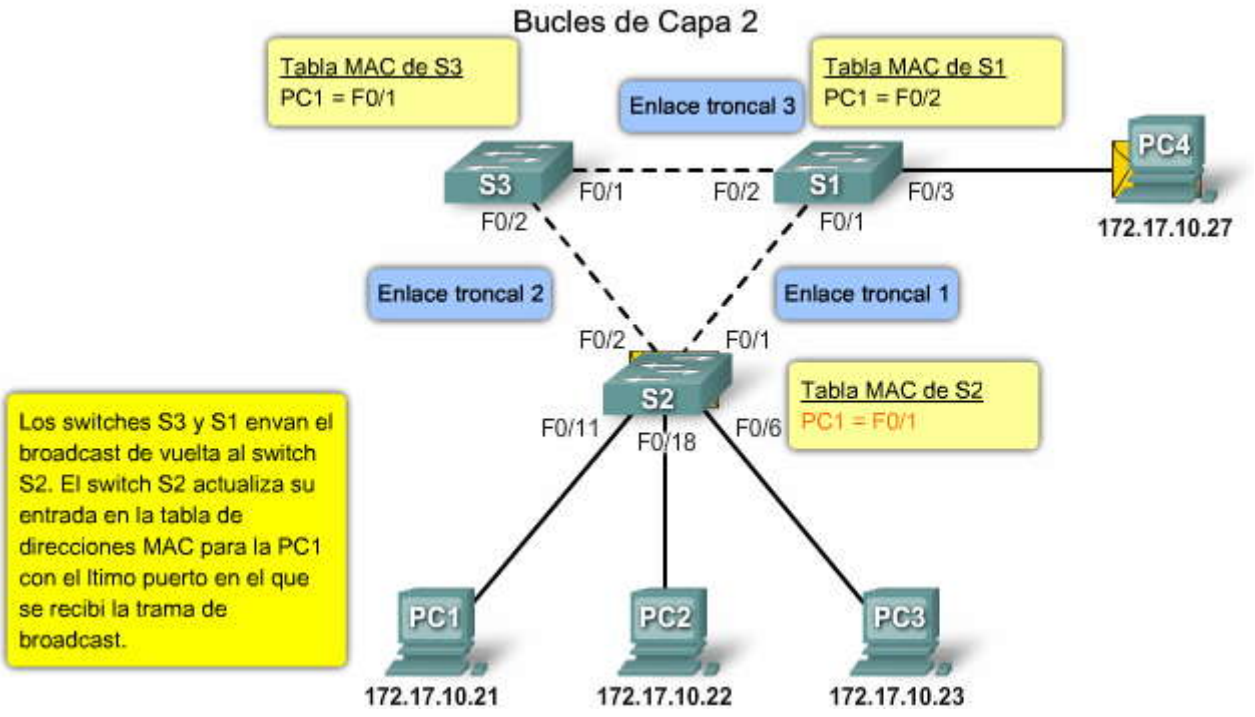
Este proceso se repite indefinidamente hasta que se elimine el bucle mediante la interrupción física de las conexiones que lo producen o de la desconexión de uno de los switches del bucle.

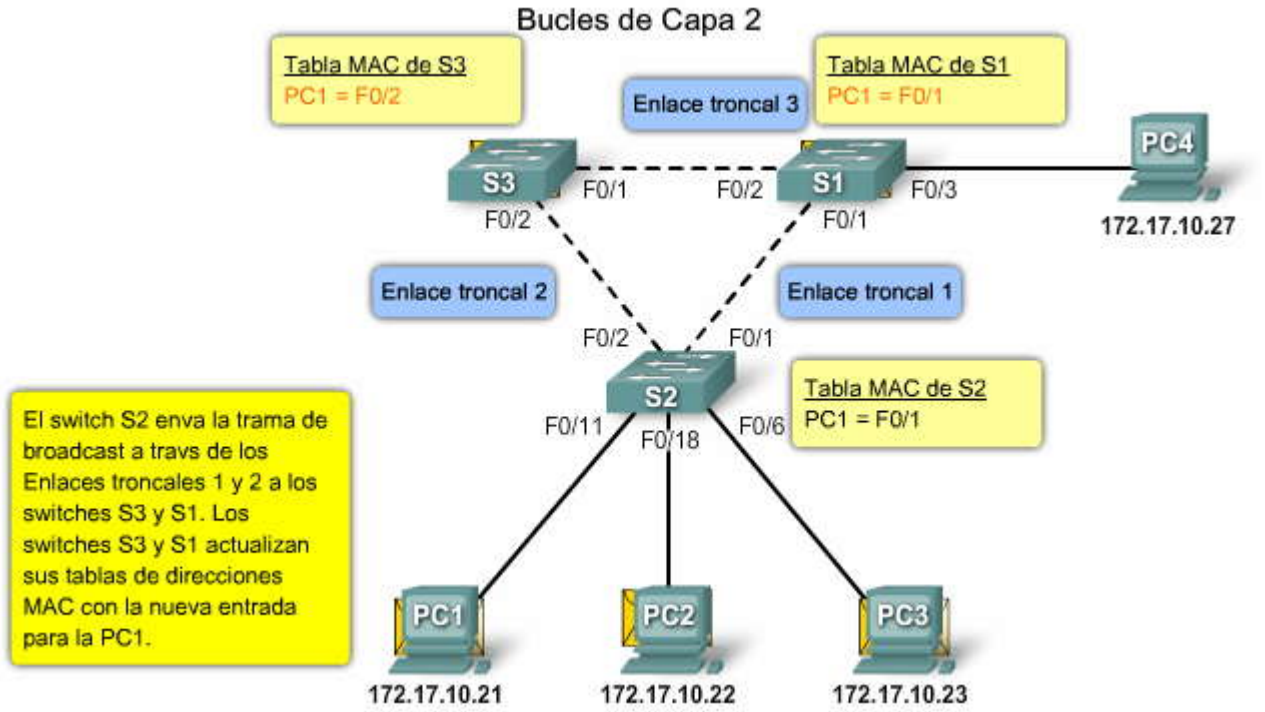
Los bucles producen una alta carga de CPU en todos los switches atrapados en el mismo. Ya que se envían las mismas tramas constantemente entre todos los switches del bucle, la CPU del switch debe procesar una gran cantidad de datos. Esto disminuye el rendimiento del switch cuando llega tráfico legítimo.

Un host atrapado en un bucle de red es inaccesible para otros hosts de la red. Ya que la tablade direcciones MAC cambia de forma constante con las actualizaciones de las tramas de broadcast, el switch no sabe a qué puerto debe enviar las tramas de unicast para que las mismas lleguen a su destino final. Las tramas de unicast también quedan atrapadas en el bucle de red. A medida que aumenta la cantidad de tramas que quedan atrapadas en el bucle de red, se produce una tormenta de broadcast.




Bucles de Capa 2
Tabla MAC de S3
PC1 = F0/1
Enlace troncal 3
Tabla MAC de S1
PC1 = F0/2
S3
F0/1
F0/2
S1
F0/3
PC4
172.17.10.27
F0/2
F0/1
Enlace troncal 2
Enlace troncal 1
F0/2
F0/1
S2
Tabla MAC de S2
PC1 = F0/11
F0/11
F0/18
F0/6
El switch S3 enva el broadcast al switch S1. El switch S1 enva el broadcast al switch S3. Ambos switches actualizan sus direcciones MAC con el nuevo puerto en el que se recibi el broadcast.
PC1
PC2
PC3
172.17.10.21
172.17.10.22
172.17.10.23


Bucles de Capa 2
Tabla MAC de S3
PC1 = F0/1
Enlace troncal 3
Tabla MAC de S1
PC1 = F0/2
S3
F0/1
F0/2
S1
F0/3
PC4
172.17.10.27
F0/2
F0/1
Enlace troncal 2
Enlace troncal 1
F0/2
F0/1
S2
Tabla MAC de S2
PC1 = F0/1
F0/11
F0/18
F0/6
Los switches S3 y S1 envan el broadcast de vuelta al switch S2. El switch S2 actualiza su entrada en la tabla de direcciones MAC para la PC1 con el ltimo puerto en el que se recibi la trama de broadcast.
PC1
PC2
PC3
172.17.10.21
172.17.10.22
172.17.10.23



Tormentas de broadcast

Una tormenta de broadcast se produce cuando existen tantas tramas de broadcast atrapadas en un bucle de Capa 2 que se consume todo el ancho de banda disponible. En consecuencia, no existe ancho de banda disponible para el tráfico legítimo y la red queda no disponible para la comunicación de datos.

La tormenta de broadcast es inevitable en una red con bucles. A medida que más dispositivos envían broadcast a la red, aumenta la cantidad de tráfico que queda atrapado en el bucle, lo que eventualmente genera una tormenta de broadcast que produce la falla de la red.

Existen otras consecuencias de las tormentas de broadcast. Debido a que el tráfico de broadcast se envía a todos los puertos del switch, todos los dispositivos conectados deben procesar todo el tráfico de broadcast que fluye indefinidamente en la red con bucles. Esto puede producir que el dispositivo final no funcione debido a los requerimientos de alto procesamiento para sostener una carga de tráfico de esas dimensiones en la tarjeta de interfaz de red.

Haga clic en el botón Reproducir de la figura para iniciar la animación.

En la animación:

1. La PC1 envía una trama de broadcast a la red con bucles.

2. La trama de broadcast termina en un bucle generado entre todos los switches interconectados de la red.

3. La PC4 también envía una trama de broadcast a la red con bucles.

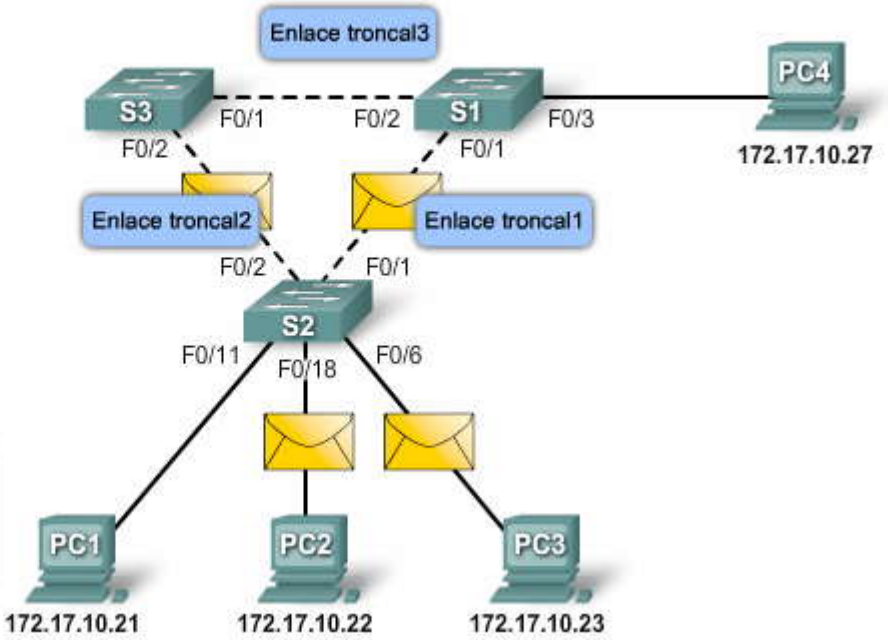
4. La trama de broadcast de la PC4 también queda atrapada en el bucle generado entre todos los switches interconectados, de la misma forma que la trama de broadcast de la PC1.

5. A medida que aumenta la cantidad de tramas de broadcast que otros dispositivos envían a la red, también aumenta el tráfico que queda atrapado en el bucle, lo que eventualmente produce una tormenta de broadcast.

6. Cuando la red está completamente saturada con tráfico de broadcast atrapado en bucles entre los switches, estosúltimos descartan el tráfico nuevo porque no pueden procesarlo.

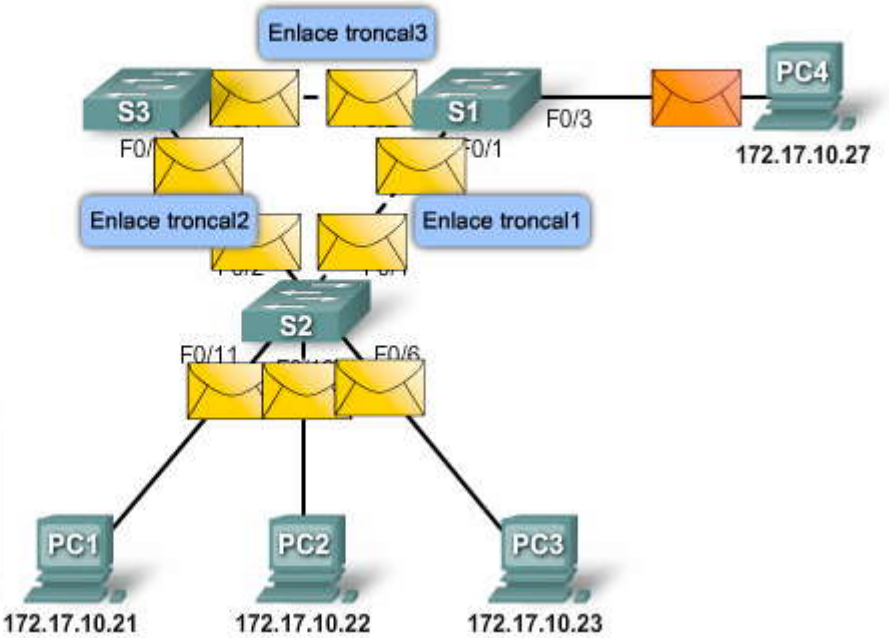
Debido a que los dispositivos conectados a la red envían tramas de broadcast de manera constante, como solicitudes de ARP, una tormenta de broadcast puede desarrollarse en cuestión de segundos. En consecuencia, cuando se genera un bucle, la red se torna no disponible rápidamente.

Tormentas de broadcast

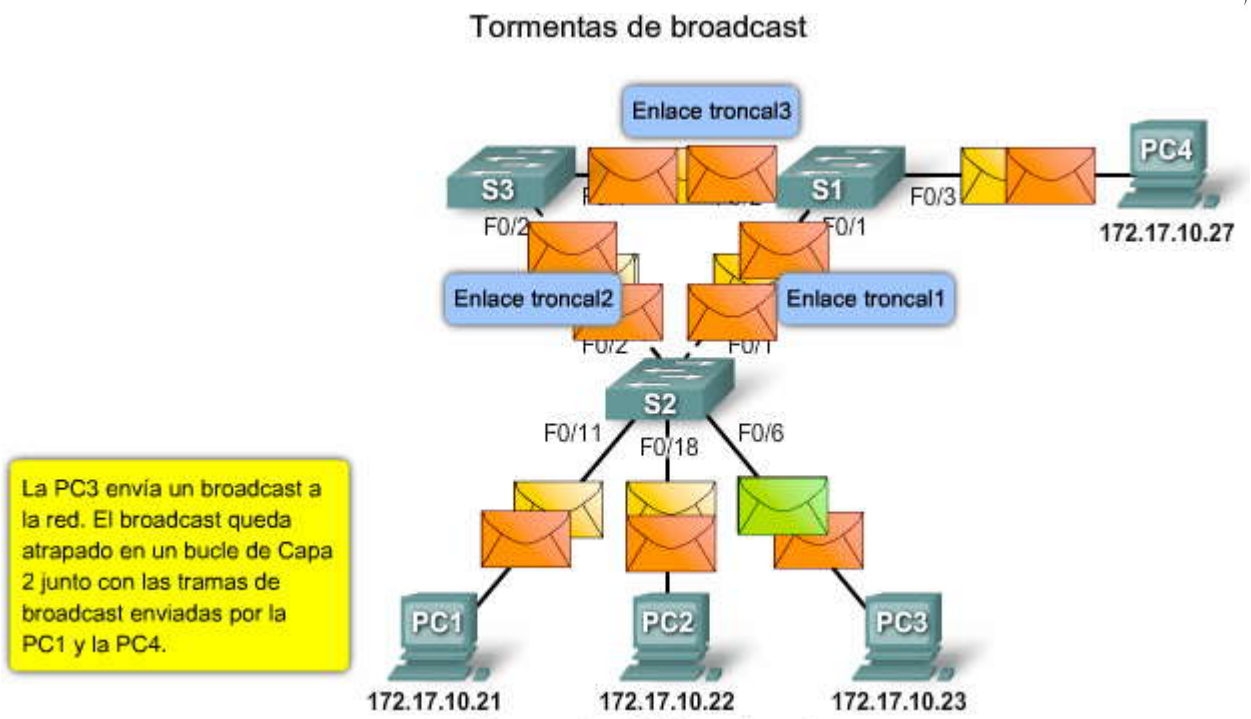


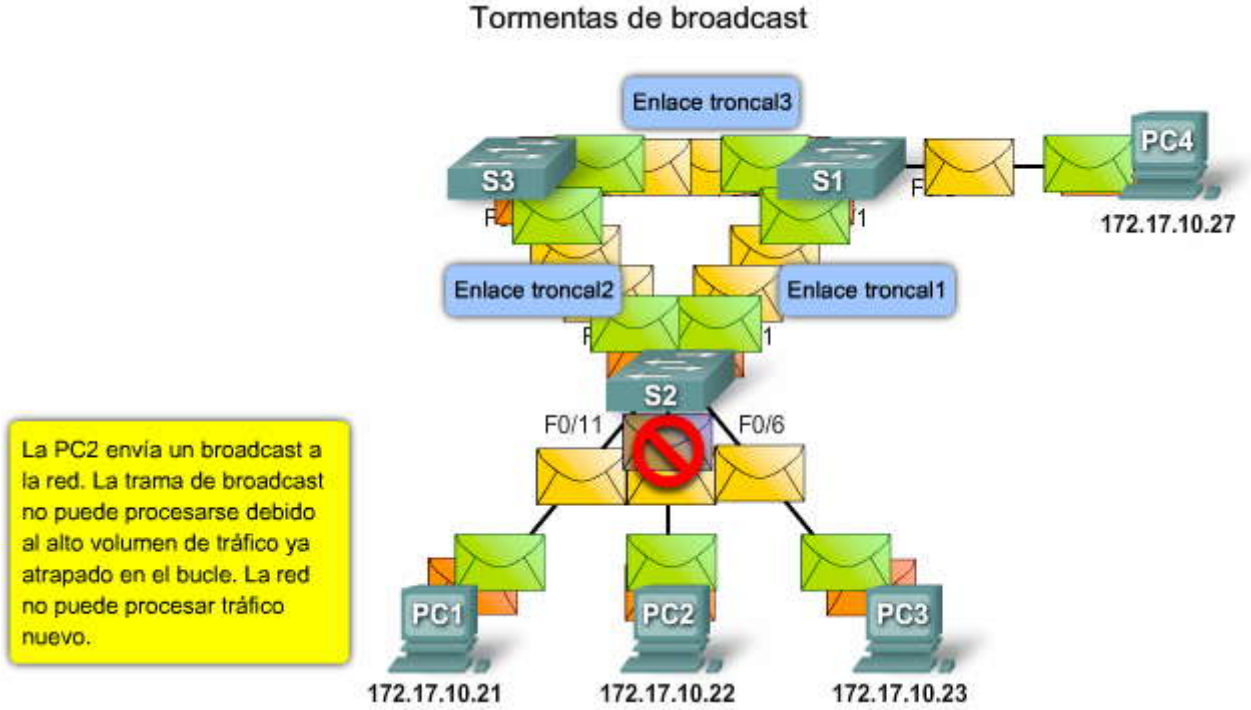
La PC1 envía un broadcast a la red. El broadcast queda atrapado en un bucle de Capa 2.

Tormentas de broadcast



La PC4 envía un broadcast a la red. El broadcast queda atrapado en un bucle de Capa 2 junto con la trama de broadcast enviada por la PC1.





Tramas de unicast duplicadas

Las tramas de broadcast no son el único tipo de tramas que son afectadas por los bucles. Las tramas de unicast enviadas a una red con bucles pueden generar tramas duplicadas que llegan al dispositivo de destino.

Haga clic en el botón Reproducir de la figura para iniciar la animación.

En la animación:

1. La PC1 envía una trama de unicast con destino a la PC4.

2. El switch S2 no cuenta con una entrada para la PC4 en su tabla MAC, de manera que envía la trama de unicast a todos los puertos de switch, en un intento de encontrar a la PC4.

3. La trama llega a los switches S1 y S3.

4. S1 no posee una entrada de dirección MAC para la PC4, de forma que reenvía la trama a la PC4.

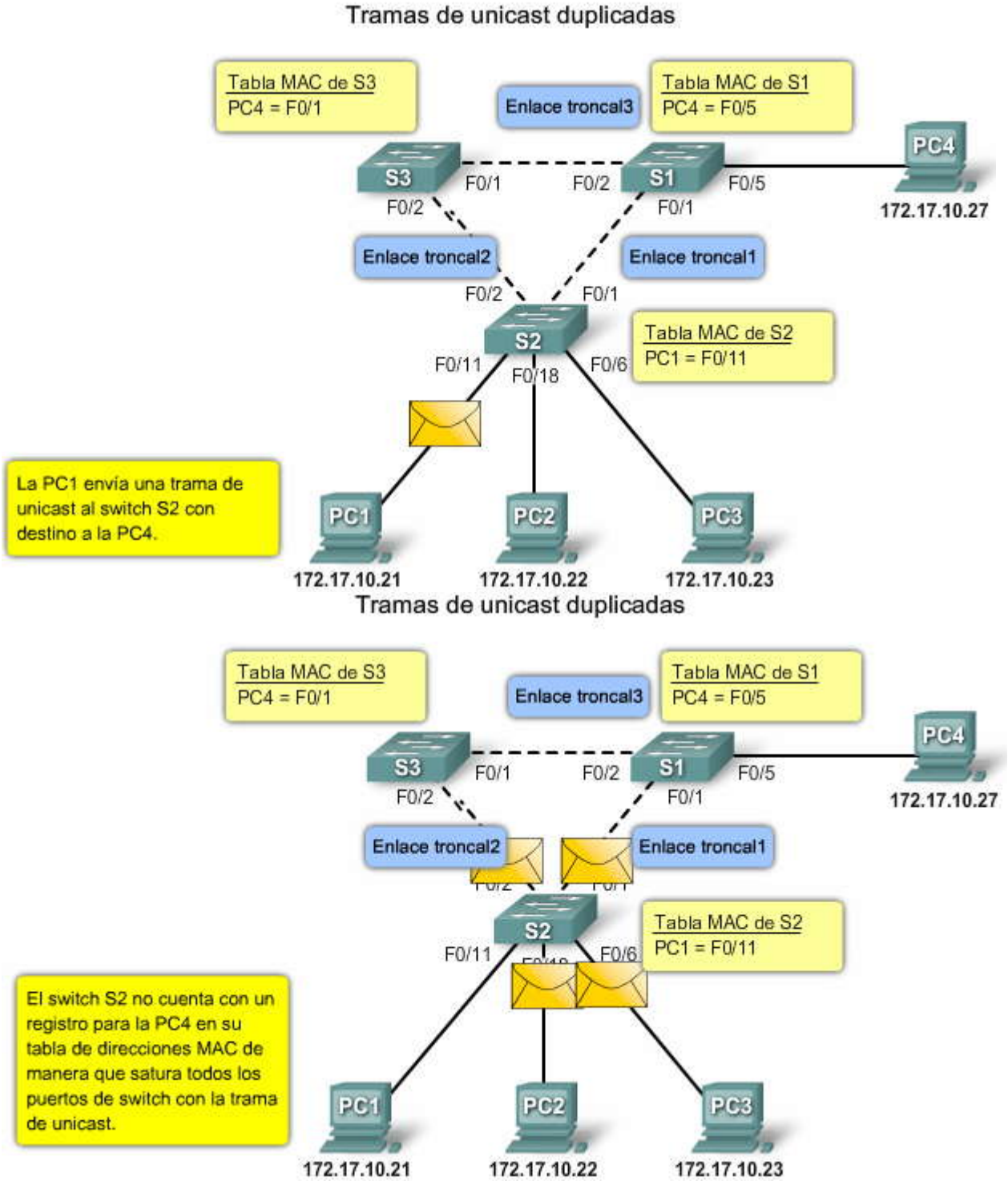
5. S3 también cuenta con una entrada en su tabla de direcciones MAC para la PC4, de manera que reenvía la trama de unicast a través del Enlace troncal3 a S1.

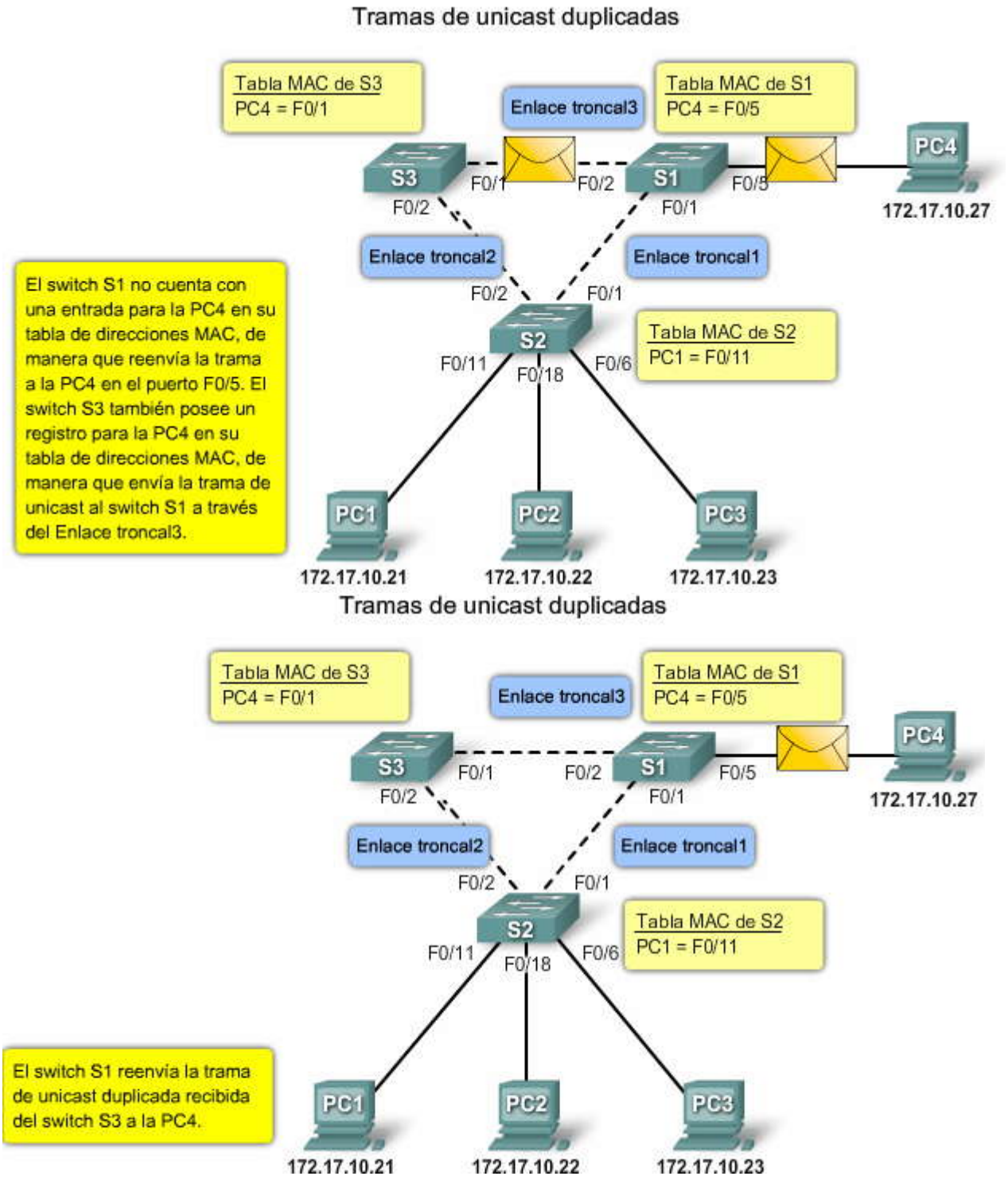
6. S1 recibe la trama duplicada y una vez más la reenvía a la PC4.

7. La PC4 ha recibido ahora la misma trama dos veces.

La mayoría de los protocolos de capa superior no están diseñados para reconocer transmisiones duplicadas o para enfrentarlas. En general, los protocolos que utilizan un mecanismo de numeración en secuencia asumen que la transmisión ha fallado y que el número de secuencia se ha reciclado para otra sesión de comunicación. Otros protocolos intentan enviar la transmisión duplicada al protocolo de capa superior adecuado para que sea procesada y posiblemente descartada.

Afortunadamente, los switches pueden detectar bucles en una red. El protocolo spanning tree (STP) elimina estos inconvenientes relacionados con bucles. Aprenderá acerca de STP en la sección siguiente.





5.1.3 INCOVENIENTES REALES RELACIONADOS CON LA REDUNDANCIA.-

Bucles en el armario de cableado

La redundancia es un componente importante de una topología de red jerárquica de alta disponibilidad, pero los bucles pueden surgir como resultado de varias rutas configuradas en la red. Se pueden evitar los bucles mediante el protocolo spanning tree (STP). Sin embargo, si STP no se ha implementado en la preparación de una topología redundante, los bucles pueden ocurrir de improviso.

El cableado de red para pequeñas y medianas empresas puede tornarse demasiado confuso. Los cables de red entre los switches de la capa de acceso, ubicados en los armarios de cableado, desaparecen en las paredes, pisos y techos donde vuelven a los switches de la capa de distribución de la red. Si los cables de red no están rotulados de forma adecuada cuando finalizan en el panel de conexión del armario de cableado, es difícil determinar cuál es el destino del puerto en el panel de

conexión de la red. Los bucles de red que son el resultado de conexiones duplicadas accidentales en los armarios de cableado son muy comunes.

Haga clic en el botón Bucle de dos conexiones al mismo switch que se muestra en la figura.

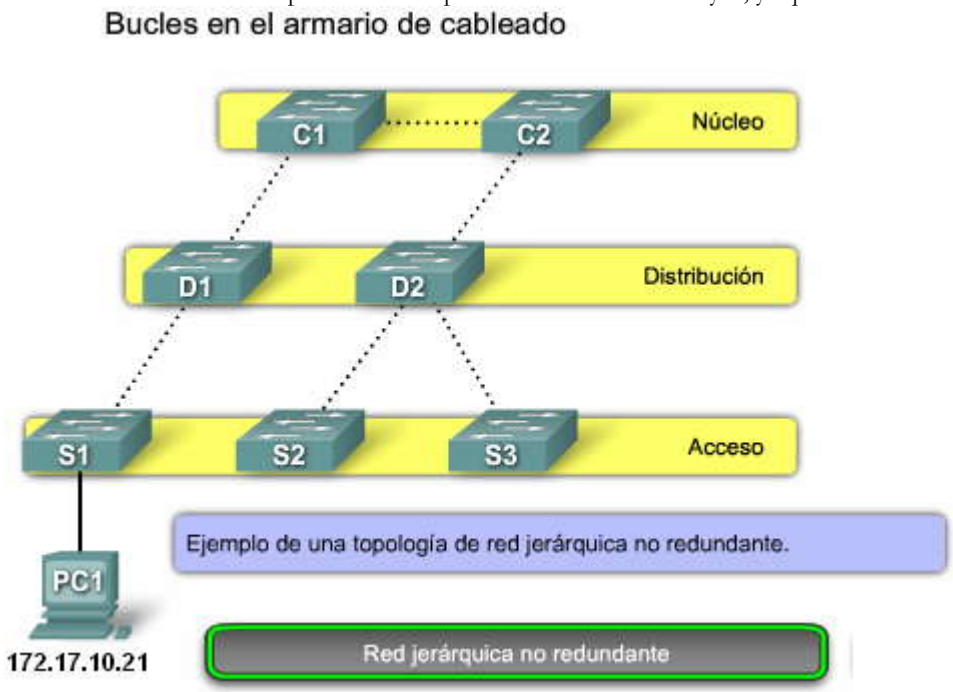
El ejemplo muestra un bucle que se genera cuando dos conexiones del mismo switch se conectana otro switch. El bucle se localiza en los switches que están interconectados. Sin embargo, el bucle afecta al resto de la red debido a la gran cantidad de envíos de broadcast que llega a todos los otros switches de la red. Quizá el impacto en los otros switches no sea suficiente como para interrumpir las comunicaciones legítimas, pero puede afectar de manera notable al rendimiento total de los demás switches.

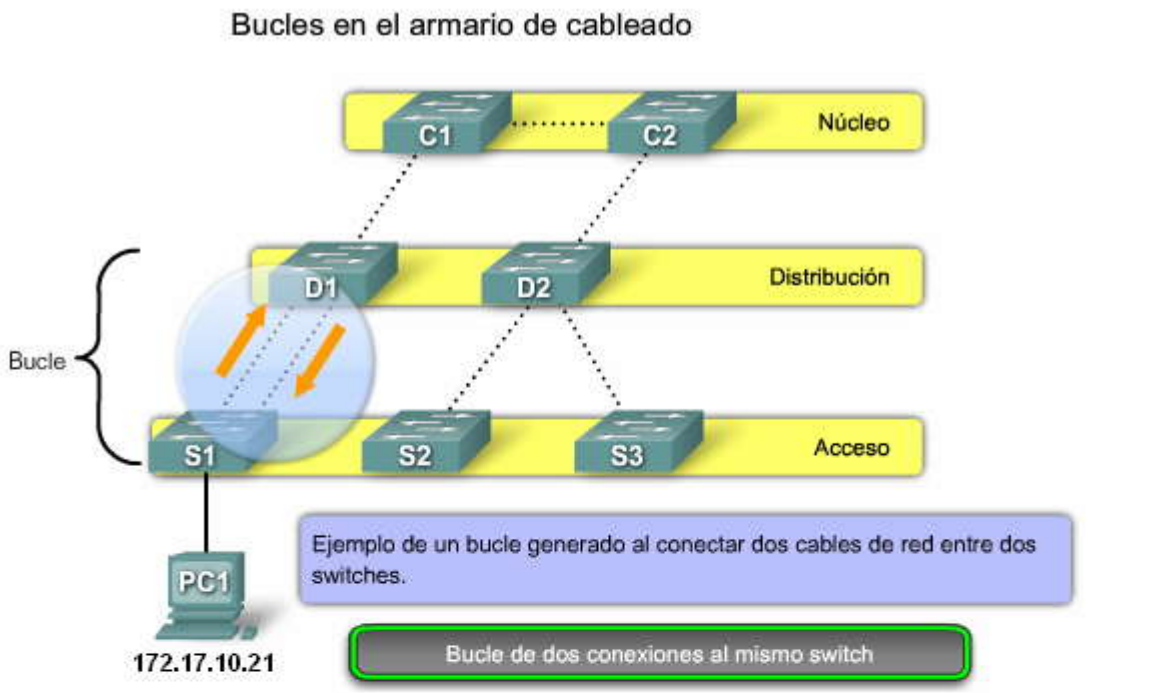
Este tipo de bucle es muy común en el armario de cableado. Sucede cuando un administrador conecta de manera errónea un cable al mismo switch al que ya está conectado. Por lo general, esto sucede cuando los cables de red no están rotulados o están mal rotulados o cuando el administrador no se ha tomado tiempo para verificar dónde están conectados losmismos.

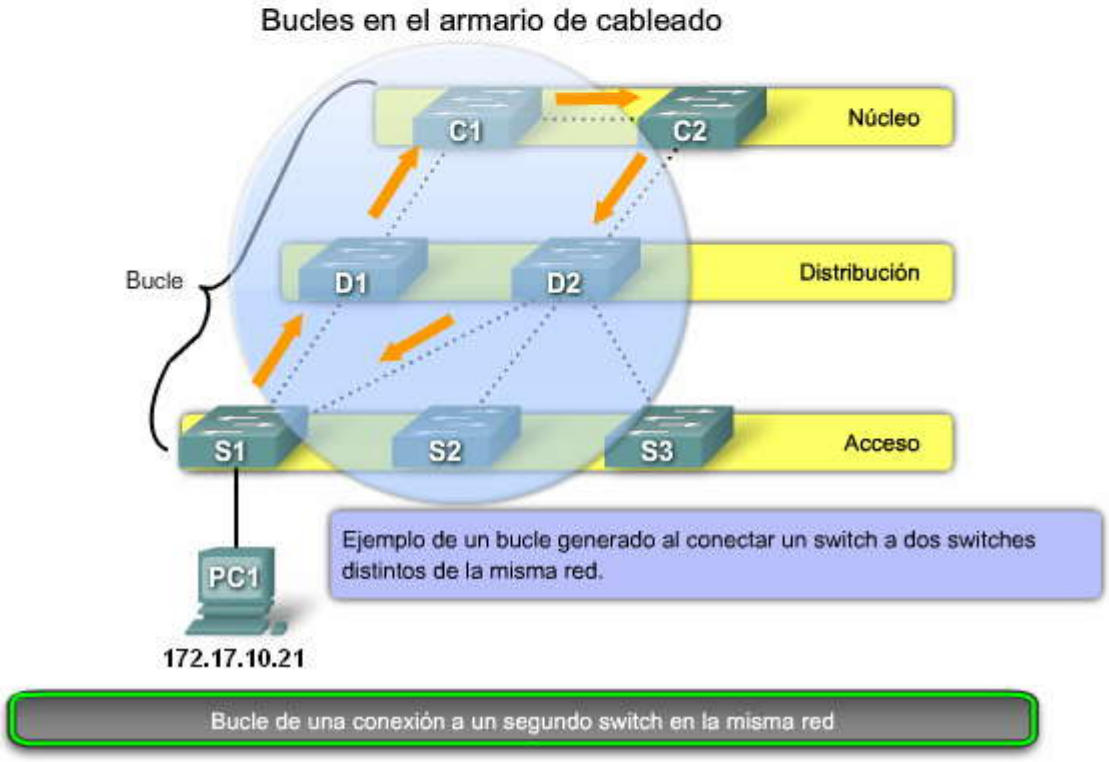
Existe una excepción para este problema. Un EtherChannel es un grupo de puertos Ethernet en un switch que actúa como una única conexión de red lógica. Debido a que el switch trata a los puertos configurados para el EtherChannel como un único enlace de red, los bucles no son posibles. La configuración de EtherChannels excede el alcance de este curso. Si desea obtener más información acerca de EtherChannels, visite:
http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml

Haga clic en el botón Bucle de una conexión a un segundo switch en la misma red que se muestra en la figura.

El ejemplo muestra un bucle que se genera cuando un switch se conecta a dos switches distintos de la red que a su vez están interconectados entre sí. El impacto de este tipo de bucle es mucho mayor, ya que afecta a más switches de forma directa.







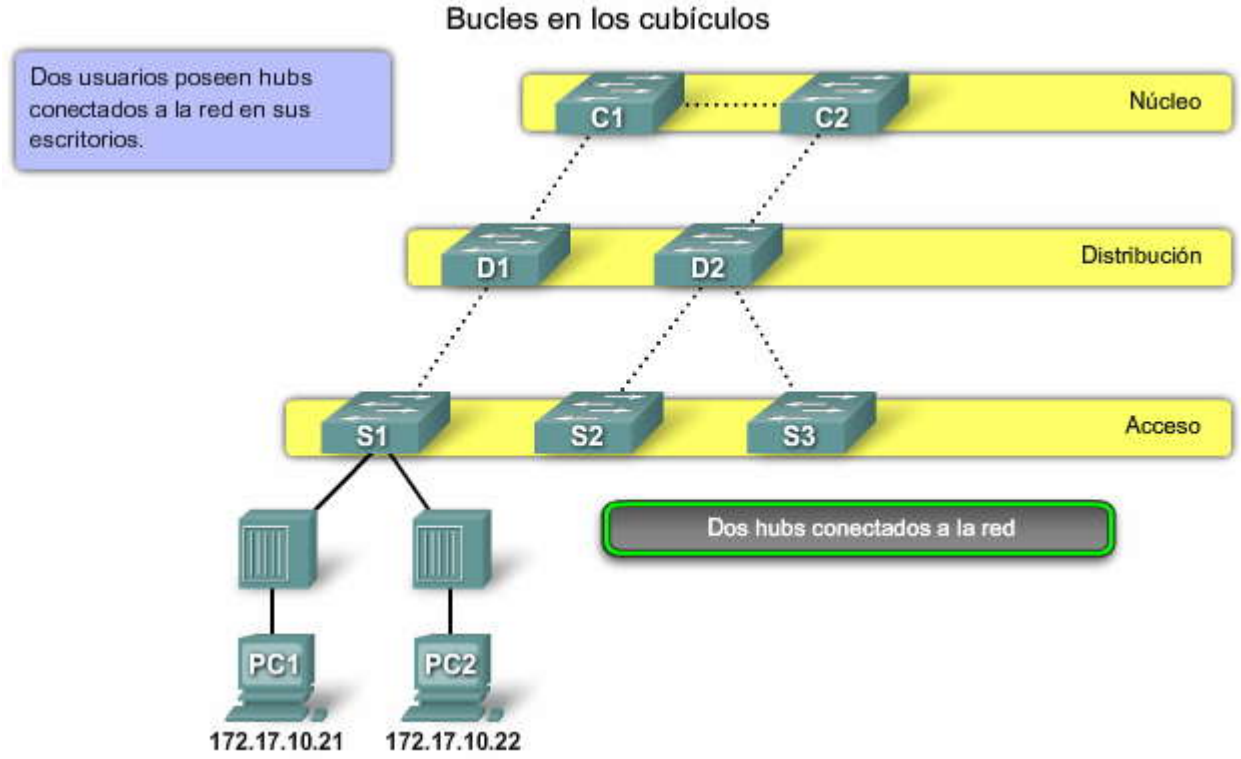
Bucles en los cubículos

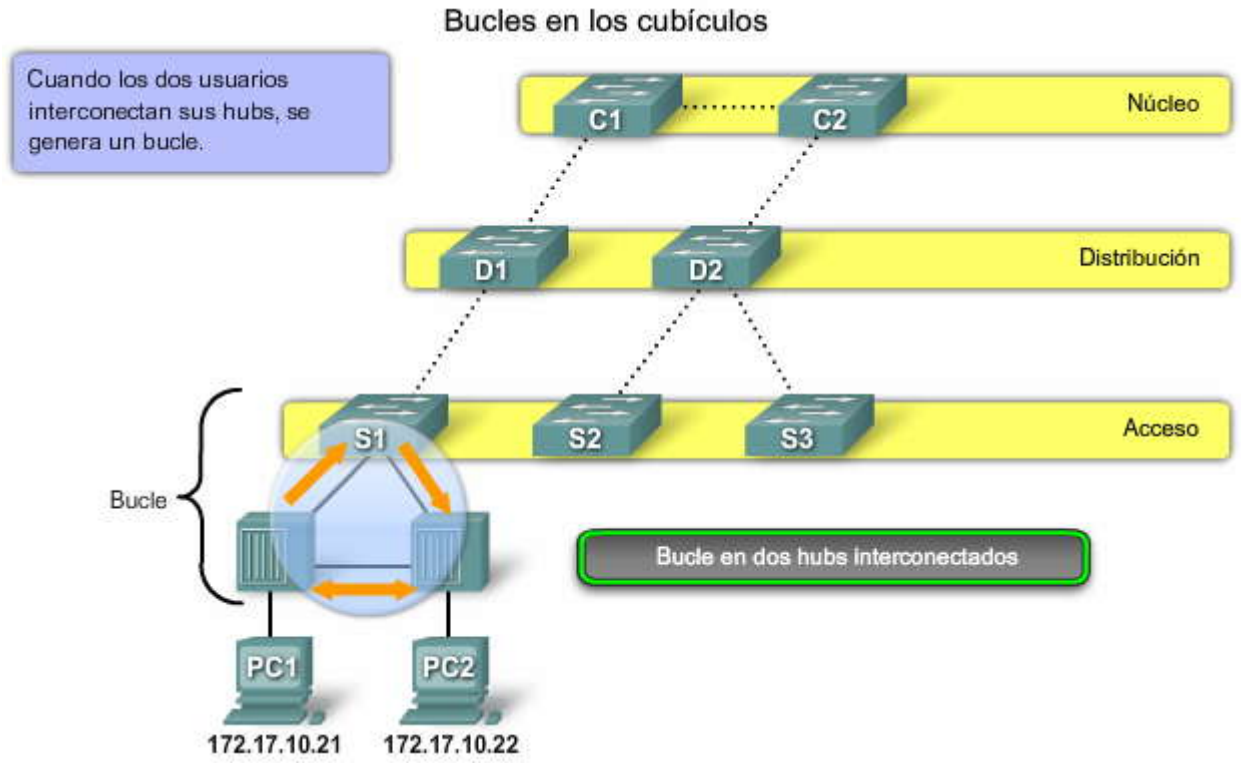
Debido a conexiones de datos de red insuficientes, algunos usuarios finales poseen un hub o switch personal ubicado en su entorno de trabajo. En vez de incurrir en el costo de mantener conexiones de datos de red adicionales en el lugar de trabajo, un hub o switch simples se conectan a una conexión de datos de red existente, lo que permite que todos los dispositivos conectados al hub o switch personal puedan acceder a la red.

En general, los armarios de cableado están asegurados para evitar el acceso no autorizado, de manera que sólo el administrador de red posee el control total sobre los dispositivos conectados a la redy la forma en que los mismos están conectados. A diferencia del armario de cableado, el administrador no posee el control sobre la forma en que los switches o hubs personales están conectados o son utilizados, de manera que el usuario final puede interconectarlos de forma accidental.

Haga clic en botón Bucle en dos hubs interconectados que se muestra en la figura.

En el ejemplo, los dos hubs de usuario están interconectados, lo que genera un bucle de red. El bucle interrumpe la comunicación entre todos los dispositivos conectados al switch S1.





5.2 INTRODUCCION A STP.-
5.2.1 EL ALGORITMO SPANNING TREE.-
Topología de STP

La redundancia aumenta la disponibilidad de la topología de red al proteger la red de un único punto de falla, como un cable de red o switch que fallan. Cuando se introduce la redundancia en un diseño de la Capa 2, pueden generarse bucles y tramas duplicadas. Los bucles y las tramas duplicadas pueden tener consecuencias graves en la red. El protocolo spanning tree (STP) fue desarrollado para enfrentar estos inconvenientes.

STP asegura que exista sólo una ruta lógica entre todos los destinos de la red, al bloquear de forma intencional aquellas rutas redundantes que puedan ocasionar un bucle. Un puerto se considera bloqueado cuando el tráfico dela red no puede ingresar ni salir del puerto. Esto no incluye las tramas de unidad de datos del protocolo de puentes (BPDU) utilizadas por STP para evitar bucles. Aprenderá más acerca de las tramas de BPDU de STP más adelante en este capítulo. El bloqueo de las rutas redundantes es fundamental para evitar bucles en la red. Las rutas físicas aún existen para proporcionar la redundancia, pero las mismas se deshabilitan para evitar que se generen bucles. Si alguna vez la ruta es necesaria para compensar la falla de un cable de red o de un switch, STP vuelve a calcular las rutas y desbloquea los puertos necesarios para permitir que la ruta redundante se active.

Haga clic en el botón Reproducir de la figura para iniciar la animación.

En el ejemplo, STP está habilitado en todos los switches.

1. La PC1 envía un broadcast a la red.

2. El switch S3 se configura con STP y establece el puerto para el Enlace troncal2 en el estado de bloqueo. El estado de bloqueo evita que los puertos sean utilizados para enviar tráfico de switch, lo que impide que se generen bucles. El switch S2 envía una trama de broadcast a todos los puertos de switch, excepto el puerto de origen para la PC1 y el puerto del Enlace troncal2, que lleva al puerto bloqueado en S3.

3. El switch S1 recibe la trama de broadcast y la reenvía a todos sus puertos de switch, donde llega a la PC4 y S3. S3 no reenvía la trama de vuelta a S2 a través del Enlace troncal2 debido al puerto bloqueado. Se evita el bucle de Capa 2.

Haga clic en el botón STP compensa las fallas de la red en la figura y haga clic en Reproducir para iniciar la animación.

En este ejemplo:

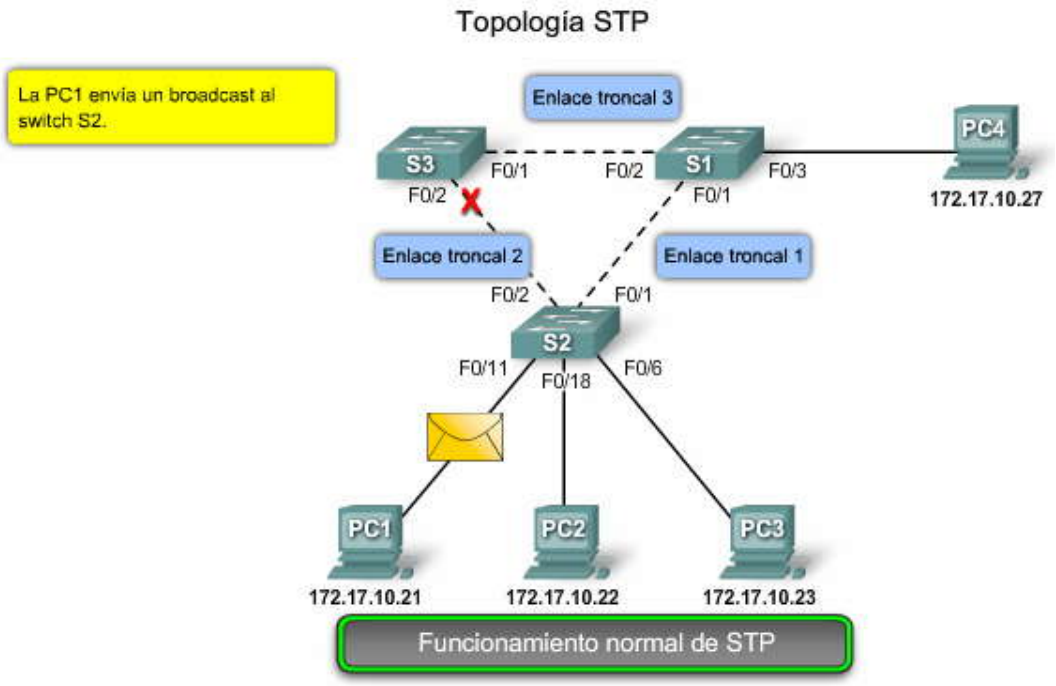
1. La PC1 envía un broadcast a la red.

2. Luego el broadcast se envía a través de la red, de la misma forma que en la animación anterior.

3. El enlace troncal entre el switch S2 y el switch S1 falla, lo que produce la interrupción de la ruta anterior.

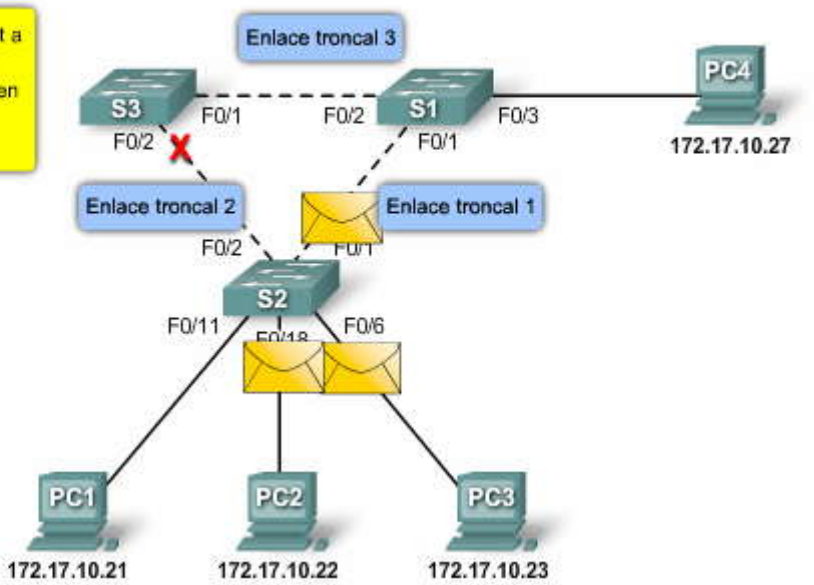
4. El switch S3 desbloquea el puerto bloqueado anteriormente para el Enlace troncal2 y permite que el tráfico de broadcast se transmita por la ruta alternativa por toda la red, lo que posibilita la continuidad de la comunicación. Si este enlace vuelve a conectarse, STP vuelve a converger y el puerto de S3 vuelve a bloquearse.

STP evita que se generen bucles mediante la configuración de una ruta sin bucles a través de la red en base a puertos en estado de bloqueo colocados de manera estratégica. Los switches que ejecutan STP pueden compensar las fallas mediante el desbloqueo dinámico de los puertos bloqueados anteriormente y el permiso para que el tráfico se transmita por las rutas alternativas. El tema siguiente describe la forma en que STP logra este proceso de forma automática.



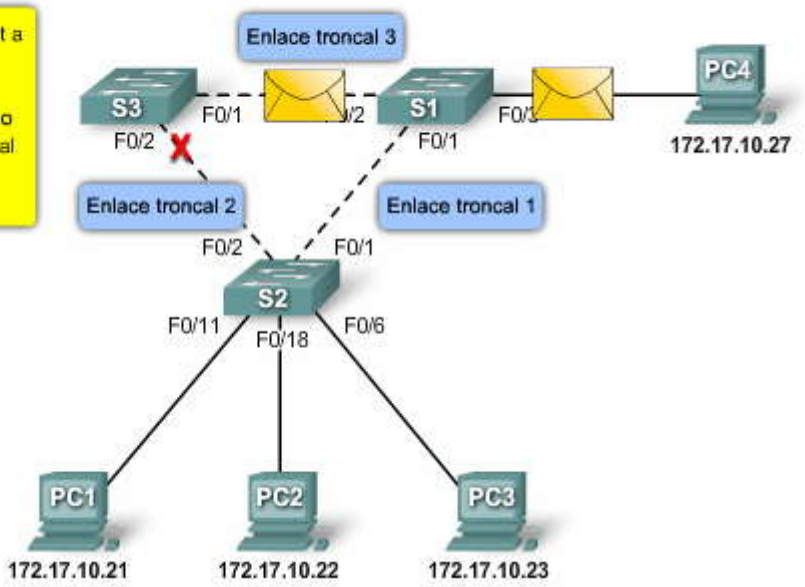
Topología STP

El switch S2 reenvía el broadcast a través de todos los puertos del switch, excepto el puerto de origen y el puerto relacionado con el Enlace troncal 2.



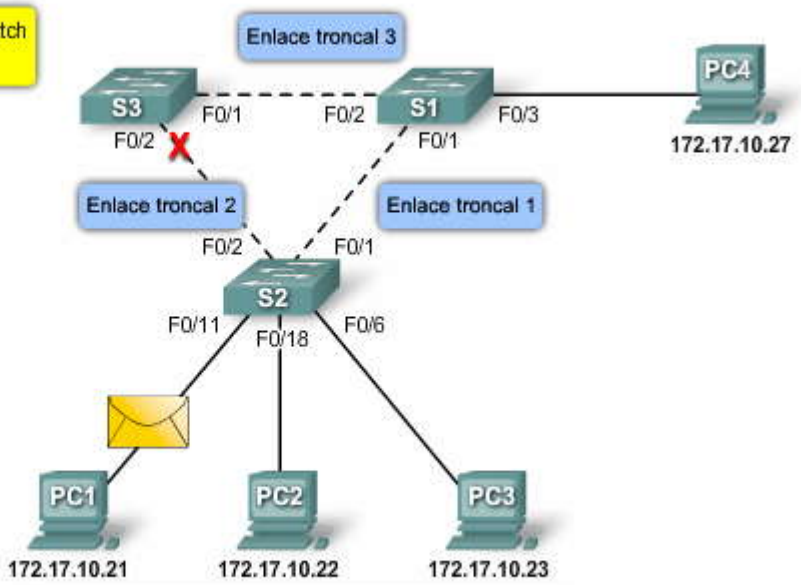
Topología STP

El switch S1 reenvía el broadcast a través de todos los puertos, excepto el puerto de origen. El switch S3 recibe la trama, pero no continúa reenviándola de nuevo al switch S2 debido al puerto bloqueado.



Topología STP

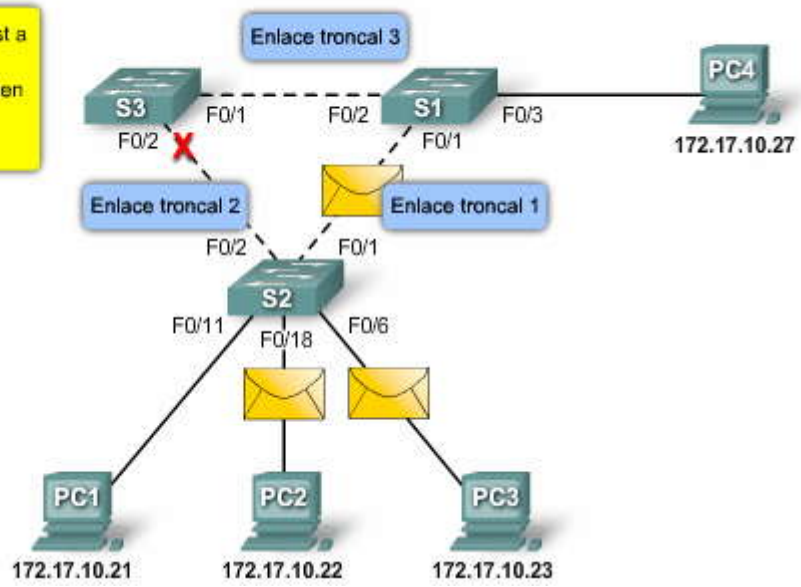
La PC1 envía un broadcast al switch S2.



STP compensa las fallas de la red

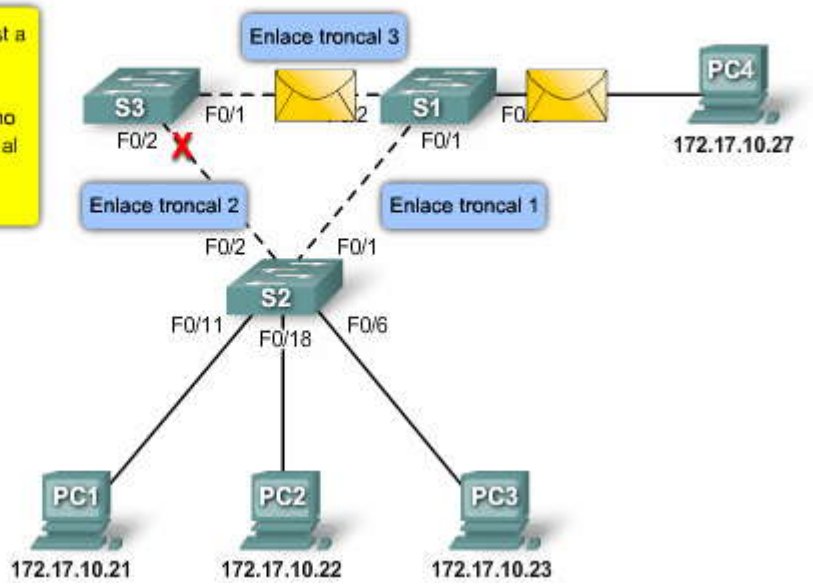
Topología STP

El switch S2 reenvía el broadcast a través de todos los puertos del switch, excepto el puerto de origen y el puerto relacionado con el Enlace troncal 2.



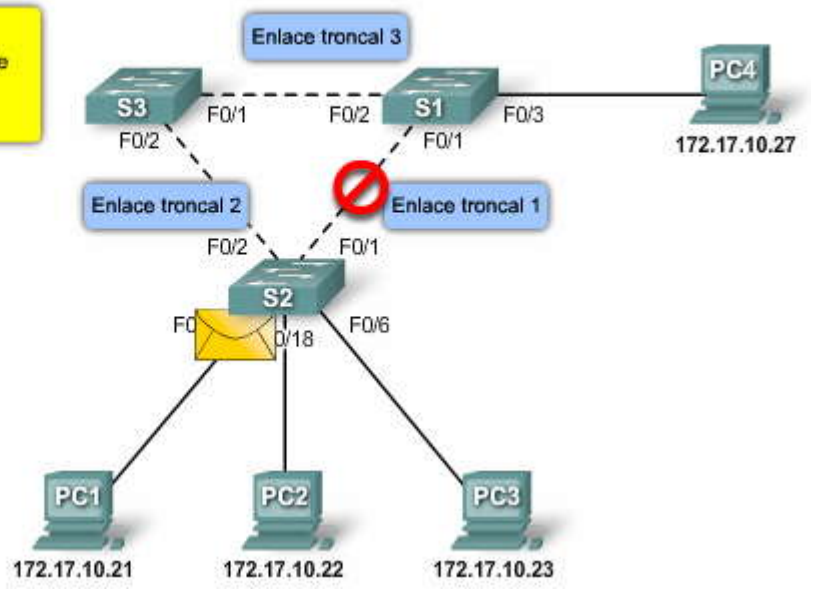
Topología STP

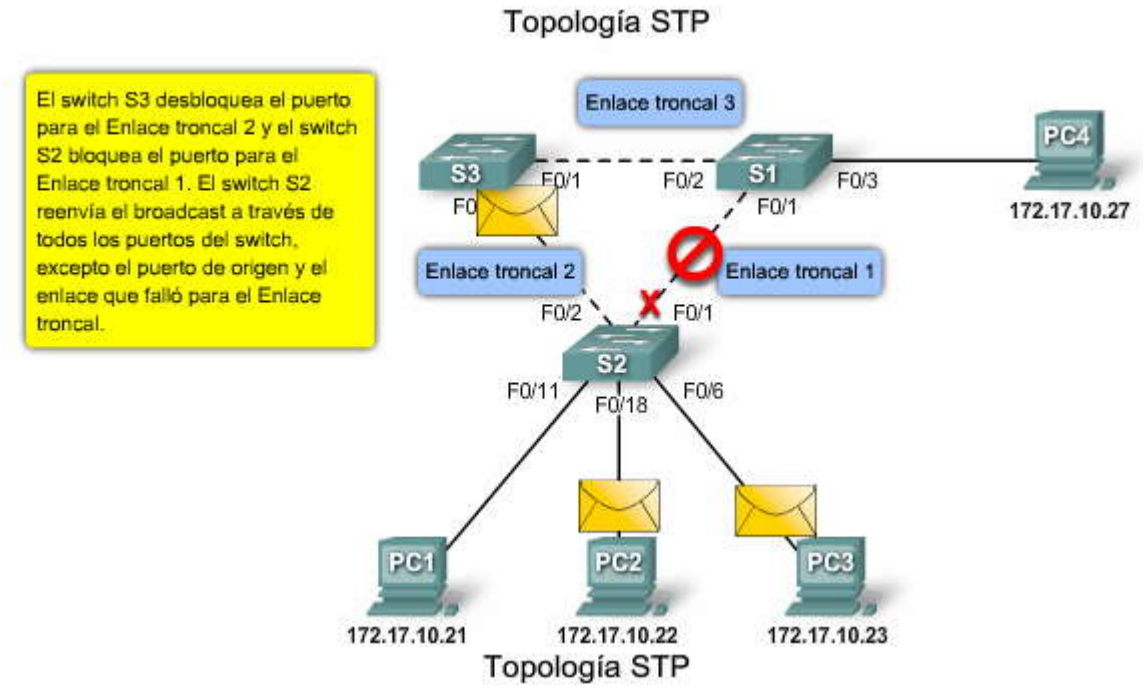
El switch S1 reenvía el broadcast a través de todos los puertos, excepto el puerto de origen. El switch S3 recibe la trama, pero no continúa reenviándola de nuevo al switch S2 debido al puerto bloqueado.

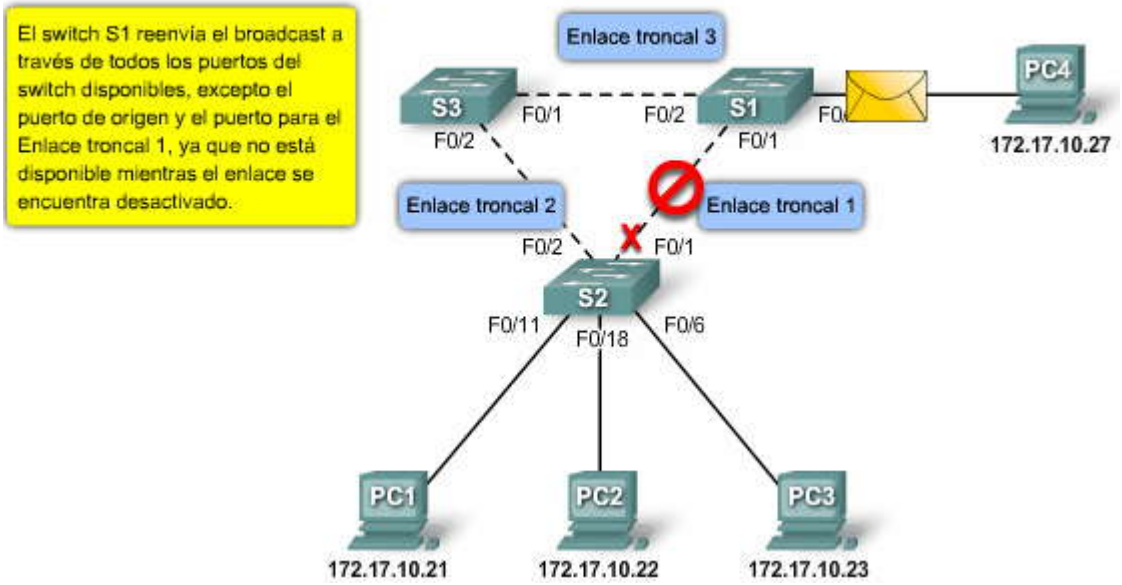


Topología STP

La PC1 envía una trama de broadcast al switch S2. El enlace troncal entre el switch S2 y el switch S1 ha fallado.







Algoritmo STP

STP utiliza el algoritmo spanning tree (STA) para determinar los puertos de switch de la red que deben configurarse para el bloqueo, y así evitar que se generen bucles. El STA designa un único switch como puente raíz y lo utiliza como punto de referencia para todos los cálculos de rutas. En la figura, el puente raíz, el switch S1, se escoge a través de un proceso de elección. Todos los switches que comparten STP intercambian tramas de BPDU para determinar el switch que posee el menor ID de puente (BID) en la red. El switch con el menor BID se transforma en el puente raíz de forma automática según los cálculos del STA. El proceso de elección del puente raíz se explicará en detalle más adelante en este capítulo.

La BPDU es la trama de mensaje que se intercambia entre los switches en STP. Cada BPDU contiene un BID que identifica al switch que envió la BPDU. El BID contiene un valor de prioridad, la dirección MAC del switch emisor y un ID de sistema extendido opcional. Se determina el BID de menor valor mediante la combinación de estos tres campos. Aprenderá más acerca del puente raíz, la BPDU y el BID en temas posteriores.

Después de determinar el puente raíz, el STA calcula la ruta más corta hacia el mismo. Todos los switches utilizan el STA para determinar los puertos que deben bloquearse. Al determinar el STA las mejores rutas hacia el puente raíz para todos los destinos del dominio de broadcast, se evita que todo el tráfico sea enviado a través de la red. El STA considera los costos tanto de la ruta como del puerto cuando determina la ruta que debe permanecer desbloqueada. Los costos de la ruta se calculan mediante los valores de costo de puerto asociados con las velocidades de los puertos para cada puerto de switch que atraviesa una ruta determinada. La suma de los valores de costo de puerto determina el costo de ruta total para el puente

raíz. Si existe más de una ruta a escoger, el STA elige la de menor costo de ruta. Aprenderá más acerca de costos de rutas y de puertos en temas posteriores.

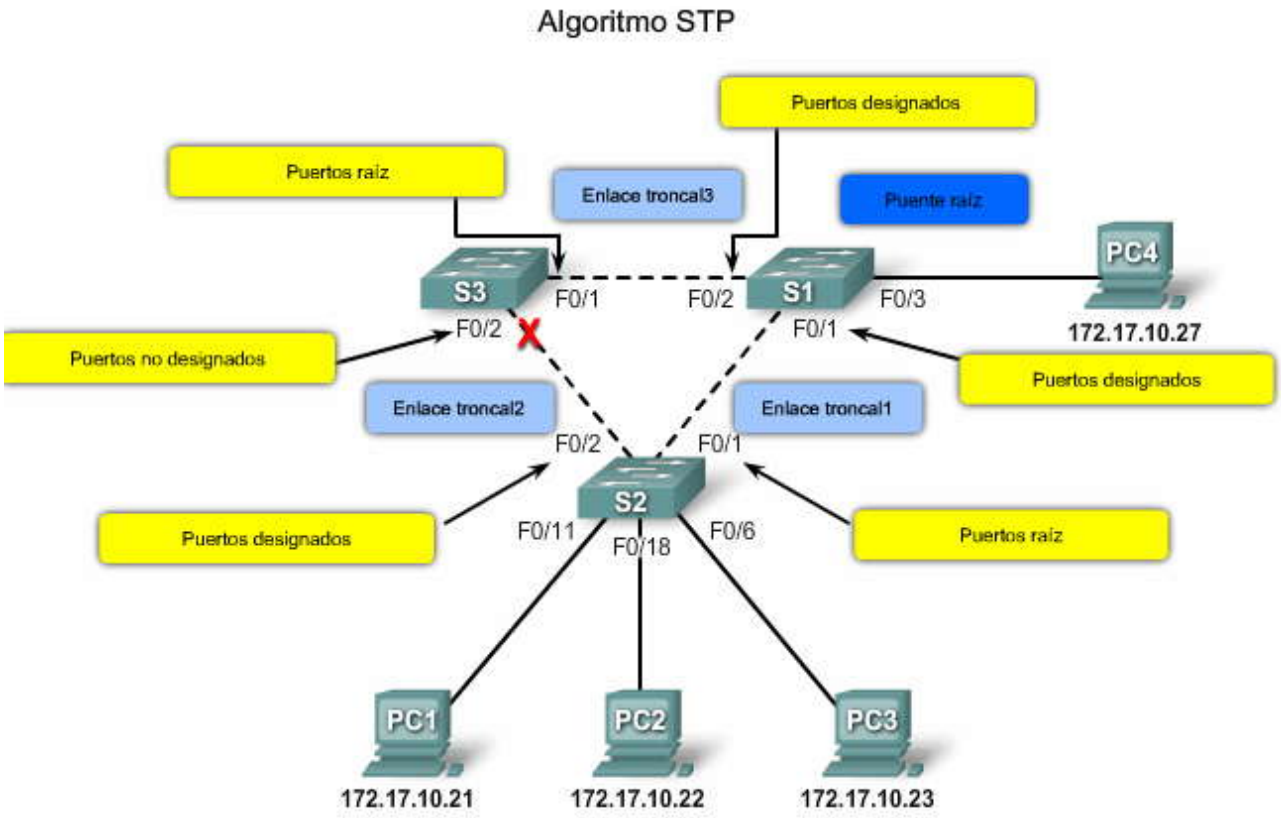
Cuando el STA determina las rutas que deben permanecer disponibles, configura los puertos de switch de acuerdo con distintas funciones. Las funciones de los puertos describen su relación en la red con el puente raíz y si los mismos pueden enviar tráfico.

Puertos raíz: los puertos de switch más cercanos al puente raíz. En el ejemplo, el puerto raíz del switch S2 es F0/1, configurado para el enlace troncal entre el switch S2 y el switch S1. El puerto raíz del switch S3 es F0/1, configurado para el enlace troncal entre el switch S3 y el switch S1.

Puertos designados: todos los puertos que no son raíz y que aún pueden enviar tráfico a la red. En el ejemplo, los puertos de switch F0/1 y F0/2 del switch S1 son puertos designados. El switch S2 también cuenta con su puerto F0/2 configurado como puerto designado.

Puertos no designados: todos los puertos configurados en estado de bloqueo para evitar los bucles. En el ejemplo, el STA configura al puerto F0/2 del switch S3 en la función no designado. El puerto F0/2 del switch S3 se encuentra en estado de bloqueo.

Aprenderá más acerca de las funciones y estados de los puertos en temas posteriores.



El puente raíz

Toda instancia de spanning-tree (LAN conmutada o dominio de broadcast) posee un switch designado como puente raíz. El puente raíz sirve como punto de referencia para todos los cálculos de spanning-tree para determinar las rutas redundantes que deben bloquearse.

Un proceso de elección determina el switch que se transforma en el puente raíz.

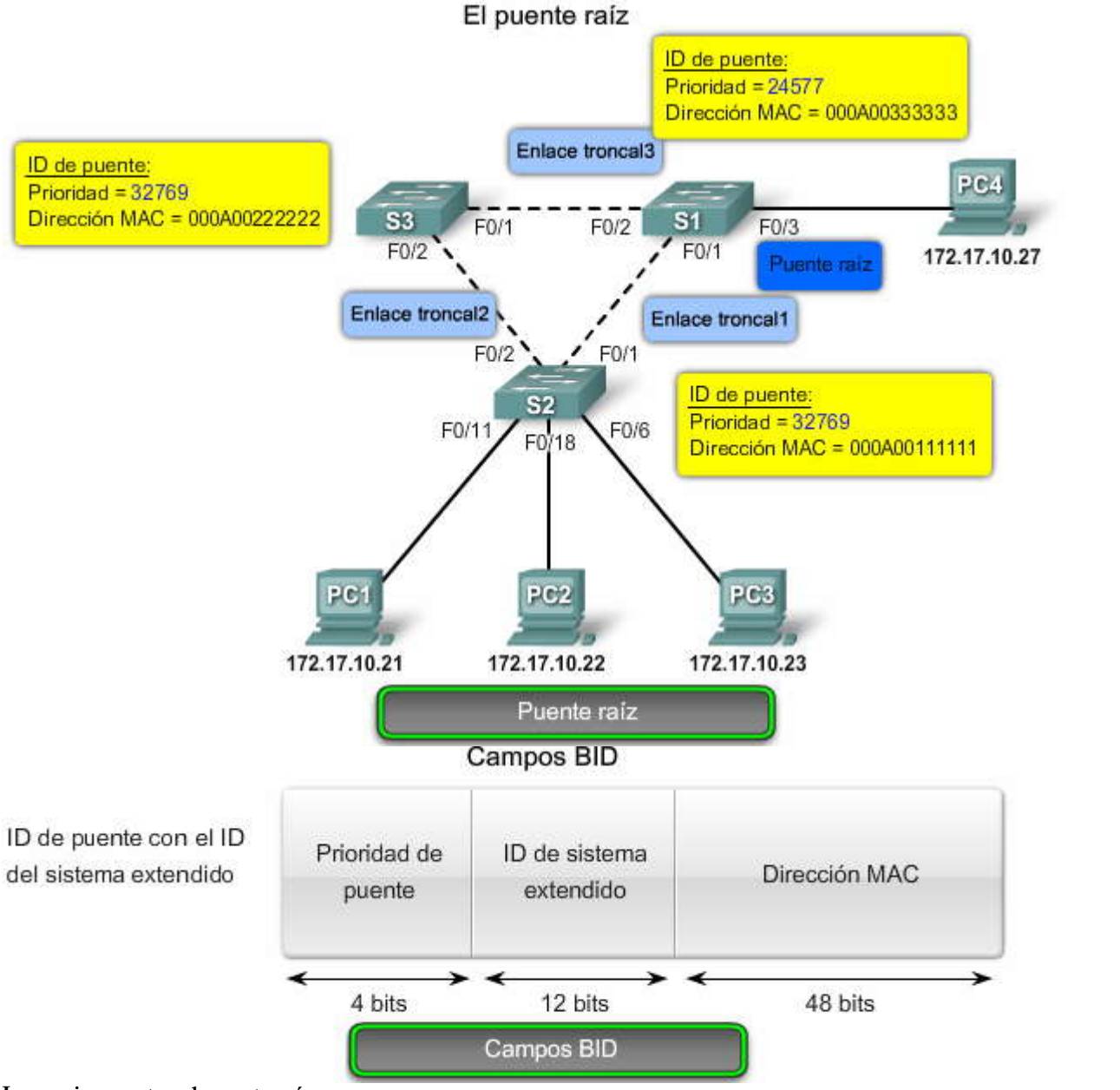
Haga clic en el botón Campos BID que se muestra en la figura.

La figura muestra los campos BID. Los detalles acerca de cada campo BID se explicarán más adelante, pero es útil saber que el BID se compone de un valor de prioridad, un ID de sistema extendido y la dirección MAC del switch.

Todos los switches del dominio de broadcast participan del proceso de elección. Cuando se inicia un switch, el mismo envía tramas de BPDU que contienen el BID del switch y el ID de raíz cada dos segundos. De manera predeterminada, el ID de

raíz coincide con el BID local para todos los switches de la red. El ID de raíz identifica al puente raíz de la red. Inicialmente, cada switch se identifica a sí mismo como puente raíz después del arranque.

A medida que los switches envían sus tramas de BPDU, los switches adyacentes del dominio de broadcast leen la información del ID de raíz de la trama de BPDU. Si el ID de raíz de la BPDU recibida es menor que el ID de raíz del switch receptor, este último actualiza su ID de raíz mediante la identificación del switch adyacente como el puente raíz. Nota: Es posible que no sea un switch adyacente, sino cualquier otro switch del dominio de broadcast. Luego el switch envía nuevas tramas de BPDU con el menor ID de raíz a los otros switches adyacentes. Eventualmente, el switch con el menor BID es identificado finalmente como puente raíz para la instancia de spanning-tree.



Las mejores rutas al puente raíz

Cuando se ha designado el puente raíz para la instancia de spanning-tree, el STA comienza el proceso de determinar las mejores rutas hacia el puente raíz desde todos los destinos del dominio de broadcast.La información de ruta se determina mediante la suma de los costos individuales de los puertos que atraviesa la ruta desde el destino al puente raíz.

Los costos de los puertos predeterminados se definen por la velocidad a la que funcionan los mismos. Enla tabla, puede verse que los puertos Ethernet de 10 Gb/s poseen un costo de puerto de 2, los puertos Ethernet de 1 Gb/s poseen un costo de puerto de 4, los puertos Fast Ethernet de 100 Mb/s poseen un costo de puerto de 19 y los puertos Ethernet de 10 Mb/s poseen un costo de puerto de 100.

Nota: El IEEE define los valores de costos de puertos utilizados por STP. Actualmente, debido al ingreso reciente al mercado de tecnologías Ethernet más veloces, los valores de costos de rutas pueden cambiar para ajustarse a las distintas velocidades disponibles. Los números no lineales se ajustan a algunas mejoras del estándar Ethernet, pero tenga en cuenta

que dichos números pueden ser modificados por el IEEE si fuera necesario. En la tabla, los valores ya se han modificado para ajustarse al estándar Ethernet de 10 Gb/s más reciente.

Pese a que los puertos de switch cuentan con un costo de puerto predeterminado asociado a los mismos, tal costo puede configurarse. La capacidad para configurar los costos de puertos individuales proporciona al administrador la flexibilidad para controlar las rutas de spanning-tree hacia el puente raíz.

Haga clic en el botón Configurar costos de los puertos que se muestra en la figura.

Para configurar el costo de un puerto en una interfaz, ingrese el comando **spanning-tree cost** valor en modo de configuración de interfaz. El rango de valores puede oscilar entre 1 y 200 000 000.

En el ejemplo, el puerto de switch F0/1 se ha configurado con un costo de puerto de 25 mediante el comando de configuración de interfaz **spanning-tree cost 25** en la interfaz de F0/1.

Para volver a establecer el costo de puerto al valor predeterminado, ingrese el comando de configuración de interfaz no **spanning-tree cost**.

Haga clic en el botón Costos de ruta que se muestra en la figura.

El costo de la ruta es la suma de todos los costos de puertos que atraviesan la ruta hacia el puente raíz. La ruta con el menor costo de ruta se convierte en la ruta preferida y todas las demás rutas redundantes se bloquean. En el ejemplo, el costo de ruta desde el switch S2 hacia el switch puente raíz S1, a través de la ruta 1 es 19 (en base a los costos de puertos individuales especificados por el IEEE), mientras que el costo de ruta a través de la ruta 2 es 38. Ya que la ruta 1 poseeel menor costo total de ruta hacia el puente raíz, la misma es la ruta preferida. Luego, STP configura la ruta redundante que debe bloquearse y evita así la generación de bucles.

Haga clic en el botón Verificar costos de puerto y de ruta que se muestra en la figura.

Para verificar el costo de puerto y de ruta hacia el puente raíz, ingrese el comando del modo EXEC privilegiado **show spanning-tree**. El campo Costo del resultado es el costo de ruta total hacia el puente raíz. Este valor cambia en función de la cantidad de puertos de switch necesarios para llegar al puente raíz. En el resultado, cada interfaz también se identifica con un costo de puerto individual de 19.

Otro comando para examinar es el comando del modo EXEC privilegiado **show spanning-tree detail**.

Las mejores rutas al puente raiz

Velocidad de enlace	Costo (especificación IEEE revisada)	Costo (especificación IEEE anterior)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

Costos de puertos

Las mejores rutas al puente raíz

Configurar costo del puerto

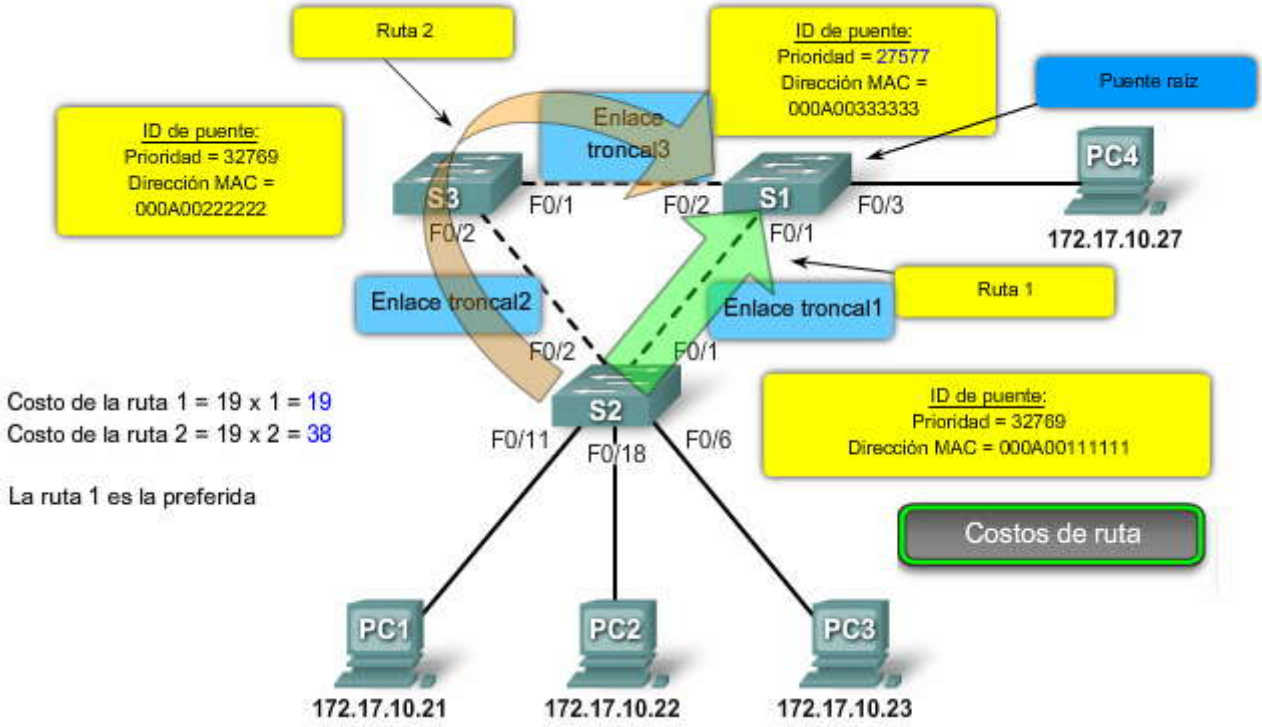
```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#spanning-tree cost 25
S2(config-if)#end
S2#
```

Configurar costos de los puertos

Restablecer costo del puerto

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#no spanning-tree cost
S2(config-if)#end
S2#
```

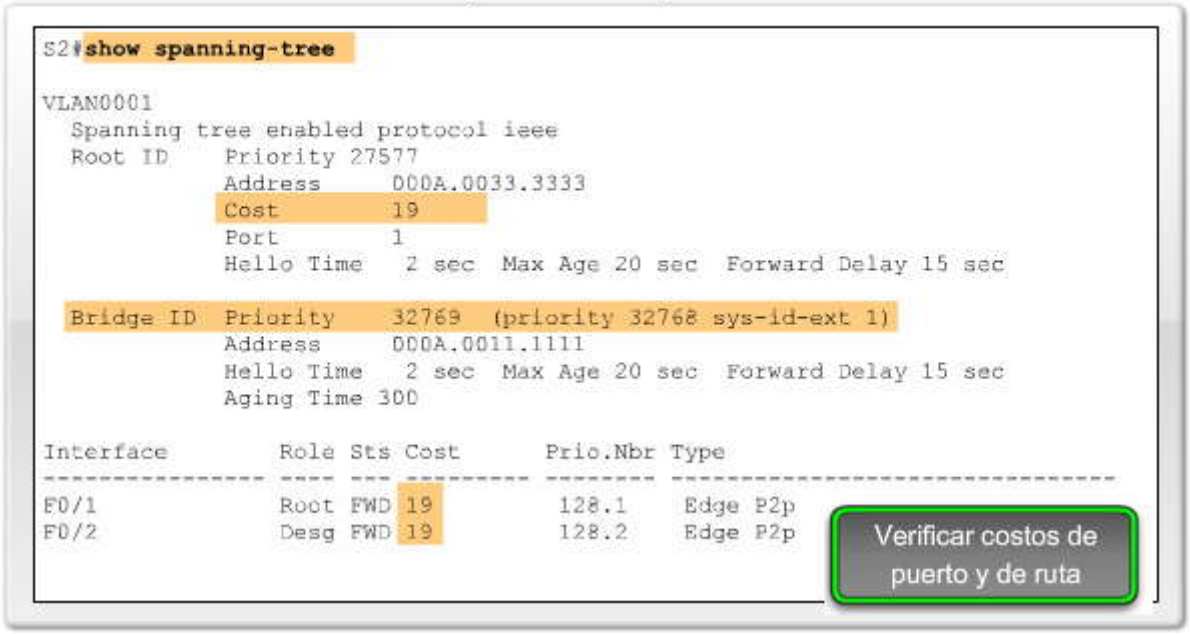
Las mejores rutas al puente raíz



Costo de la ruta 1 = 19 x 1 = 19
Costo de la ruta 2 = 19 x 2 = 38

La ruta 1 es la preferida

Las mejores rutas al puente raíz



5.2.2 BPDU EN STP.-

Campos BPDU

En el tema anterior aprendió que STP determina un puente raíz para la instancia de spanning-tree mediante el intercambio de BPDU. En este tema aprenderá los detalles de la trama de BPDU y la forma en que la misma facilita el proceso de spanning-tree.

La trama de BPDU contiene 12 campos distintos que se utilizan para transmitir información de prioridad y de ruta que STP necesita para determinar el puente raíz y las rutas al mismo.

Desplace el mouse sobre los campos BPDU de la figura para ver su contenido.

Los primeros cuatro campos identifican el protocolo, la versión, el tipo de mensaje y los señaladores de estado.
Los cuatro campos siguientes se utilizan para identificar el puente raíz y el costo de la ruta hacia el mismo.
Los últimos cuatro campos son todos campos temporizadores que determinan la frecuencia en que se envían los mensajes de BPDU y la cantidad de tiempo que la información recibida a través del proceso BPDU (siguiente tema) es retenida. La función de los campos temporizadores se explicará con más detalle posteriormente en este curso.

Haga clic en el botón Ejemplo de BPDU que se muestra en la figura.

El ejemplo de la figura se capturó con Wireshark. En el ejemplo, la trama de BPDU contiene más campos de los que se describieron anteriormente. El mensaje de BPDU se encapsula en una trama de Ethernet cuando se transmite a través de la red. El encabezado 802.3 indica las direcciones de origen y destino de la trama de BPDU. Esta trama posee una dirección MAC de destino 01:80:C2:00:00:00, que corresponde a una dirección multicast para el grupo de spanning-tree. Cuando se envía una trama con esta dirección MAC, todos los switches que están configurados para spanning tree aceptan y leen la información de la trama. Al utilizar esta dirección de grupo multicast, todos los otros dispositivos en la red que reciben la trama la ignoran.

En este ejemplo, el ID de raíz y el BID son iguales en la trama de BPDU capturada. Esto indica que la trama se capturó de un switch del puente raíz.

Todos los temporizadores se establecen en sus valores predeterminados.

Campos BPDU

Campo #	Bytes	Campo
4	2	ID de protocolo
	1	Versión
	1	Tipo de mensaje
	1	Señaladores
8	8	ID de raíz
	4	Costo de la ruta
	8	ID de puente
	2	ID del puerto
12	2	Antigüedad del mensaje
	2	Antigüedad máxima
	2	Tiempo de saludo
	2	Retraso en el envío

Campos BPDU

El campo ID de protocolo indica el tipo de protocolo que se utiliza. Este campo contiene el valor cero.

El campo Versión indica la versión del protocolo. Este campo contiene el valor cero.

El campo Tipo de mensaje indica el tipo de mensaje. Este campo contiene el valor cero.

El campo Señaladores incluye uno de los siguientes valores:
Bit de Cambio de topología (TC), que señala un cambio en la topología en el caso de que una ruta al puente raíz se haya interrumpido.
Bit de Acuse de recibo de cambio de topología (TCA), que se establece para acusar recibo de un mensaje de configuración con el bit de TC configurado.

El campo ID de raíz indica el puente raíz enumerando su prioridad de 2 bytes seguida por su ID de dirección MAC de 6 bytes. Cuando se inicia un switch por primera vez, el ID de raíz es igual al ID de puente. Sin embargo, a medida que se desarrolla el proceso de elección, el ID de puente más bajo reemplaza al ID de raíz local para identificar al switch del puente raíz.

El campo Costo de la ruta indica el costo de la ruta desde el puente que envía el mensaje de configuración al puente raíz. El campo costo de la ruta es actualizado por cada switch de la ruta al puente raíz.

El campo ID de puente indica el ID de dirección MAC y de prioridad del puente que envía el mensaje. Esta etiqueta permite que el puente raíz identifique dónde se originó el BPDU, así como las rutas múltiples desde el switch hasta el puente raíz. Cuando el puente raíz recibe más de un BPDU de un switch con distintos costos de ruta, reconoce que existen dos rutas diferentes y utiliza aquella ruta con el menor costo.

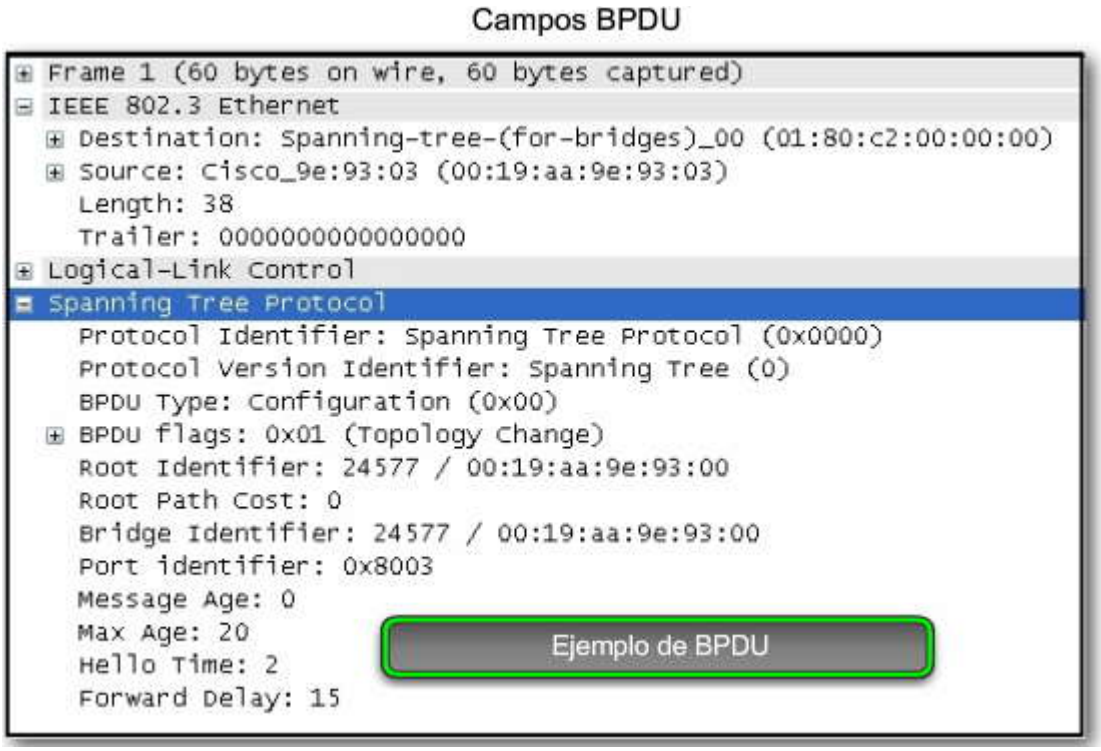
El campo ID de puerto indica el número de puerto desde el cual se envía el mensaje de configuración. Este campo permite que los bucles generados por puentes múltiples conectados sean detectados y corregidos.

El campo Antigüedad del mensaje indica la cantidad de tiempo que ha transcurrido desde que la raíz envió el mensaje de configuración en el cual se basa el mensaje de configuración actual.

El campo Antigüedad máxima indica el momento en que el mensaje de configuración actual debe ser eliminado. Una vez que la antigüedad del mensaje alcanza la antigüedad máxima, el switch elimina la configuración actual e inicia una nueva elección para determinar un puente raíz nuevo, ya que asume que ha sido desconectado del mismo. Este valor está predeterminado en 20 segundos, pero puede ajustarse a intervalos entre 6 y 40 segundos.

El campo Tiempo de saludo indica el tiempo entre los mensajes de configuración del puente raíz. El intervalo define la cantidad de tiempo que el puente raíz espera para enviar BPDU de mensajes de configuración. Este valor está predeterminado en 2 segundos pero puede ajustarse a intervalos entre 1 y 10 segundos.

El campo Retraso en el envío indica la cantidad de tiempo que los puentes deben esperar antes de sufrir la transición a un nuevo estado luego de un cambio en la topología. Si la transición de un puente es muy repentina, es posible que no todos los enlaces de la red estén preparados para cambiar sus estados, lo que puede generar bucles. Este valor es igual a 15 segundos de manera predeterminada para cada estado pero puede ajustarse a intervalos entre 4 y 30 segundos.



El proceso BPDU

Inicialmente, cada switch del dominio de broadcast supone que es el puente raíz para la instancia de spanning-tree, de manera que las tramas de BPDU enviadas contienen el BID del switch local como ID de raíz. De manera predeterminada, las tramas de BPDU se envían cada 2 segundos después de iniciar el switch; esto significa que el valor predeterminado del temporizador de saludo especificado en la trama de BPDU es 2 segundos. Cada switch mantiene información local acerca de su propio BID, el ID de raíz y el costo de la ruta hacia la raíz.

Cuando los switches adyacentes reciben una trama de BPDU, comparan el ID de raíz de la trama de BPDU con el ID de raíz local. Si el ID de raíz del BPDU es menor que el ID de raíz local, el switch actualiza el ID de raíz local y el ID de sus mensajes de BPDU. Estos mensajes sirven para indicar el nuevo puente raíz de la red. Además, el costo de la ruta se actualiza para indicar cuán lejano se encuentra el puente raíz. Por ejemplo: si el BPDU se recibió en un puerto de switch Fast Ethernet, el costo de la ruta se establece en 19. Si el ID de raíz local es menor que el ID de raíz recibido en la trama de BPDU, la misma se descarta.

Después de que se ha actualizado un ID de ruta para identificar un nuevo puente raíz, todas las tramas de BPDU subsiguientes enviadas por ese switch contienen el ID de raíz nuevo y el costo de la ruta actualizado. De esta manera, todos los otros switches adyacentes pueden ver el menor ID de raíz identificado en todo momento. A medida que las tramas de BPDU se transmiten entre otros switches adyacentes, el costo de la ruta se actualiza de forma constante para indicar el costo de ruta total hacia el puente raíz. Todos los switches del spanning tree utilizan sus costos de ruta para identificar el mejor camino posible al puente raíz.

Haga clic en cada uno de los pasos de la figura para aprender más acerca del proceso BPDU.

A continuación se resume el proceso BPDU:

Paso 1. Inicialmente, cada switch se identifica a sí mismo como puente raíz. El switch S1 es el de menor prioridad de los tres switches. Debido a que la prioridad es un factor de decisión inicial a la hora de elegir un puente raíz, S1 se convierte en el puente raíz. Si la prioridad de todos los switches fuera la misma, la dirección MAC sería el factor de decisión.

Paso 2. Cuando el switch S3 recibe una BPDU del switch S2, S3 compara su ID de raíz con la trama de BPDU recibida. Las prioridades son iguales, de manera que el switch debe examinar la parte de dirección MAC para determinar cuál es la de menor valor. Ya que S2 cuenta con un valor de dirección MAC menor, S3 actualiza su ID de raíz con el ID de raíz de S2. En este momento, S3 considera a S2 como el puente raíz.

Paso 3. Cuando S1 compara su ID de raíz con el que se recibió en la trama de BPDU, identifica al ID de raíz local como el de menor valor y descarta la BPDU de S2.

Paso 4. Cuando S3 envía sus tramas de BPDU, el ID de raíz contenido en la trama de BPDU es el de S2.

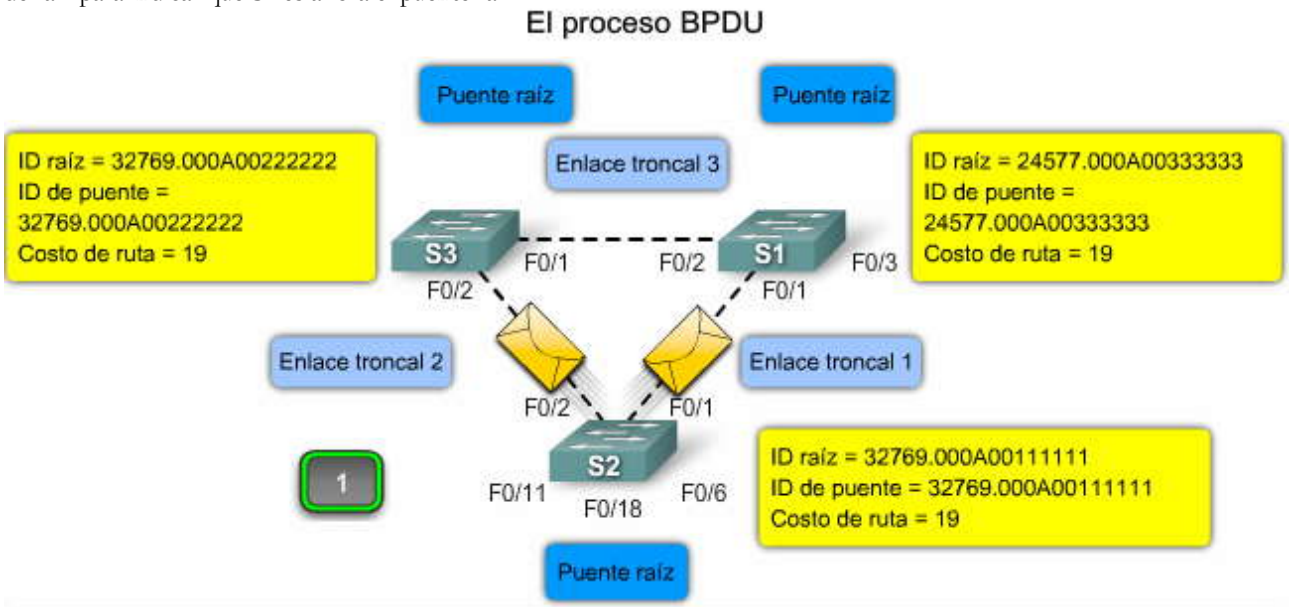
Paso 5. Cuando S2 recibe la trama de BPDU, la descarta después de verificar que el ID de raíz de la BPDU coincide con su ID de raíz local.

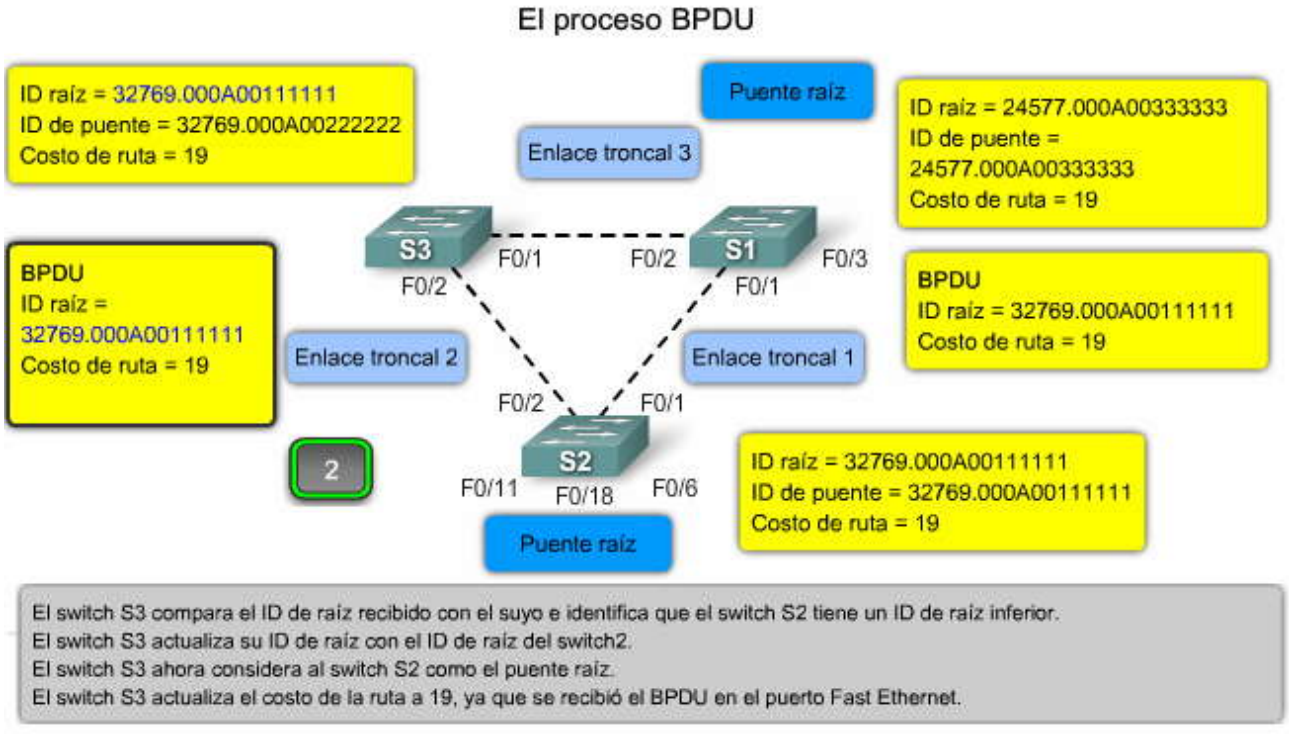
Paso 6. Debido a que S1 posee un valor de prioridad menor en su ID de raíz, descarta la trama de BPDU recibida de S3.

Paso 7. S1 envía sus tramas de BPDU.

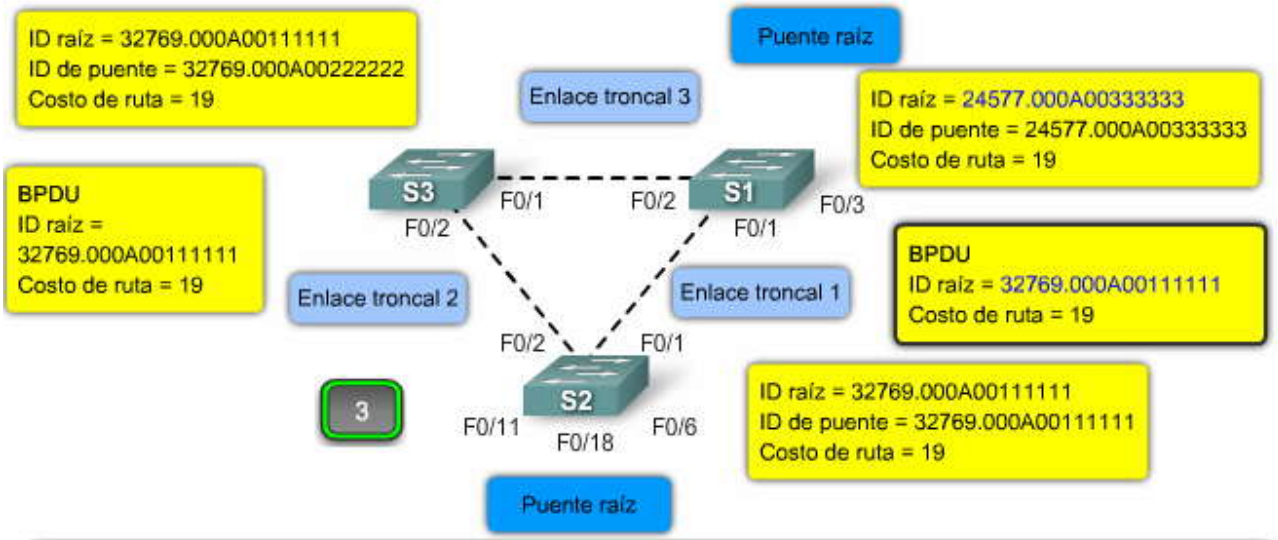
Paso 8. S3 identifica el ID de raíz en la trama de BPDU como el de menor valor y, por lo tanto, actualiza sus valores de ID de raíz para indicar que S1 es ahora el puente raíz.

Paso 9. S2 identifica el ID de raíz en la trama de BPDU como el de menor valor y, por lo tanto, actualiza sus valores de ID de raíz para indicar que S1 es ahora el puente raíz.



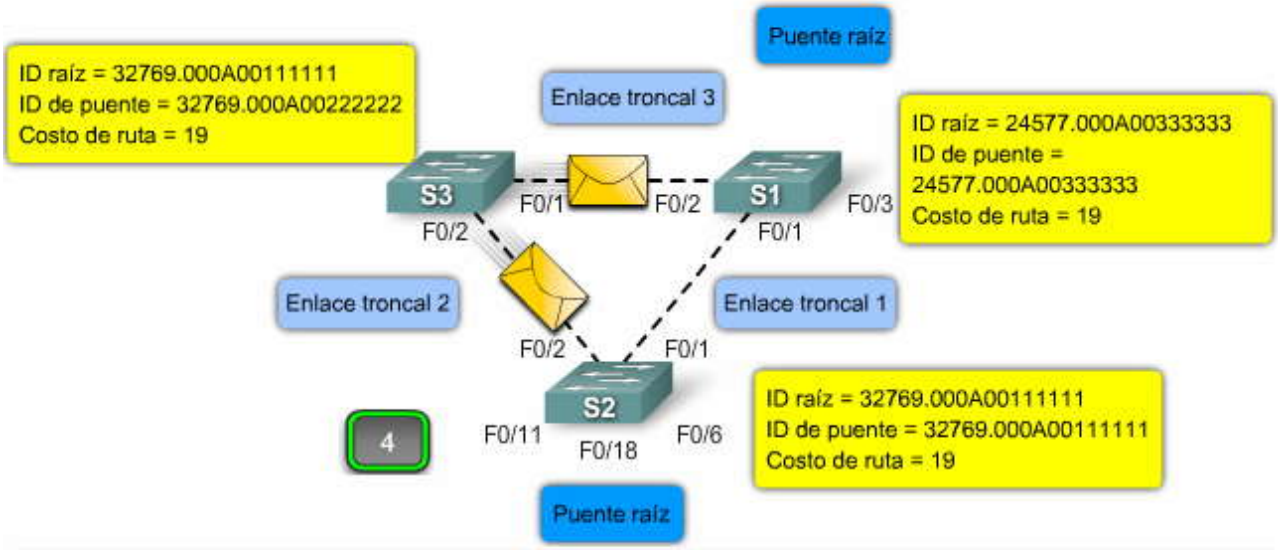


El proceso BPDU



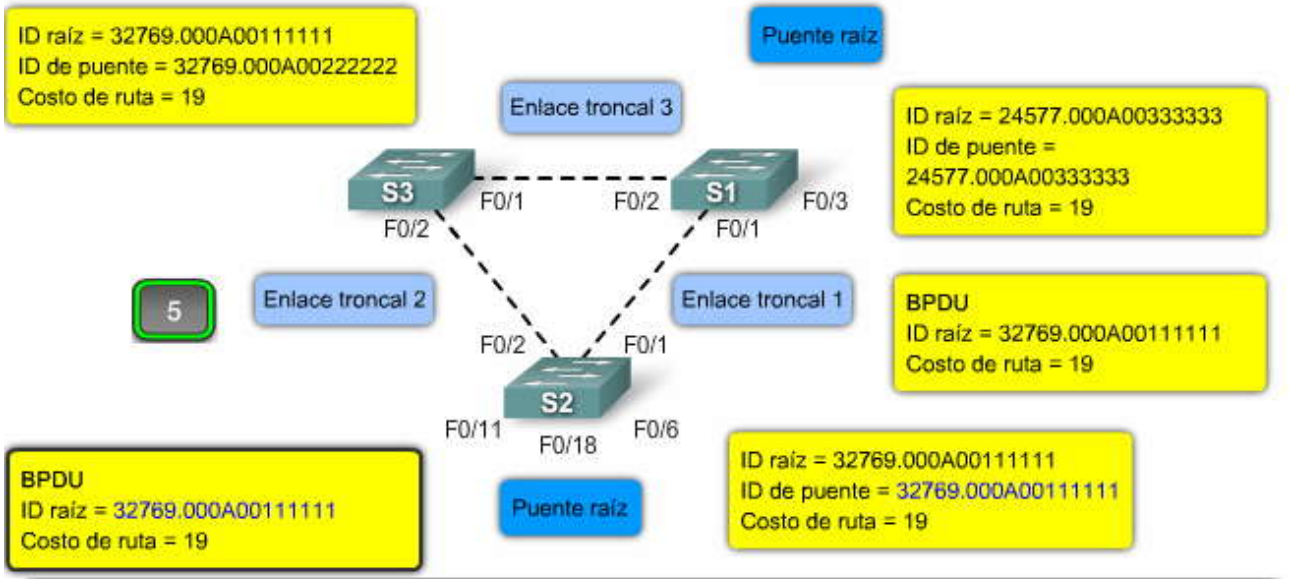
Cuando S1 compara su ID de raíz con la que recibió en la trama BPDU de S2, identifica al ID de raíz local como el valor inferior y descarta la BPDU de S2. El switch S1 todavía se considera a sí mismo el puente raíz.

El proceso BPDU



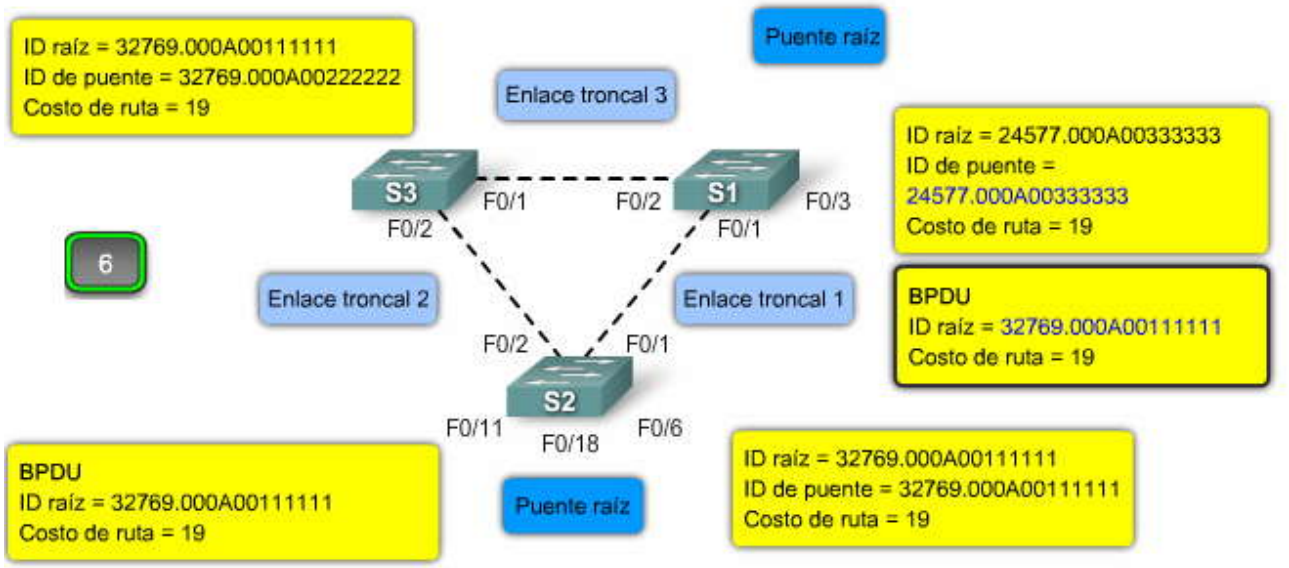
El switch S3 reenvía tramas BPDU a través de todos los puertos del switch. La trama BPDU contiene el ID de raíz del switch S2, lo que indica que es el puente raíz

El proceso BPDU



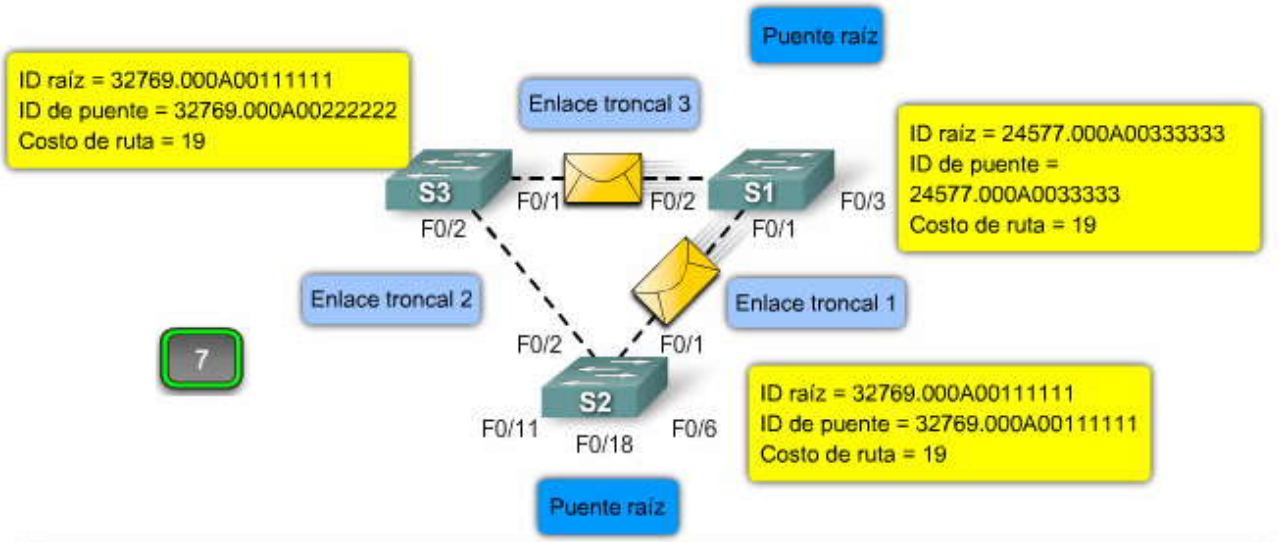
El switch S2 compara el ID de raíz BPDU recibido con el suyo e identifica que coinciden. El switch S2 continúa pensando que es el puente raíz en la red. El switch S2 no actualiza el costo de la ruta.

El proceso BPDU



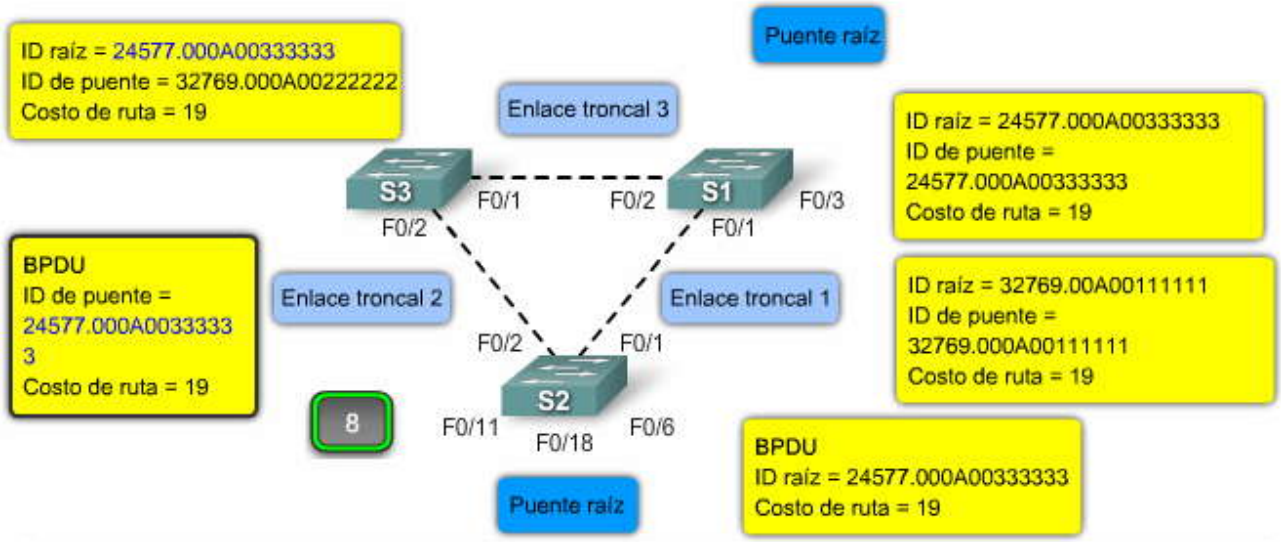
El switch S1 compara el ID de raíz BPDU recibido con el suyo e identifica que el propio es inferior. El switch S1 continúa pensando que es el puente raíz en la red. El switch S1 no actualiza el costo de la ruta.

El proceso BPDU

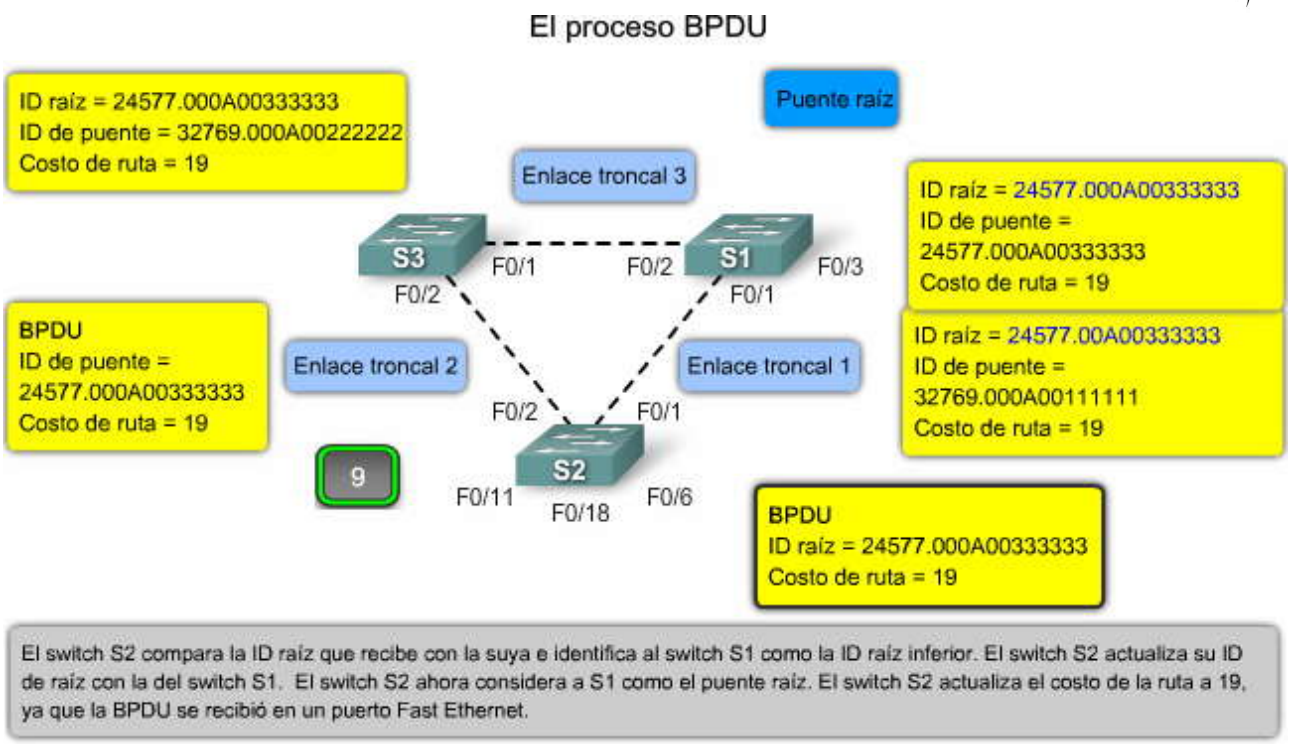


El switch S1 reenvía tramas BPDU a través de todos los puertos del switch. La trama BPDU contiene el ID del puente y el ID de raíz del switch S1, lo que indica que es el puente raíz.

El proceso BPDU



El switch S3 compara la ID raíz que recibe con la suya e identifica al switch S1 como la ID raíz inferior. El switch S3 actualiza su ID de raíz con la del switch S1. El switch S3 ahora considera a S1 como el puente raíz. El switch S3 actualiza el costo de la ruta a 19, ya que la BPDU se recibió en un puerto Fast Ethernet.



5.2.3 ID DE PUENTE.-

Campos BID

El ID de puente (BID) se utiliza para determinar el puente raíz de una red. Este tema describe cómo se compone un BID y cómo configurarlo en un switch para ejercer influencia en el proceso de elección y asegurar que se les asigne la función de puente raíz a switches específicos.

El campo BID de una trama de BPDU contiene tres campos separados: prioridad de puente, ID de sistema extendido y dirección MAC. Cada campo se utiliza durante la elección del puente raíz.

Prioridad del puente

La prioridad del puente es un valor que puede personalizarse y puede utilizarse para ejercer influencia sobre el switch que debe convertirse en el puente raíz. El switch con la menor prioridad, es decir, el menor BID, se transforma en el puente raíz (a medida que desciende el valor de prioridad, aumenta la misma). Por ejemplo: para asegurar que un switch específico sea siempre un puente raíz, se establece la prioridad a un valor menor que el del resto de los switches de la red. El valor predeterminado de la prioridad para todos los switches de Cisco es 32 768. El rango de prioridad oscila entre 1 y 65 536; por lo tanto, 1 es la prioridad más alta.

ID de sistema extendido

Como se muestra en el ejemplo, el ID de sistema extendido puede omitirse en las tramas de BPDU para algunas configuraciones. Las primeras implementaciones de STP se diseñaron para redes que no utilizaban VLAN. Existía un único spanning tree común para todos los switches. Cuando las VLAN comenzaron a ser comunes en la segmentación de la infraestructura de red, STP se mejoró para incluir el soporte para VLAN. En consecuencia, el campo ID de sistema extendido contiene el ID de la VLAN con la cual está asociada la BPDU.

Cuando se utiliza el ID de sistema extendido, se cambia la cantidad de bits disponibles para el valor de prioridad del puente, de forma que el incremento para dicho valor cambia de 1 a 4096. Por lo tanto, los valores de prioridad de puente sólo pueden ser múltiplos de 4096.

El valor de ID de sistema extendido se agrega al valor de prioridad de puente en el BID para identificar la prioridad y la VLAN de la trama de BPDU.

Aprenderá más acerca de spanning tree por VLAN (PVST) en una sección posterior de este capítulo.

Dirección MAC

Cuando dos switches se configuran con la misma prioridad y poseen el mismo ID de sistema extendido, el switch con la dirección MAC con el menor valor hexadecimal es el de menor BID. Inicialmente, todos los switches se configuran con el mismo valor de prioridad predeterminado. Luego, la dirección MAC es el factor de decisión sobre el cual el switch se convertirá en puente raíz. Esto resulta en una elección impredecible para el puente raíz. Se recomienda configurar el switch de puente raíz deseado con la menor prioridad para asegurar que sea elegido como tal. Esto también asegura que el agregado de switches a la red no provoque una nueva elección de spanning-tree, lo que podría interrumpir la comunicación en la red mientras se elige un nuevo puente raíz.

Haga clic en el botón Decisión basada en la prioridad que se muestra en la figura.

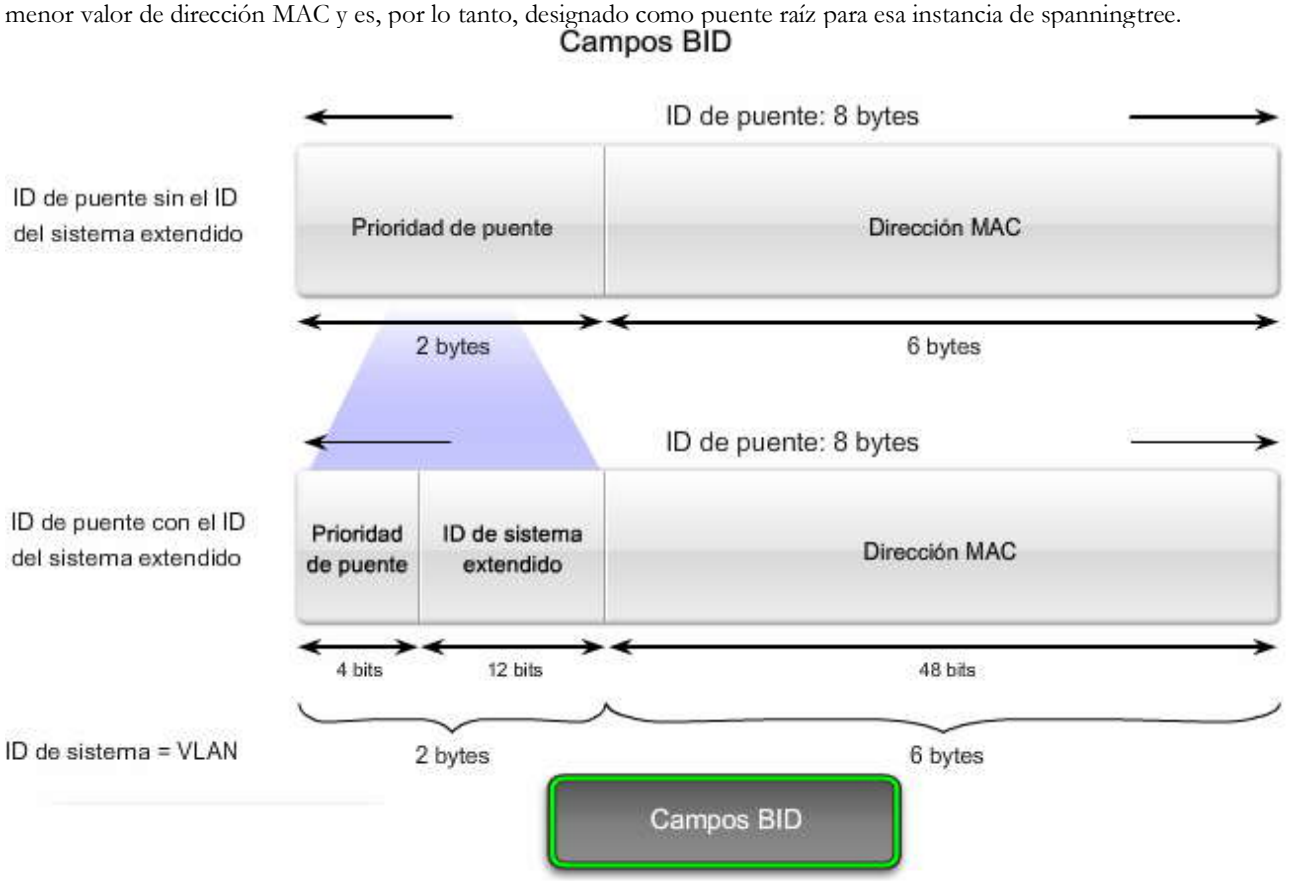
En el ejemplo, S1 posee menor prioridad que los otros switches y, por lo tanto, es el preferido como puente raíz para esa instancia de spanning-tree.

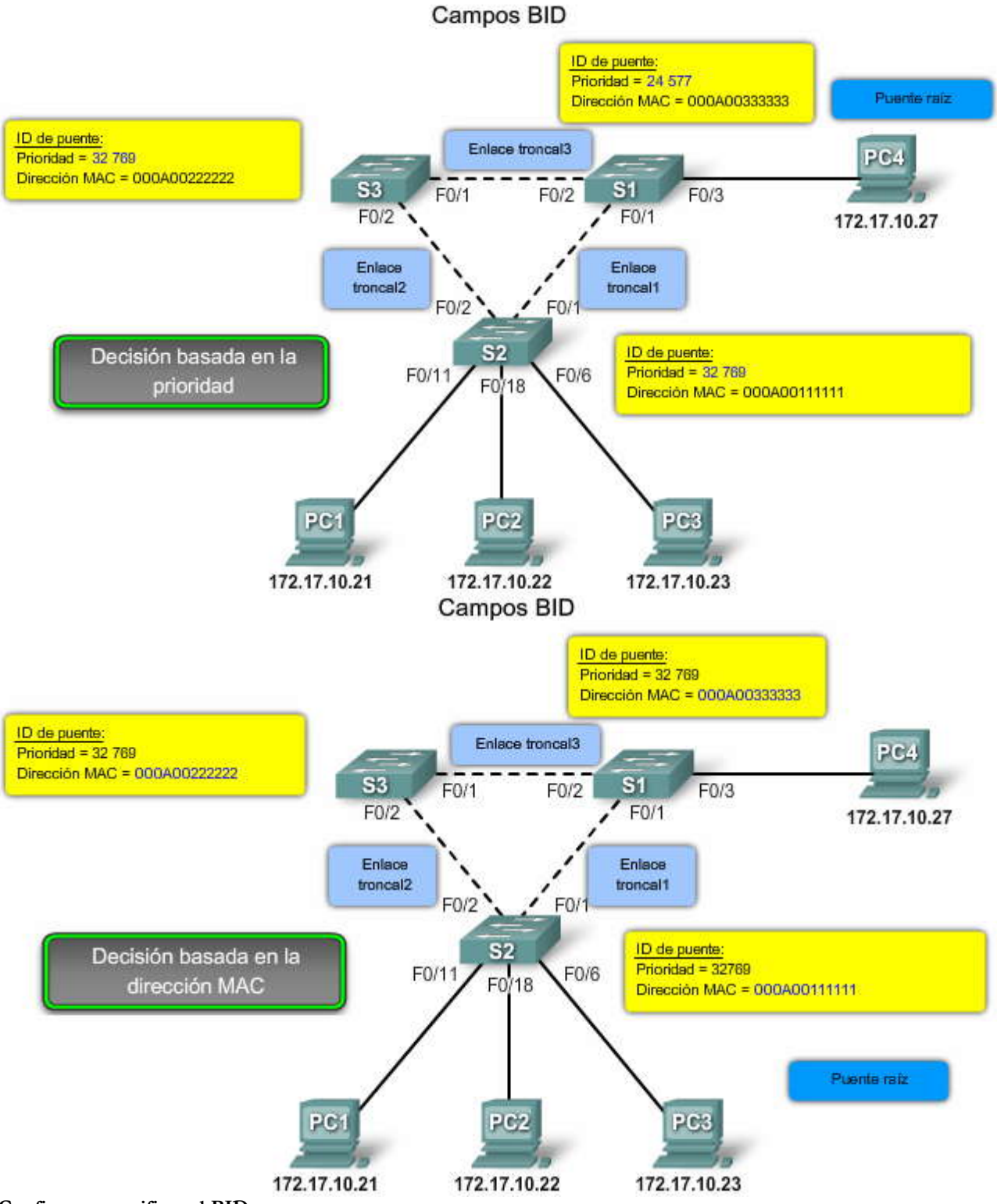
Haga clic en el botón Decisión basada en la dirección MAC que se muestra en la figura.

Cuando todos los switches se configuran con la misma prioridad, como ocurre en el caso de todos los switches mantenidos en la configuración predeterminada con prioridad de 32 768, la dirección MAC se transforma en el factor de decisión para determinar el switch que será puente raíz.

Nota: En el ejemplo, la prioridad de todos los switches es 32 769. El valor se basa en la prioridad predeterminada de 32 768 y la asignación de la VLAN 1 asociada con cada switch (1+32 768).

La dirección MAC con el menor valor hexadecimal se considera como preferida para puente raíz. En el ejemplo, S2 posee el menor valor de dirección MAC y es, por lo tanto, designado como puente raíz para esa instancia de spanning-tree.





Configurar y verificar el BID

Cuando un switch específico se transforma en puente raíz, el valor de prioridad de puente debe ajustarse para asegurar que sea menor que los valores de prioridad de puente de todos los otros switches de la red. Existen dos métodos de configuración distintos que pueden utilizarse para configurar el valor de prioridad de puente en un switch Cisco Catalyst.

Método 1: para asegurar que el switch posea el menor valor de prioridad de puente, utilice el comando **spanning-tree vlan vlan-id root primary** en modo de configuración global. La prioridad del switch se establece en el valor predefinido 24 576 o en el siguiente valor de incremento de 4096 por debajo de la menor prioridad de puente detectada en la red.

Si desea contar con un puente raíz alternativo, utilice el comando **spanning-tree vlan vlan-id root secondary** en modo de configuración global. Este comando establece la prioridad para el switch al valor preferido 28 672. Esto asegura que este

switch se convierta en el puente raíz si el puente raíz principal falla y se produce una nueva elección de puente raíz y se supone que el resto de los switches de la red tienen establecido el valor de prioridad predeterminado 32 768 definido.

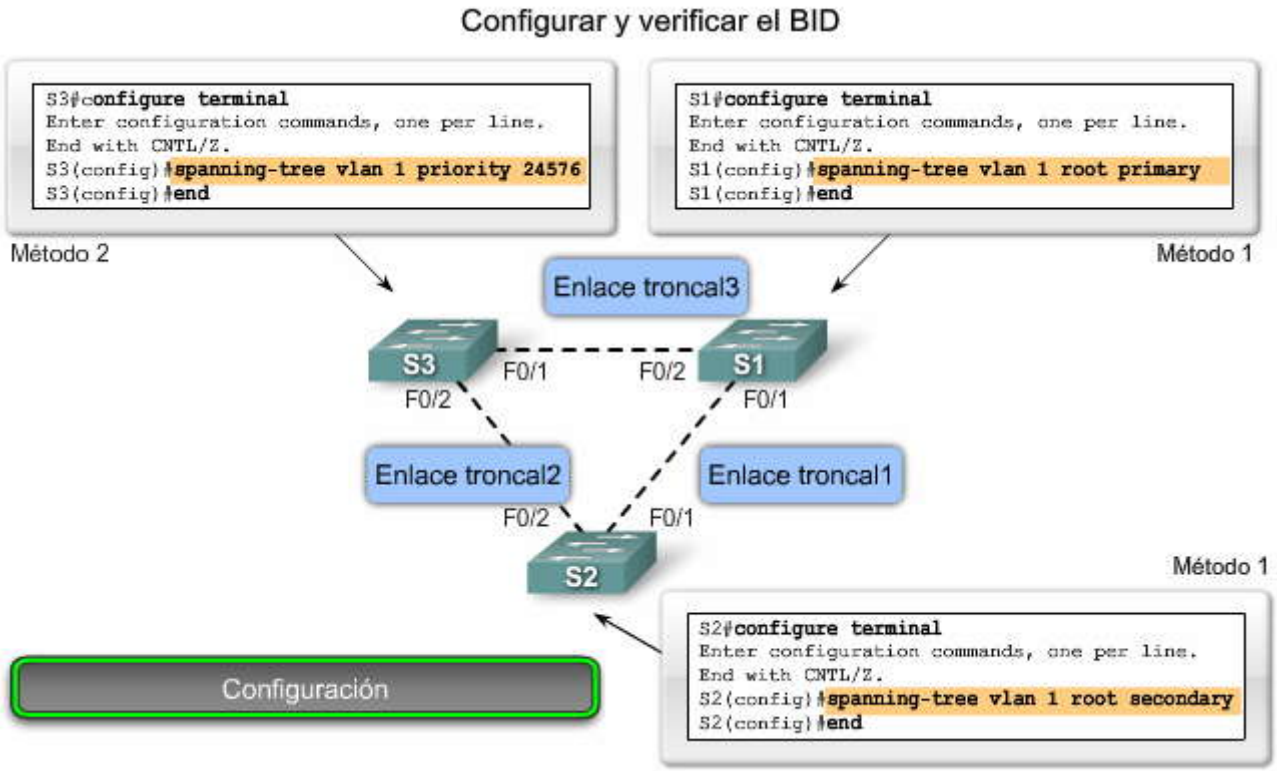
En el ejemplo, el switch S1 ha sido asignado como puente raíz principal a través del comando del modo deconfiguración global **spanning-tree vlan 1 root primary** y el switch S2 se ha configurado como puente raíz secundario mediante el comando del modo de configuración global **spanning-tree vlan 1 root secondary**.

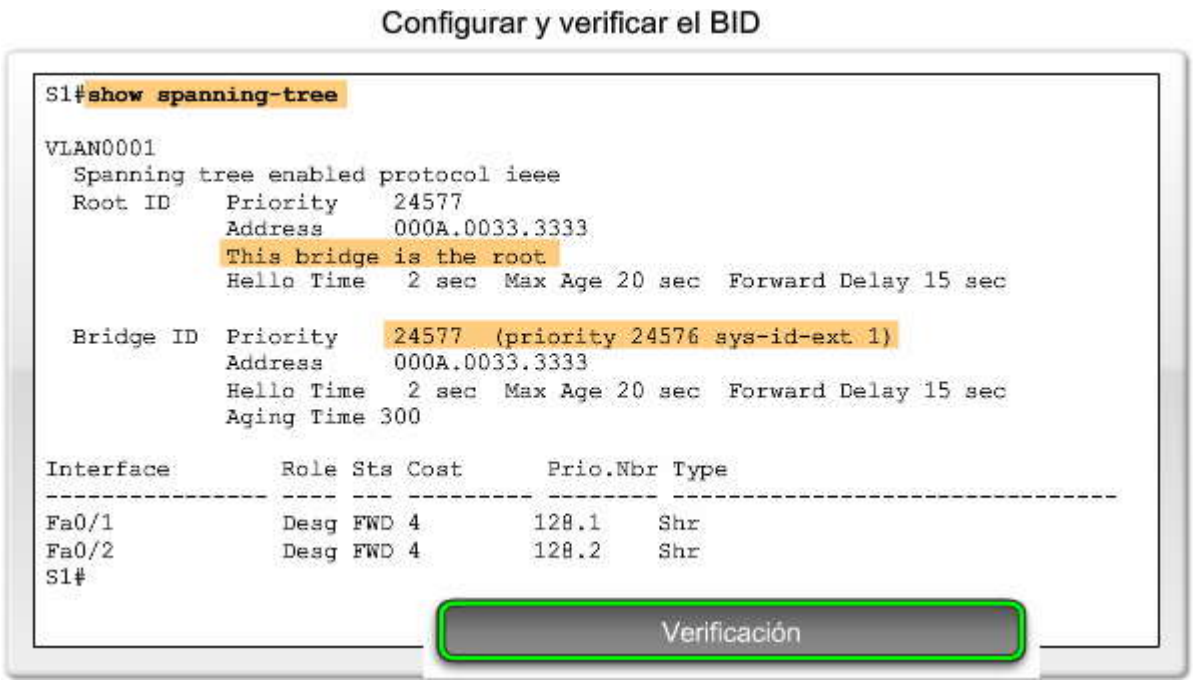
Método 2: otro método para configurar el valor de prioridad de puente es mediante el comando **spanning-tree vlan vlan-id priority** valor en modo de configuración global. Este comando proporciona más control granular sobre el valor de prioridad de puente. El valor de prioridad se configura en incrementos de 4096 entre 0 y 65 536.

En el ejemplo, el switch S3 tiene asignado un valor de prioridad de puente de 24 576 mediante el comando del modo de configuración global **spanning-tree vlan 1 priority 24576**.

Haga clic en el botón Verificación que se muestra enla figura.

Para verificar la prioridad de puente de un switch, utilice el comando del modo EXEC privilegiado **show spanning-tree**. En el ejemplo, la prioridad del switch se establece en 24 576. Observe también que el switch se designa como puente raíz para la instancia de spanning-tree.





5.2.4 FUNCIONES DE LOS PUERTOS.-

Funciones de los puertos

El puente raíz es elegido para la instancia de spanning-tree. La ubicación del puente raíz en la topología de red determina la forma en que se calculan las funciones de los puertos. Este tema describe la forma en que los puertos de switch se configuran para funciones específicas para evitar la posibilidad de bucles en la red.

Existen cuatro funciones de puertos distintas en las que los puertos de switch se configuran durante el proceso de spanning-tree.

Puerto raíz

El puerto raíz existe en los puentes que no son raíz y es el puerto de switch con el mejor camino hacia el puente raíz. Los puertos raíz envían el tráfico a través del puente raíz. Las direcciones MAC de origen de las tramas recibidas en el puerto raíz pueden llenar por completo la tabla MAC. Sólo se permite un puerto raíz por puente.

En el ejemplo, el switch S1 es el puente raíz y los switches S2 y S3 poseen puertos raíz definidos en los enlaces troncales que los conectan con S1.

Puerto designado

El puerto designado existe en los puentes raíz y en los que no son raíz. Para los puentes raíz, todos los puertos de switch son designados. Para los puentes que no son raíz, un puerto designado es el switch que recibe y envía tramas a través del puente raíz según sea necesario. Sólo se permite un puerto designado por segmento. Si existen varios switches en el mismo segmento, un proceso de elección determina el switch designado y el puerto de switch correspondiente comienza a enviar tramas para ese segmento. Los puertos designados pueden llenar por completo la tabla MAC.

En el ejemplo, el switch S1 posee ambos conjuntos de puertos para sus dos enlaces troncales configurados como puertos designados. El switch S2 también cuenta con un puerto designado configurado en el enlace troncal que va hacia el switch S3.

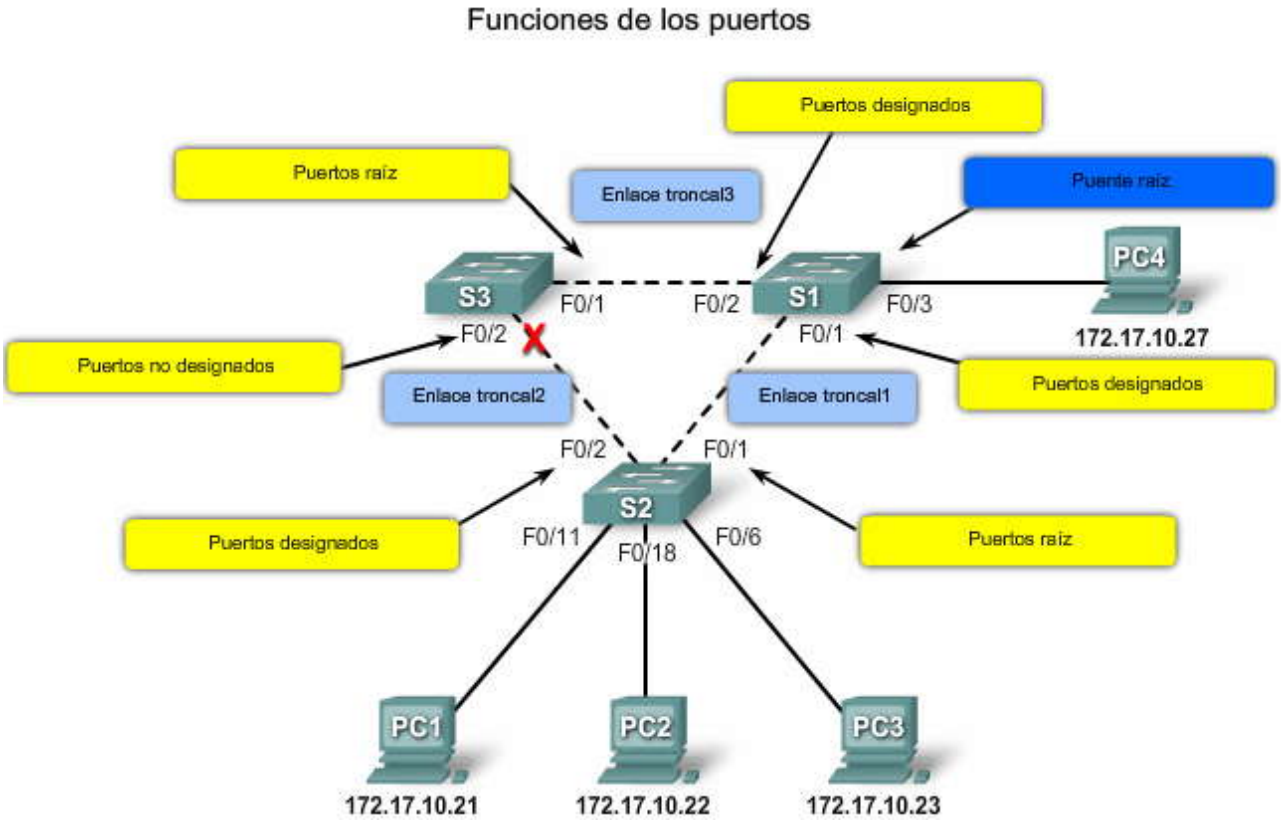
Puerto no designado

El puerto no designado es aquel puerto de switch que está bloqueado, de manera que no envía tramas de datos ni llena la tabla de direcciones MAC con direcciones de origen. Un puerto no designado no es un puerto raíz o un puerto designado. Para algunas variantes de STP, el puerto no designado se denomina puerto alternativo.

En el ejemplo, el switch S3 posee el único puerto no designado de la topología. Los puertos no designados evitan la generación de bucles.

Puerto deshabilitado

El puerto deshabilitado es un puerto de switch que está administrativamente desconectado. Un puerto deshabilitado no funciona en el proceso de spanning-tree. No hay puertos deshabilitados en el ejemplo.



Funciones de los puertos

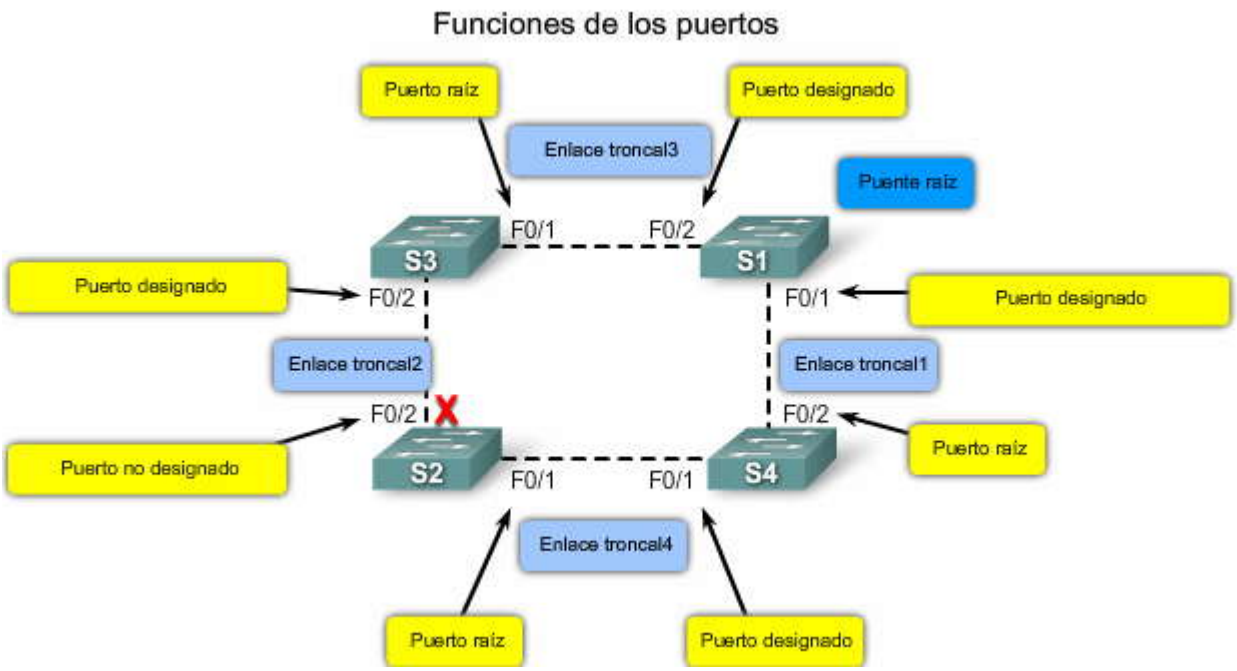
El STA determina la función de puerto que debe asignarse a cada puerto de switch.

Cuando se determina el puerto raíz de un switch, este último compara los costos de rutas de todos lospuertos de switch que participan en el spanning tree. Al puerto de switch con el menor costo de ruta total hacia la raíz se le asigna de manera automática la función de puerto raíz, ya que es el más cercano al puente raíz. En una topología de la red, todos los switches que utilizan spanning tree, excepto el puente raíz, poseen un único puerto raíz definido.

Cuando existen dos puertos de switch con el mismo costo de ruta hacia el puente raíz y ambos son los de menor costo de ruta en el switch, este último debe determinar cuál de los dos es el puerto raíz. El switch utiliza el valor de prioridad de puerto personalizable o el menor ID de puerto si ambos valores de prioridad de puerto coinciden.

El ID de puerto es el ID de interfaz del puerto de switch. Por ejemplo: la figura muestra cuatro switches. Los puertos F0/1 y F0/2 del switch S2 poseen el mismo valor de costo de ruta hacia el puente raíz. Sin embargo, el puerto F0/1 del switch S2 es el puerto preferido, ya que posee el menor valor de ID de puerto.

El ID de puerto está adjunto a la prioridad del puerto. Por ejemplo: el puerto de switch F0/1 posee un valor de prioridad de puerto predeterminado de 128.1, donde 128 es el valor de prioridad de puerto configurable y .1 es el ID de puerto. El puerto de switch F0/2 posee un valor de prioridad de puerto de 128.2 de manera predeterminada.

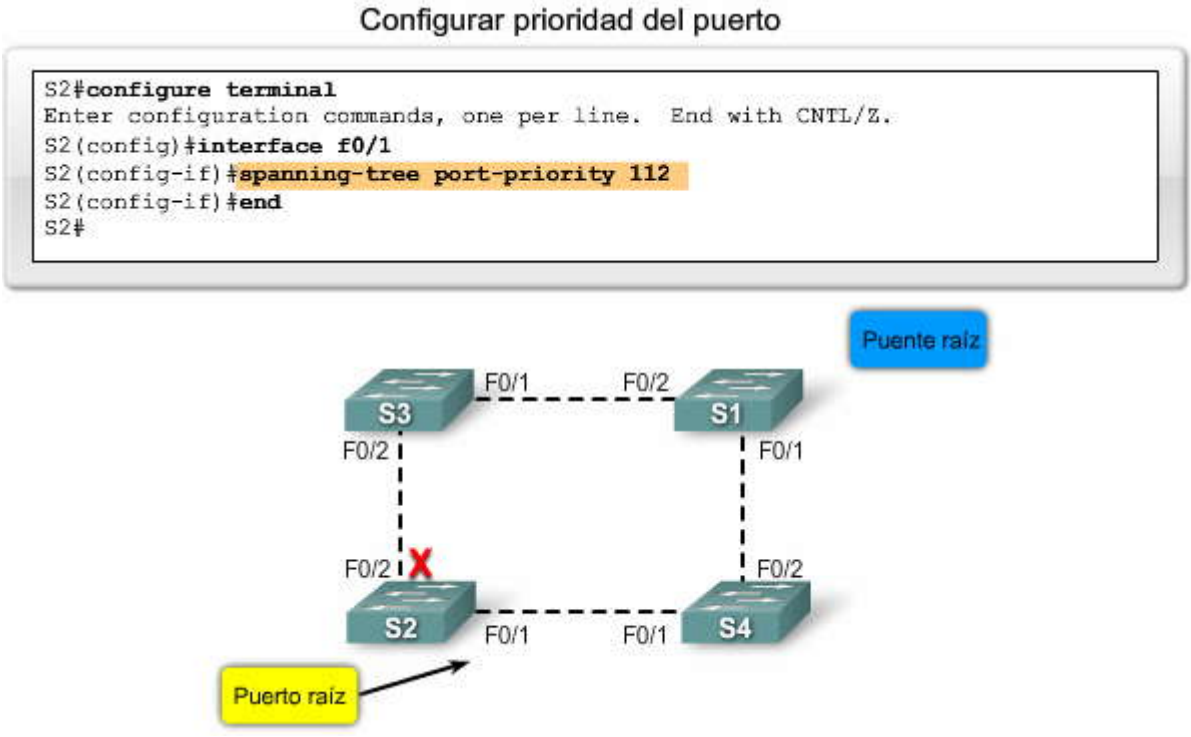


Configurar prioridad del puerto

Se puede configurar el valor de prioridad del puerto a través del comando **spanning-tree port-priority** valor en modo de configuración de interfaz. Los valores de prioridad de puerto oscilan entre 0 y 240, en incrementos de 16. El valor de prioridad de puerto predeterminado es 128. Al igual que con la prioridad de puente, los valores de prioridad de puerto menores proporcionan al puerto una mayor prioridad.

En el ejemplo, la prioridad de puerto para el puerto F0/1 se ha establecido en 112, que está por debajo de la prioridad de puerto predeterminada, que es 128. Esto asegura que el puerto sea el preferido cuando compita con otro puerto para una función de puerto específica.

Cuando el switch decide utilizar un puerto por sobre otro como puerto raíz, este último se configura como puerto no designado para evitar la generación de bucles.



Decisiones de las funciones de los puertos

En el ejemplo, el switch S1 es el puente raíz. Los switches S2 y S3 cuentan con puertos raíz configurados para los puertos que se conectan con S1.

Después de que el switch ha determinado cuál de sus puertos está configurado en la función de puerto raíz, debe decidirqué puertos poseen las funciones de designados y no designados.

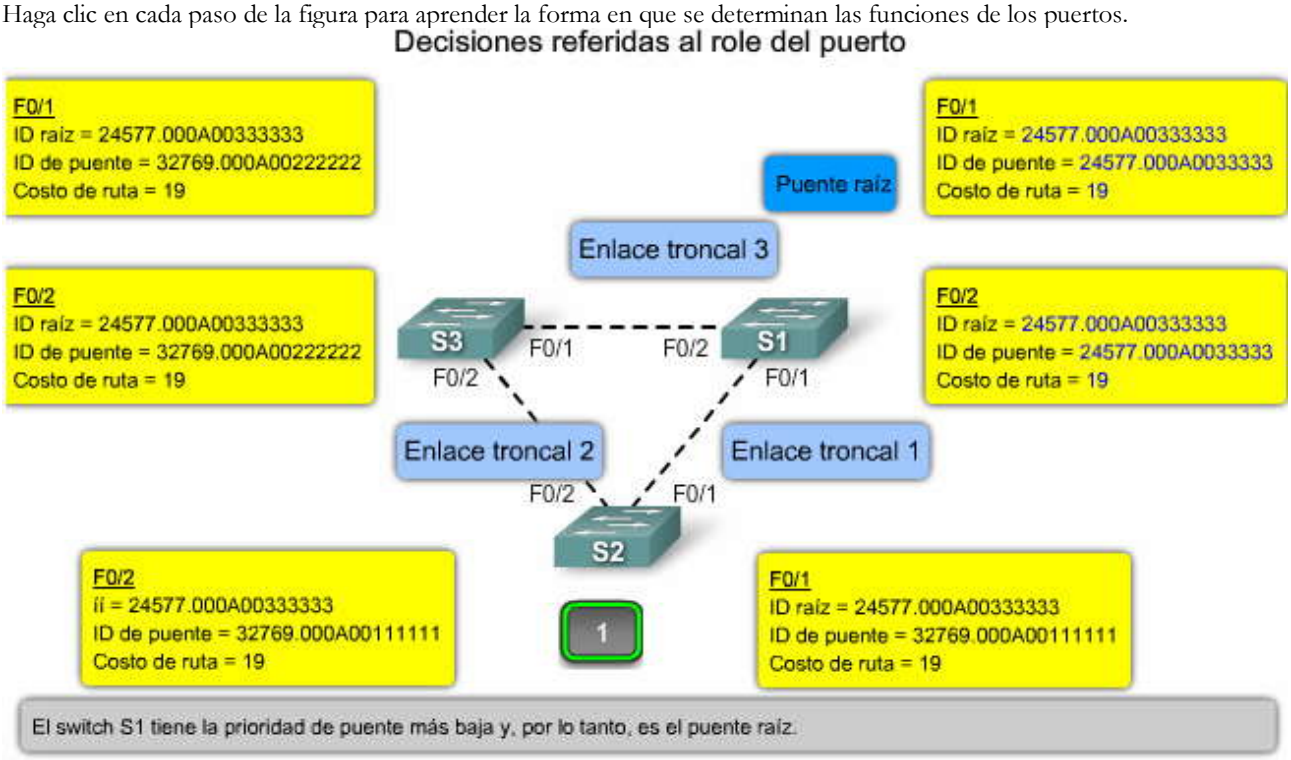
El puente raíz configura de forma automática todos sus puertos de switch en la función de designado. Otros switches de la topología configuran sus puertos que no son raíz como designados o nodesignados.

Los puertos designados se configuran para todos los segmentos de LAN. Cuando dos switches están conectados al mismo segmento de LAN y los puertos raíz ya se han definido, los dos switches deben decidir el puerto que debe configurarse como designado y el que debe permanecer como no designado.

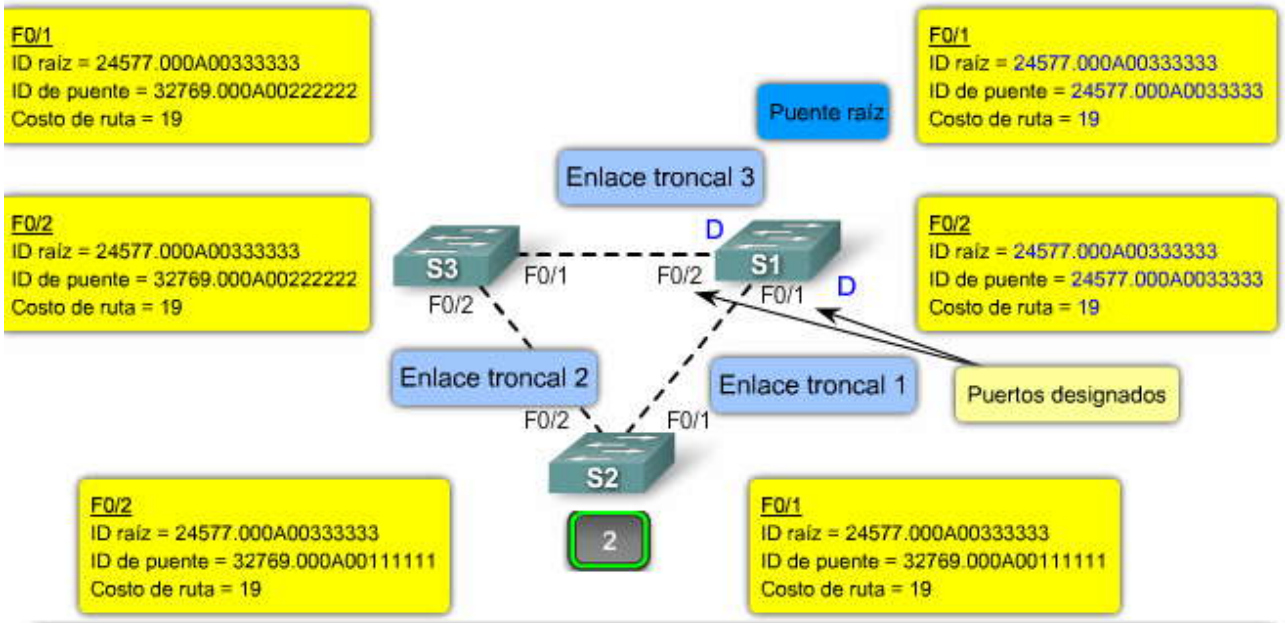
Los switches del segmento de LAN en cuestión intercambian tramas de BPDU, que contienen el BID del switch. En general, el switch con el menor BID posee su puerto configurado como designado, mientras que d switch con el mayor BID posee su puerto configurado como no designado. Sin embargo, tenga en cuenta que la primera prioridad es el menor costo de ruta hacia el puente raíz y que el BID del emisor sólo lo es cuando los costos de los puertos son iguales.

En consecuencia, cada switch determina las funciones de puertos que se asignan a cada uno de sus puertos para crear el spanning tree sin bucles.

Haga clic en cada paso de la figura para aprender la forma en que se determinan las funciones de los puertos.

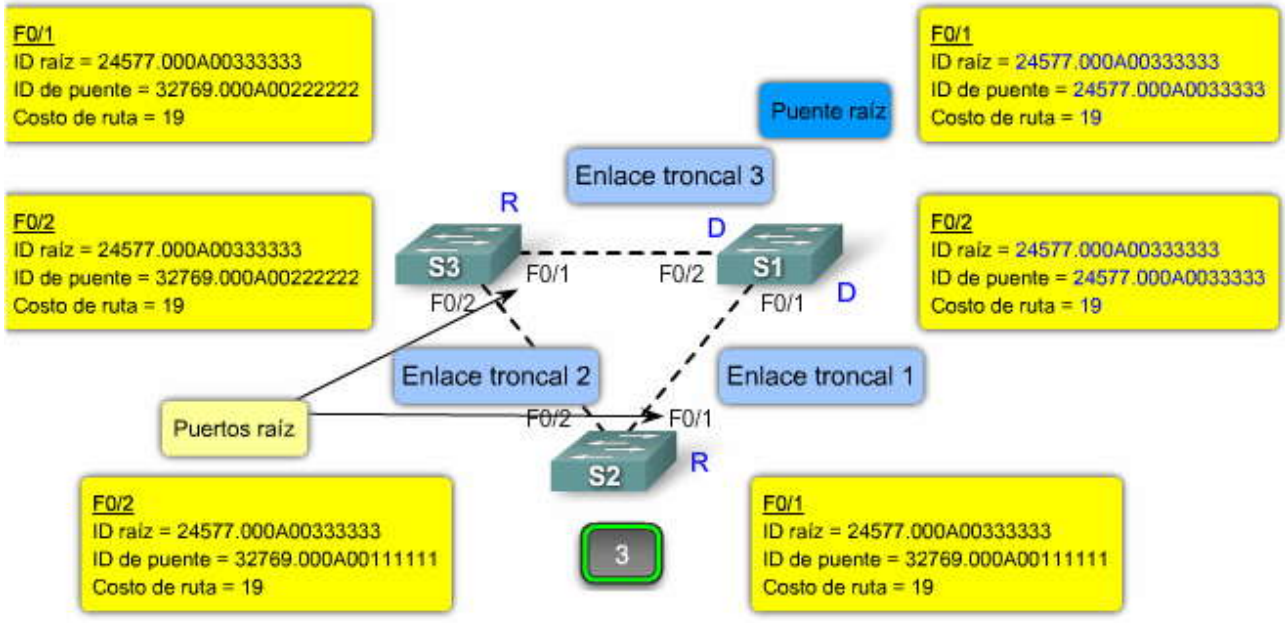


Decisiones referidas al role del puerto



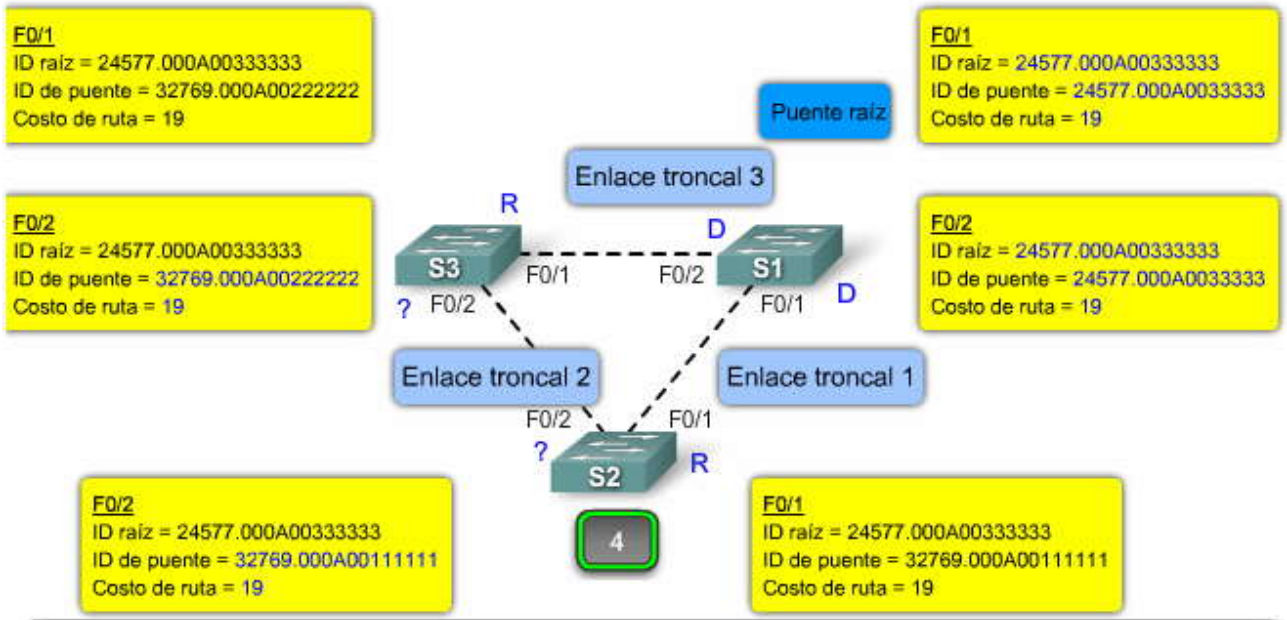
El switch S1 configura sus dos puertos de enlace troncal como puertos designados.

Decisiones referidas al role del puerto



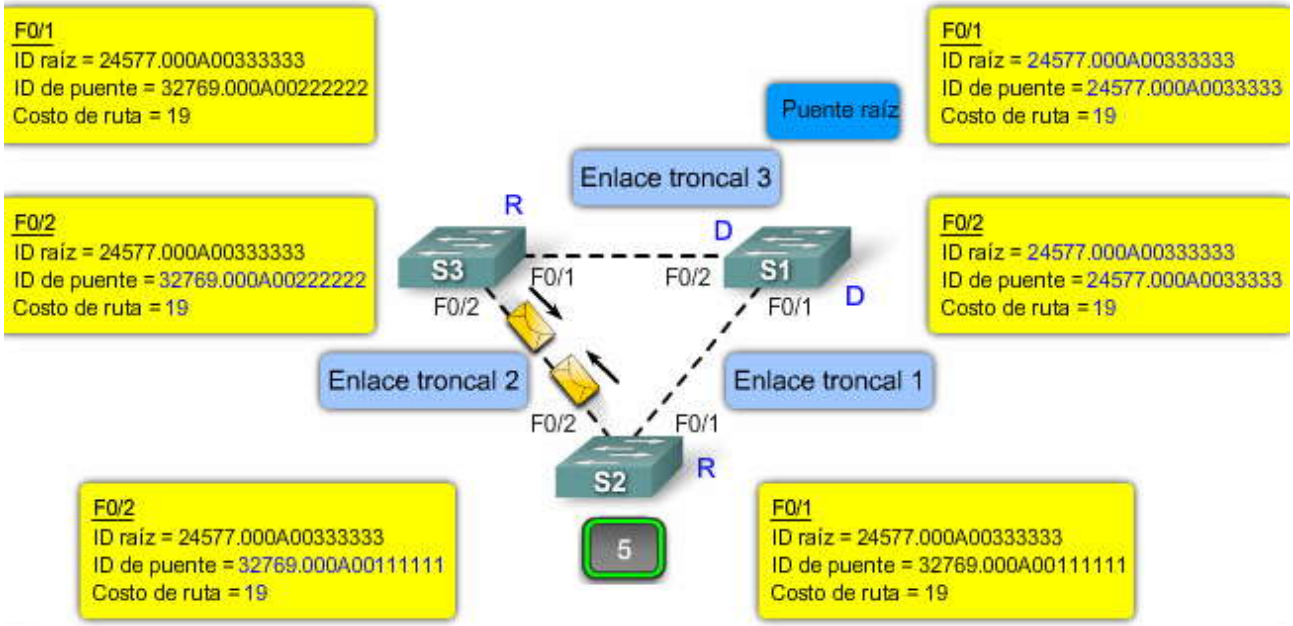
El switch S2 configura el puerto F0/1 como puerto raíz.
El switch S3 configura el puerto F0/1 como puerto raíz.

Decisiones referidas al role del puerto

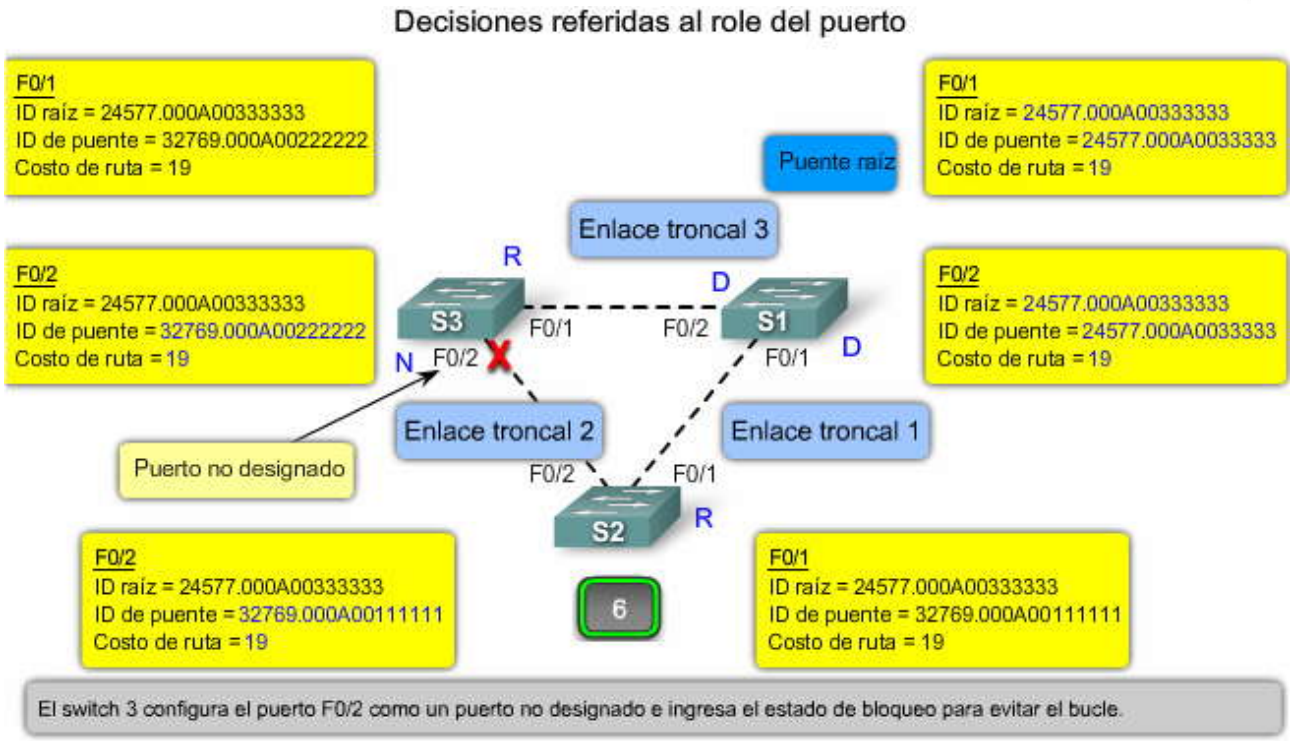


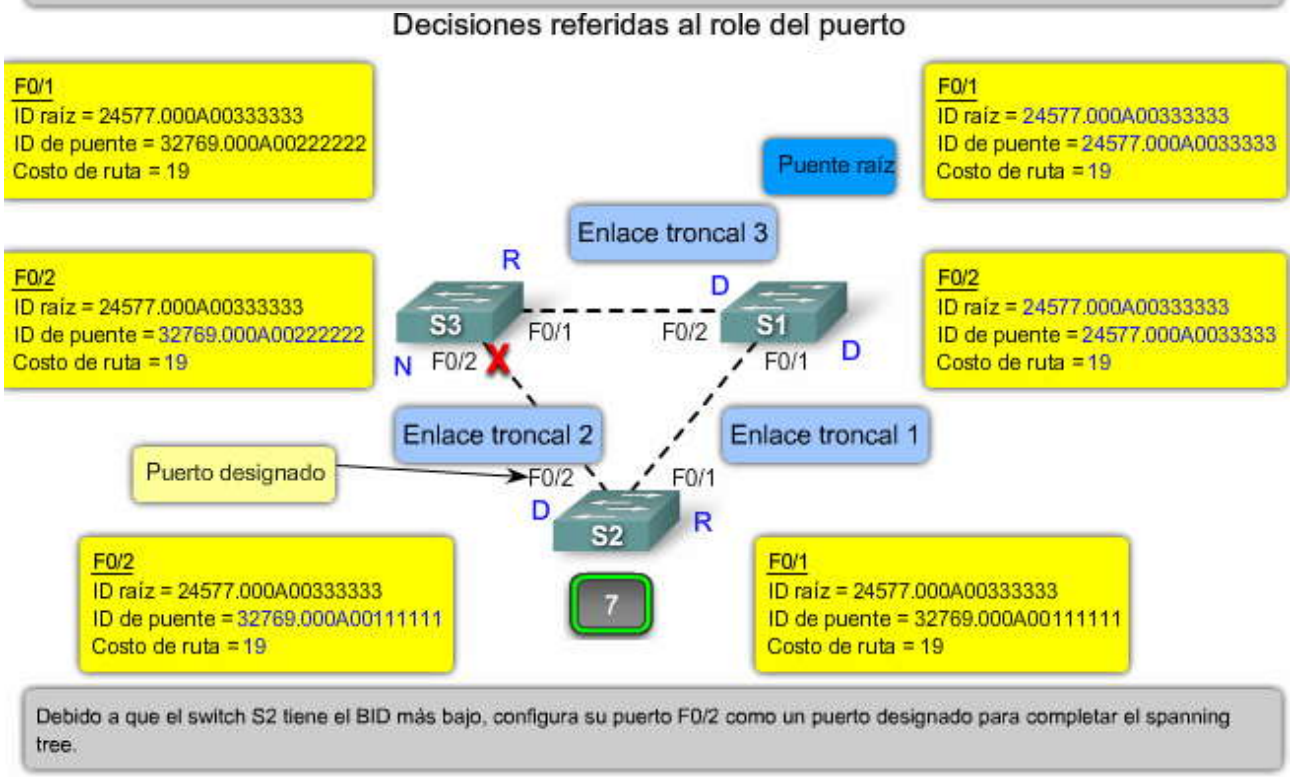
El switch S2 y el switch S3 comparten un segmento de LAN común. Necesitan determinar cuál de ellos tiene el BID más bajo para identificar qué switch puede configurar su puerto como un puerto designado.

Decisiones referidas al role del puerto



El switch S2 y el switch S3 intercambian tramas BPDU. El switch 3 identifica que el switch S2 tiene un BID inferior basado en la dirección MAC inferior del switch S2.





Verificación de las funciones y la prioridad de los puertos

Ahora que spanning tree ha determinado la topología de la red lógica sin bucles, se deben confirmar las funciones y prioridades de los puertos que deben configurarse para todos los puertos de switch de la red.

Para verificar las funciones y las prioridades de los puertos para los puertos de switch, utilice el comando show spanning-tree en modo EXEC privilegiado.

En el ejemplo, el resultado de show spanning-tree muestra todos los puertos de switch y sus funciones definidas. Los puertos de switch F0/1 y F0/2 se configuran como puertos designados. El resultado también muestra la prioridad de puerto de cada puerto de switch. El puerto de switch F0/1 posee una prioridad de puerto de 128.1.

Verificación de las funciones y la prioridad de los puertos

```
S2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0019.aa9e.b000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0019.aa9e.b000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p

S2#
```

5.2.5 ESTADOS DE LOS PUERTOS Y TEMPORIZADORES DE BDPU EN STP.-

Estados de los puertos

STP determina la ruta lógica sin bucles a través de todo el dominio de broadcast. El spanning tree se determina a través de la información obtenida en el intercambio de tramas de BPDU entre los switches interconectados. Para facilitar el aprendizaje del spanning tree lógico, cada puerto de switch sufre una transición a través de cinco estados posibles y tres temporizadores de BPDU.

El spanning tree queda determinado inmediatamente después de que el switch finaliza el proceso de arranque. Si un puerto de switch experimenta una transición directa desde el estado de bloqueo al estado de enviar, dicho puerto puede crear temporalmente un bucle de datos si el switch no advierte toda la información de la topología en ese momento. Por esta razón, STP introduce cinco estados de puertos. La tabla resume cada uno de los estados de puertos. A continuación se proporciona información adicional acerca de la forma en que los estados delos puertos aseguran la ausencia de bucles durante la creación del spanning tree lógico.

Bloqueo: el puerto es un puerto no designado y no participa en el envío de tramas. El puerto recibe tramas de BPDU para determinar la ubicación y el ID de raíz del switch del puente raíz y las funciones de puertos que cada uno de los mismos debe asumir en la topología final de STP activa.
Escuchar: STP determina que el puerto puede participar en el envío de tramas de acuerdo a las tramas de BPDU que el switch ha recibido hasta ahora. En este momento, el puerto de switch no sólo recibe tramas de BPDU, sino que también transmite sus propias tramas de BPDU e informa a los switches adyacentes que el mismo se prepara para participar en la topología activa.
Aprender: el puerto se prepara para participar en el envío de tramas y comienza a llenar la tabla de direcciones MAC.
Enviar: el puerto se considera parte de la topología activa, envía tramas y envía y recibe tramas de BPDU.
Deshabilitado: el puerto de la Capa 2 no participa en el spanning tree y no envía tramas. El estado deshabilitado se establece cuando el puerto de switch se encuentra administrativamente deshabilitado.

Estados de los puertos

Procesos	Bloqueo	Escuchar	Aprender	Enviar	Deshabilitar
Recibe y procesa las BPDU	[1] SI	SI	SI	SI	NO
Enviar tramas de datos recibidas en la interfaz	NO	NO	NO	SI	NO
Enviar tramas de datos conmutadas de otra interfaz	NO	NO	NO	SI	NO
Aprender las direcciones MAC	NO	NO	SI	SI	NO

[1]Volver al bloqueo si no es la ruta de menor costo al puente raíz

Temporizadores de BPDU

La cantidad de tiempo que un puerto permanece en los distintos estados depende de los temporizadores de BPDU. Sólo el switch con función de puente raíz puede enviar información a través del árbol para ajustar los temporizadores. Los siguientes temporizadores determinan el rendimiento de STP y los cambios de estado:

Tiempo de saludo
Retraso en el envío
Antigüedad máxima

Haga clic en Funciones y temporizadores en la figura.

Cuando STP está habilitado, todos los puertos de switch de la red atraviesan el estado de bloqueo y los estados transitorios escuchar y aprender al iniciarse. Luego los puertos se estabilizan al estado de enviar o de bloqueo, como se ve en el ejemplo. Durante un cambio en la topología, el puerto implementa temporalmente los estados escuchar y aprender durante un período de tiempo específico denominado "intervalo de retraso de envío".

Estos valores permiten el tiempo adecuado para la convergencia en la red con un diámetro de switch de valor siete. Recuerde que el diámetro de switch es la cantidad de switches que debe atravesar una trama para viajar a través de los dos puntos más lejanos del dominio de broadcast. Un diámetro de switch de siete es el valor mayor permitido por STP debido a los tiempos de convergencia. La convergencia en relación a spanning tree es el tiempo que toma volver a calcular el spanning tree en el caso de una falla en un switch o en un enlace. Aprenderá la forma en que funciona la convergencia en la sección siguiente.

Haga clic en el botón Configurar diámetro de la red en la figura.

Se recomienda que los temporizadores BPDU no se ajusten de forma directa, ya que estos valores se han optimizado para el diámetro de switch de siete. Si se ajusta el valor del diámetro del spanning-tree en el puente raíz a un valor menor, automáticamente se ajustan los temporizadores de retraso de envío y la antigüedad máxima de forma proporcional según el nuevo diámetro. En general, no deben ajustarse los temporizadores BPDU ni reconfigurar el diámetro de la red. Sin embargo, si después de la búsqueda un administrador de red determina que el tiempo de convergencia de la red puede optimizarse, el mismo lo hace mediante la reconfiguración del diámetro de la red, pero no los temporizadores BPDU.

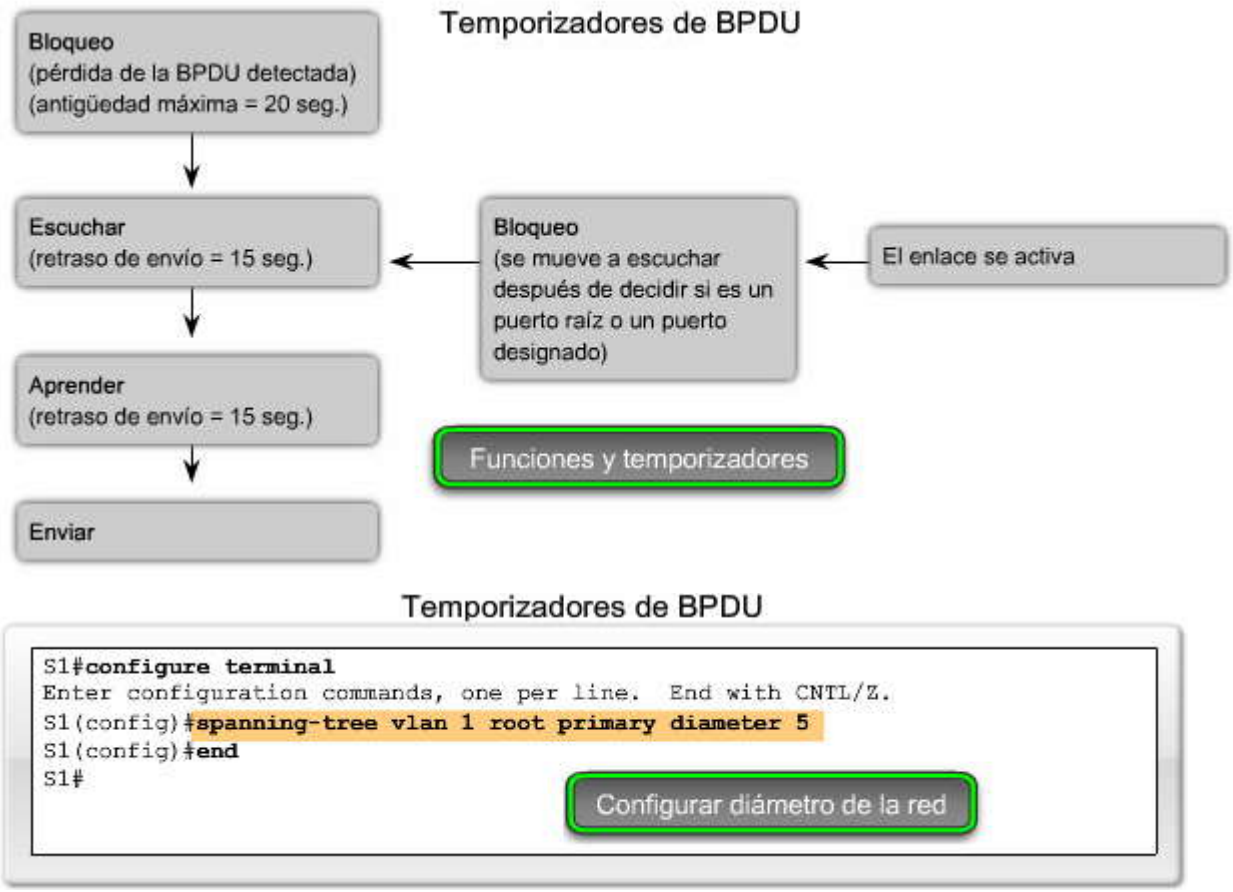
Para configurar un diámetro de red distinto en STP, utilice el comando spanning-tree vlan vlan id root primary diameter valor en modo de configuración global en el switch puente raíz.

En el ejemplo, el comando del modo de configuración global spanning-tree vlan 1 root primary diameter 5 se ingresó para ajustar el diámetro de spanning tree en cinco switches.

Temporizadores de BPDU

Tiempo de saludo	El tiempo de saludo es el tiempo que transcurre cada vez que una trama de BPDU es enviada a un puerto. Este valor está predeterminado en 2 segundos pero puede ajustarse al intervalo de 1 a 10 segundos.
Retraso de envío	El retraso de envío es el tiempo que transcurre en los estados de escuchar y aprender. Este valor es igual a 15 segundos de manera predeterminada para cada estado pero puede ajustarse al intervalo de 4 a 30 segundos.
Antigüedad máxima	El temporizador de antigüedad máxima controla la cantidad máxima de tiempo en que un puerto de switch guarda información de la configuración de la BPDU. Este valor está predeterminado en 20 segundos pero puede ajustarse al intervalo de 6 a 40 segundos.

Temporizadores de BPDU



Tecnología PortFast de Cisco

PortFast es una tecnología de Cisco. Cuando un switch de puerto configurado con PortFast se establece como puerto de acceso, sufre una transición del estado de bloqueo al de enviar de manera inmediata, saltando los pasos típicos de escuchar y aprender. Puede utilizarse PortFast en puertos de acceso, conectados a una única estación de trabajo o servidor, para permitir que dichos dispositivos se conecten a la red de manera inmediata sin esperar la convergencia del árbol de expansión. Si una interfaz configurada con PortFast recibe una trama de BPDU, spanning tree puede colocar el puerto en estado de bloqueo mediante una función denominada protección de BPDU. La configuración de protección de BPDU excede el alcance de este curso.

Nota: La tecnología PortFast de Cisco puede utilizarse para el soporte de DHCP. Sin PortFast, un equipo puede enviar una solicitud de DHCP antes de que el puerto se encuentre en estado de enviar e impedirle al host la posibilidad de obtener una dirección IP utilizable y cualquier otra información. Debido a que PortFast cambia el estado a enviar de manera inmediata, el equipo siempre obtiene una dirección IP utilizable.

Para obtener más información acerca de la configuración de la protección BPDU, consulte:

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a008009482f.shtml.

Nota: Debido a que el objetivo de PortFast es minimizar el tiempo que los puertos de acceso deben esperar para la convergencia de spanning tree, sólo debe utilizarse en puertos de acceso. Si se habilita PortFast en un puerto conectado a otro switch, se corre el riesgo de generar un bucle de spanning-tree.

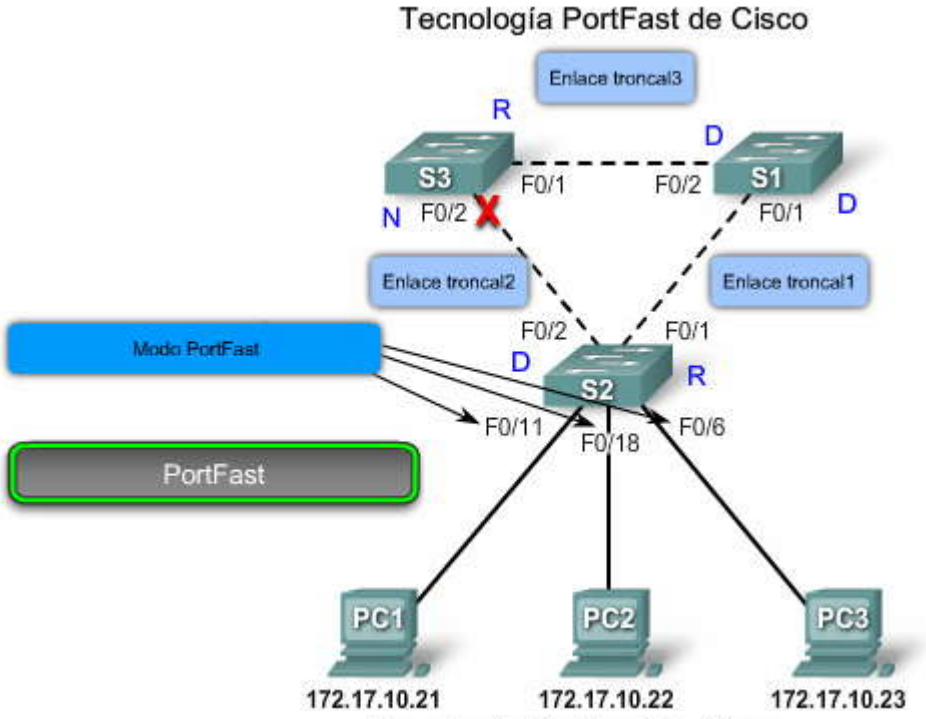
Haga clic en el botón Configurar PortFast que se muestra en la figura.

Para configurar PortFast en un puerto de switch, ingrese el comando spanning-tree portfast en modo de configuración de interfaz en todas las interfaces en las que se habilitará PortFast.

Para deshabilitar PortFast, ingrese el comando no spanning-tree portfast en modo de configuración de interfaz en todas las interfaces en las que se deshabilitará PortFast.

Haga clic en el botón Verificar PortFast que se muestra en la figura.

Para verificar que PortFast se ha habilitado para un puerto de switch, utilice el comando show running-config en modo EXEC privilegiado. La ausencia del comando spanning-tree portfast en la configuración en ejecución de una interfaz indica que PortFast se ha deshabilitado para la misma. PortFast está deshabilitado en todas las interfaces de manera predeterminada.



Tecnología PortFast de Cisco

Habilitar PortFast

```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
 Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

 Portfast has been configured on FastEthernet0/11 but will only
 have effect when the interface is in a non-trunking mode.
S2(config-if)# end
```

Deshabilitar PortFast

Configurar PortFast

```
S2(config)# interface FastEthernet 0/11
S2(config-if)# no spanning-tree portfast
S2(config-if)# end
```

Tecnología PortFast de Cisco

```
S2#show running-config
<output omitted>
!
interface FastEthernet0/11
 switchport mode access
 spanning-tree portfast
!
<output omitted>
end
S2#
```

Verificar PortFast

5.3 CONVERGENCIA DE STP.-

5.3.1 CONVERGENCIA DE STP.-

Pasos de convergencia de STP

La sección anterior describía los componentes que permiten a STP crear la topología de la red lógica sin bucles. En esta sección se examinará el proceso de STP completo, desde el principio hasta el final.

La convergencia es un aspecto importante del proceso de spanning-tree. La convergencia es el tiempo que le toma a la red determinar el switch que asumirá la función del puente raíz, atravesar todos los otros estados de puerto y configurar todos los puertos de switch en sus funciones de puertos finales de spanning-tree, donde se eliminan todos los posibles bucles. El proceso de convergencia demora un tiempo en completarse debido a los distintos temporizadores que se utilizan para coordinar el proceso.

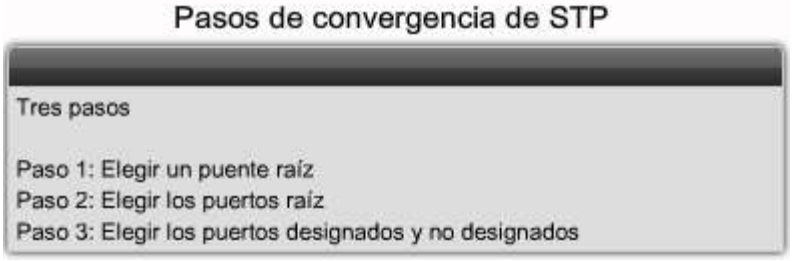
Para comprender el proceso de convergencia de forma más profunda, el mismo se ha dividido en tres pasos distintos:

Paso 1. Elegir un puente raíz

Paso 2. Elegir los puertos raíz

Paso 3. Elegir los puertos designados y no designados

El resto de esta sección explora cada paso del proceso de convergencia.



5.3.2 ELEGIR UN PUENTE RAIZ.-

Paso 1. Elegir un puente raíz

El primer paso de la convergencia en el proceso spanning-tree es la elección del puente raíz. El puente raíz es la base para todos los cálculos de costos de ruta de spanning-tree y en definitiva conduce a la asignación de las distintas funciones de puertos utilizadas para evitar la generación de bucles.

La elección de un puente raíz se genera después de que el switch ha finalizado el proceso de arranque o cuando se detecta una falla en alguna ruta de la red. Inicialmente, todos los puertos de switch se configuran en estado de bloqueo, que demora 20 segundos de manera predeterminada. Esto se lleva a cabo para evitar la generación de un bucle antes de que STP haya contado con el tiempo para calcular las mejores rutas a la raíz y configurar todos los puertos de switch en sus funciones específicas. Como los puertos de switch se encuentran en estado de bloqueo, aún pueden enviar y recibir tramas de BPDU, de manera que pueda continuar la elección de la raíz del spanning-tree. Spanning tree admite un diámetro de red máximo de 7 siete saltos de switch de extremo a extremo. Esto permite que todo el proceso de elección del puente raíz suceda en 14 segundos, que es menor que el tiempo que el puerto de switch permanece en estado de bloqueo.

Inmediatamente después de que los switches finalizan el proceso de arranque, comienzan a enviar tramas de BPDU publicando sus BID, en un intento de convertirse en el puente raíz. Inicialmente, todos los switches de la red asumen que son el puente raíz para ese dominio de broadcast. La saturación de las tramas de BPDU en la red tiene el campo de ID en coincidencia con campo BID, lo que indica que cada switch se considera a sí mismo el puente raíz. Estas tramas de BPDU se envían cada 2 segundos en base al valor predeterminado del temporizador de saludo.

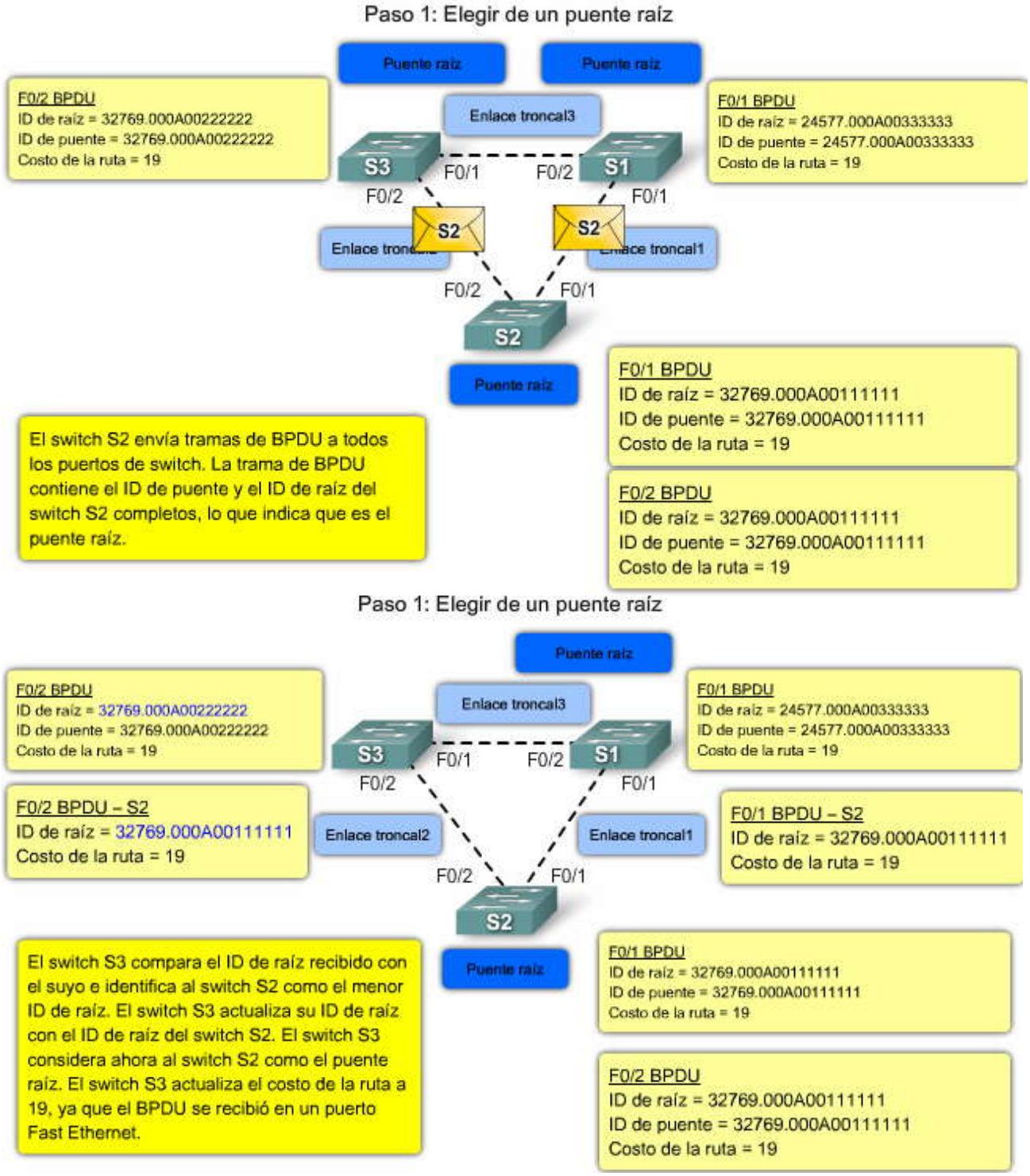
A medida que los switches reciben las tramas de BPDU de sus switches vecinos, comparan el ID de raíz de la trama de BPDU recibida con el ID de raíz configurado localmente. Si el ID de raíz de la trama de BPDU recibida es menor que el propio, el campo ID de raíz se actualiza y se indica el nuevo mejor candidato para la función de puente raíz.

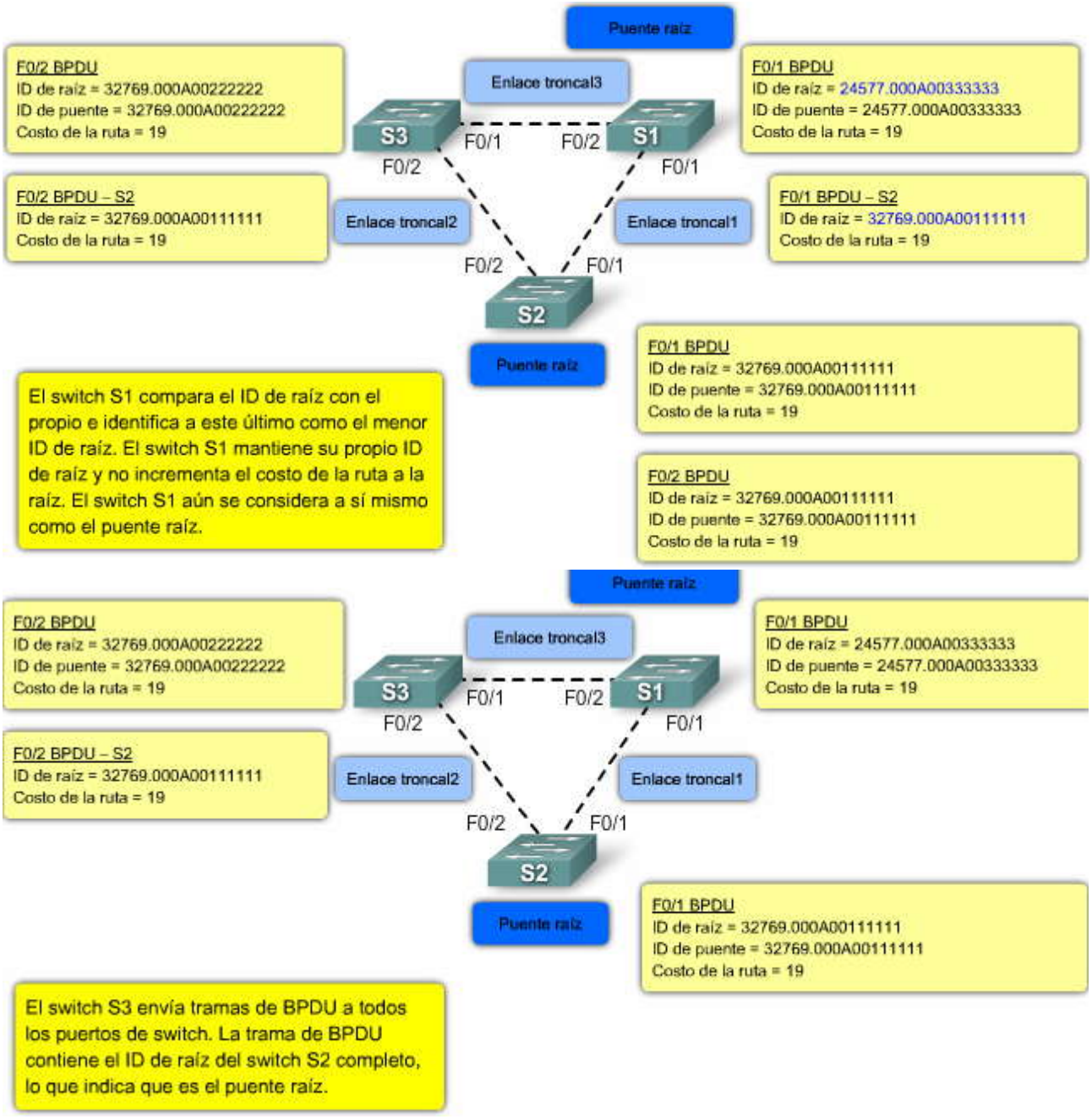
Después de que el campo ID de raíz se actualiza en un switch, este último incorpora el ID de raíz nuevo en todas las transmisiones de tramas de BPDU futuras. Esto asegura que el menor ID de raíz sea siempre enviado a todos los switches adyacentes de la red. La elección del puente raíz finaliza una vez que el menor ID de raíz llena el campo ID de raíz de todos los switches del dominio de broadcast.

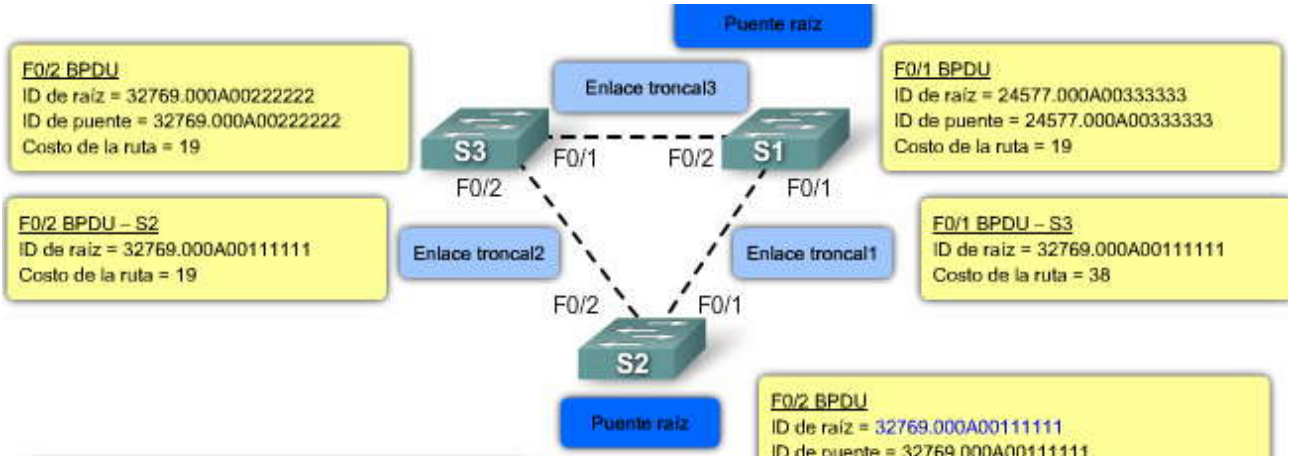
Aunque el proceso de elección del puente raíz finaliza, los switches continúan enviando sus tramas de BPDU y publicando el ID de raíz del puente raíz cada 2 segundos. Cada switch se configura con un temporizador de antigüedad máxima que determina la cantidad de tiempo que el switch mantiene la configuración de BPDU actual en el caso de que deje de recibir las actualizaciones de los switches vecinos. De manera predeterminada, el temporizador de antigüedad máxima se establece en 20 segundos. Por lo tanto, si un switch no puede recibir 10 tramas de BPDU consecutivas de uno de sus vecinos, asume que ha fallado una ruta lógica del spanning tree y que la información de la BPDU ya no es válida. Esto provoca otra elección de puente raíz de spanning-tree.

Haga clic en el botón Reproducir de la figura para volver a ver los pasos que utiliza STP para elegir un puente raíz

A medida que repase la forma en que STP elige un puente raíz, recuerde que el proceso de elección del puente raíz se produce con todos los switches que envían y reciben tramas de BPDU al mismo tiempo. La realización del proceso de elección de forma simultánea permite a los switches determinar de manera más rápida el switch que se convertirá en el puente raíz.



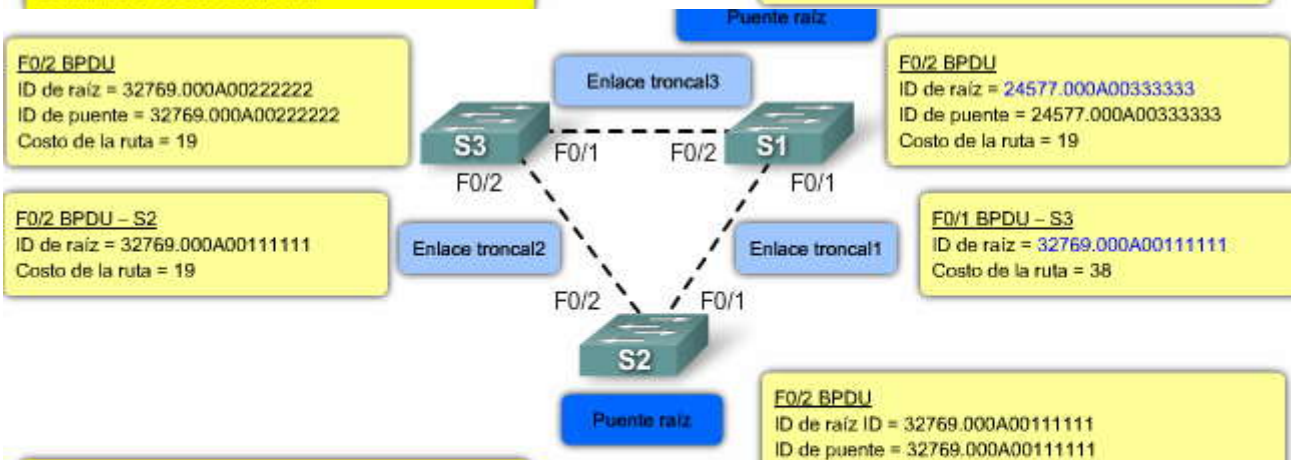

Puente raíz
F0/2 BPDU
ID de raíz = 32769.000A00222222
ID de puente = 32769.000A00222222
Costo de la ruta = 19
Enlace troncal3
F0/1 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 24577.000A00333333
Costo de la ruta = 19
S3
F0/1
F0/2
F0/2
S1
F0/1
F0/2 BPDU – S2
ID de raíz = 32769.000A00111111
Costo de la ruta = 19
Enlace troncal2
Enlace troncal1
F0/1 BPDU – S2
ID de raíz = 32769.000A00111111
Costo de la ruta = 19
F0/2
F0/1
S2
Puente raíz
F0/1 BPDU
ID de raíz = 32769.000A00111111
ID de puente = 32769.000A00111111
Costo de la ruta = 19
El switch S1 compara el ID de raíz con el propio e identifica a este último como el menor ID de raíz. El switch S1 mantiene su propio ID de raíz y no incrementa el costo de la ruta a la raíz. El switch S1 aún se considera a sí mismo como el puente raíz.
F0/2 BPDU
ID de raíz = 32769.000A00111111
ID de puente = 32769.000A00111111
Costo de la ruta = 19
Puente raíz
F0/2 BPDU
ID de raíz = 32769.000A00222222
ID de puente = 32769.000A00222222
Costo de la ruta = 19
Enlace troncal3
F0/1 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 24577.000A00333333
Costo de la ruta = 19
S3
F0/1
F0/2
F0/2
S1
F0/1
F0/2 BPDU – S2
ID de raíz = 32769.000A00111111
Costo de la ruta = 19
Enlace troncal2
Enlace troncal1
F0/2
F0/1
S2
Puente raíz
F0/1 BPDU
ID de raíz = 32769.000A00111111
ID de puente = 32769.000A00111111
Costo de la ruta = 19
El switch S3 envía tramas de BPDU a todos los puertos de switch. La trama de BPDU contiene el ID de raíz del switch S2 completo, lo que indica que es el puente raíz.



El switch S2 compara el ID de raíz de BPDU recibido con el propio e identifica la coincidencia. El switch S2 sigue considerando que es el puente raíz de la red. El switch S2 no actualiza el costo de la ruta.

F0/2 BPDU
ID de raíz = 32769.000A00111111
ID de puente = 32769.000A00111111
Costo de la ruta = 19

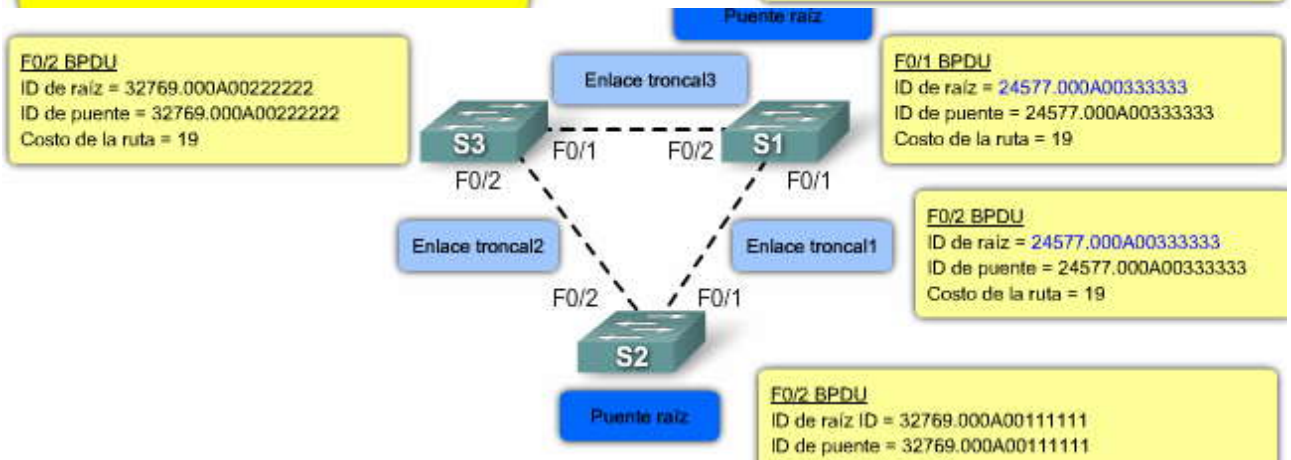
F0/2 BPDU – S3
ID de raíz = 32769.000A00111111
Costo de la ruta = 19



El switch S1 compara el ID de raíz de BPDU recibido con el propio e identifica que este último es menor. El switch S1 sigue considerando que es el puente raíz de la red. El switch S1 no actualiza el costo de la ruta.

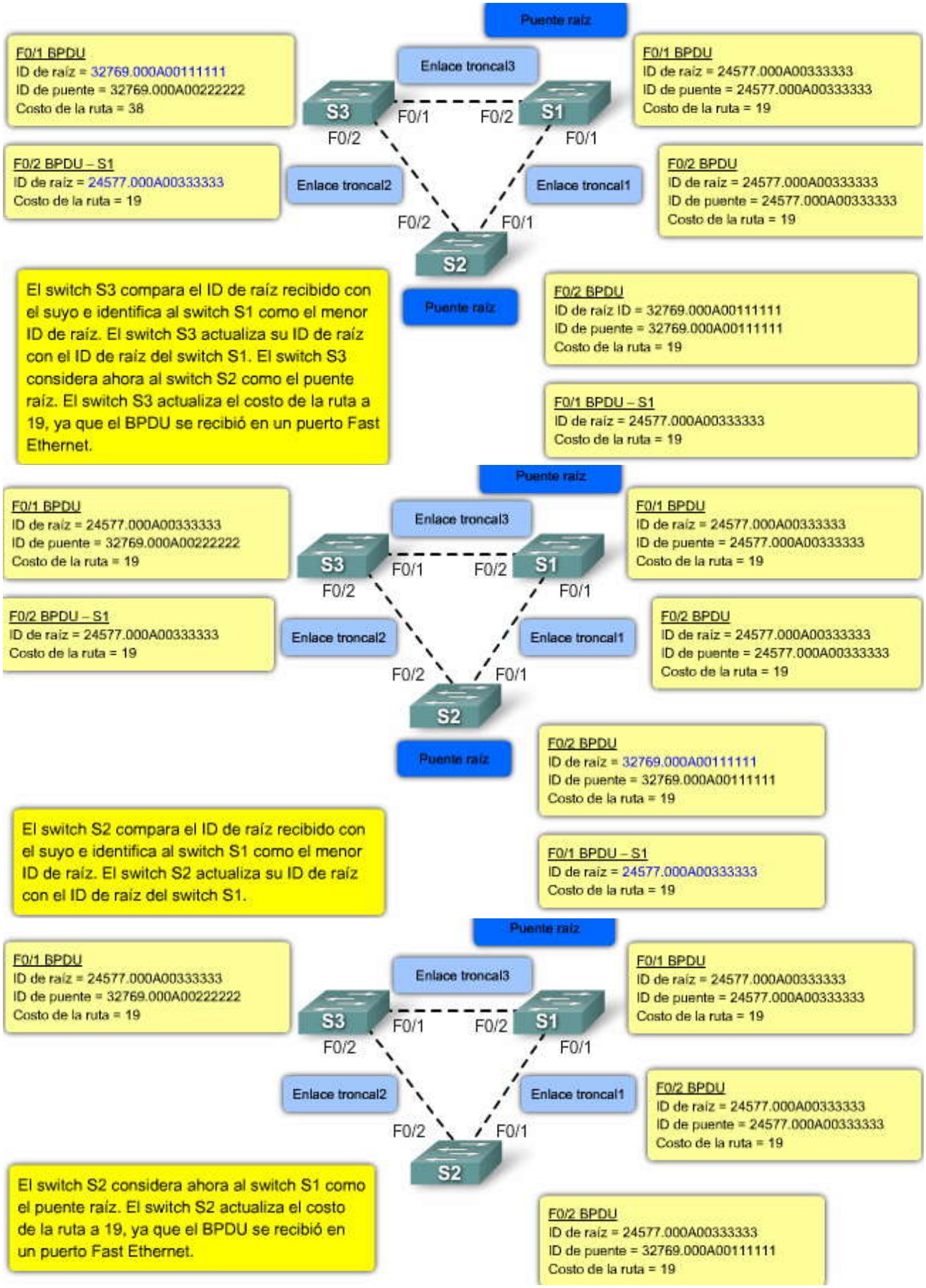
F0/2 BPDU
ID de raíz ID = 32769.000A00111111
ID de puente = 32769.000A00111111
Costo de la ruta = 19

F0/2 BPDU – S3
ID de raíz = 32769.000A00111111
Costo de la ruta = 19



El switch S1 envía tramas de BPDU a todos los puertos de switch. La trama de BPDU contiene el ID de puente y el ID de raíz del switch S1 completos, lo que indica que es el puente raíz.

F0/2 BPDU
ID de raíz ID = 32769.000A00111111
ID de puente = 32769.000A00111111
Costo de la ruta = 19



Verificar la elección del puente raíz

Cuando finaliza la elección del puente raíz, se puede verificar la identidad del mismo a través del comando show spanning-tree en modo EXEC privilegiado

En la topología de ejemplo, el switch S1 posee el menor valor de prioridad de los tres switches, de manera que se puede asumir que el mismo se convertirá en el puente raíz.

Haga clic en el botón Resultado del switch S1 que se muestra en la figura.

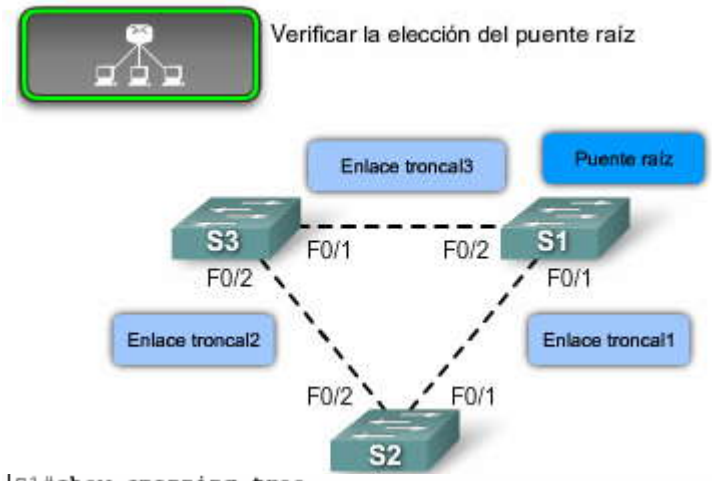
En el ejemplo, el resultado de show spanning-tree para el switch S1 revela que es el puente raíz. Se puede observar que el BID coincide con el ID de raíz, lo que confirma que S1 es el puente raíz.

Haga clic en el botón Resultado del switch S2 que se muestra en la figura.

En el ejemplo, el resultado de show spanning-tree para el switch S2 muestra que el ID de raíz coincide con el ID de raíz esperado del switch S1, lo que indica que S2 considera a S1 como el puente raíz.

Haga clic en el botón Resultado del switch S3 que se muestra en la figura.

En el ejemplo, el resultado de show spanning-tree para el switch S3 muestra que el ID de raíz coincide con el ID de raíz esperado del switch S1, lo que indica que S3 considera a S1 como el puente raíz.




```
S1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     000A.0033.3333
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    Shr
Fa0/2            Desg FWD 19        128.2    Shr
```

```
S2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.0011.1111
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Root FWD 19        128.1    Shr
Fa0/2            Desg FWD 19        128.2    Shr
```

```
S3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.0022.2222
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    Shr
Fa0/2            Altn BLK 19        128.2    Shr
```

5.3.3 ELEGIR LOS PUERTOS RAIZ.-

Paso 2. Elegir los puertos raíz

Ahora que se ha determinado el puente raíz, los switches comienzan a configurar las funciones de los puertos para cada uno de sus puertos de switch. La primera función de puerto que debe determinarse es la de puerto raíz.

Todos los switches de un topología spanning-tree, excepto el puente raíz, poseen un único puerto raíz definido. El puerto raíz es el puerto de switch con el menor costo de ruta hacia el puente raíz. Normalmente, sólo el costo de ruta determina el puerto de switch que se convierte en puerto raíz. Sin embargo, algunas características adicionales de los puertos determinan el puerto raíz cuando dos o más puertos del mismo switch poseen el mismo costo de rutahacia la raíz. Esto puede suceder cuando se utilizan enlaces redundantes para conectar un switch a otro en el caso de que no se utilice una configuración EtherChannel. Recuerde que la tecnología EtherChannel de Cisco permite configurar varios enlaces físicos de tipo Ethernet como un solo enlace lógico.

Los puertos de switch con costos de ruta hacia la raíz equivalentes utilizan el valor de prioridad de puerto configurable. Utilizan el ID de puerto para tomar la decisión. Cuando un switch elige un puerto de igual costo de puerto que el raíz por sobre otro, el puerto que no es elegido se configura como no designado para evitar un bucle.

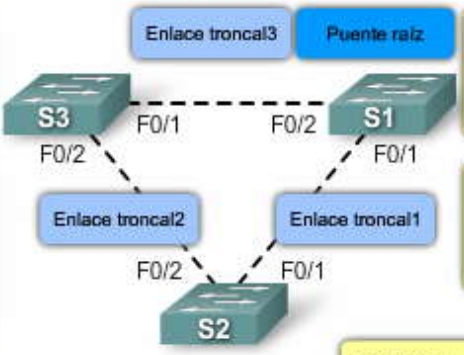
El proceso de determinar el puerto que se convierte en puerto raíz se produce durante el intercambio de BPDU en la elección del puente raíz. Los costos de ruta se actualizan de forma inmediata cuando llegan las tramas de BPDU, lo que indica la presencia de un nuevo ID de raíz o ruta redundante. En el momento en que se actualiza el costo, el switch ingresa en el modo de decisión para determinar si las configuraciones de los puertos deben actualizarse. Las decisiones sobre las funciones de puertos no esperan hasta que todos los switches establezcan cuál será el puente raíz definitivo. En consecuencia, la función de puerto para un puerto de switch determinado puede cambiar varias veces durante la convergencia, hasta que finalmente se establece en su función de puerto definitiva después de que el ID de raíz cambia por última vez.

Haga clic en cada paso de la figura para aprender acerca de la elección de puertos raíz.

Paso 2. Elegir los puertos raíz

F0/1 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00222222
Costo de la ruta = 19

F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00222222
Costo de la ruta = 38



F0/1 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 24577.000A00333333
Costo de la ruta = 19

F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 24577.000A00333333
Costo de la ruta = 19

1

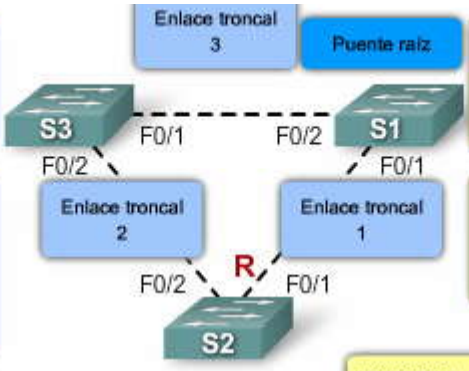
F0/1 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00111111
Costo de la ruta = 19

F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00111111
Costo de la ruta = 38

El switch S2 compara los costos de rutas para cada uno de sus puertos de switch.

F0/1 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00222222
Costo de la ruta = 19

F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00222222
Costo de la ruta = 38



F0/1 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 24577.000A00333333
Costo de la ruta = 19

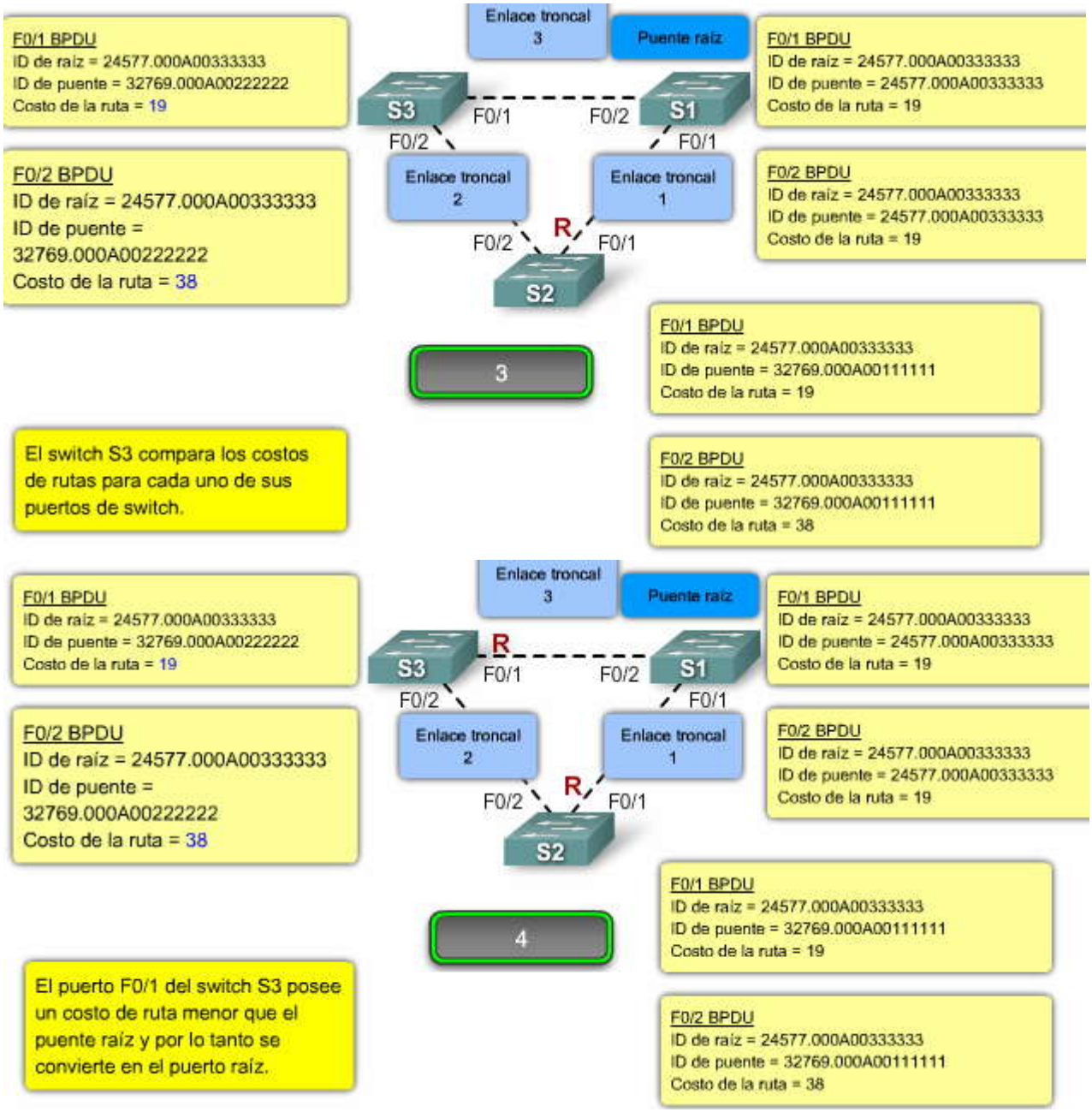
F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 24577.000A00333333
Costo de la ruta = 19

2

F0/1 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00111111
Costo de la ruta = 19

F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00111111
Costo de la ruta = 38

El puerto F0/1 del switch S2 posee un costo de ruta menor que el puente raíz y por lo tanto se convierte en el puerto raíz.



Verificar el puerto raíz

Cuando finaliza la elección del puente raíz, se puede verificar la configuración de los puertos raíz a través del comando show spanning-tree en modo EXEC privilegiado.

En la topología de ejemplo, el switch S1 ha sido identificado como puente raíz. El puerto F0/1 de S2 y el puerto F0/1 del switch S3 son los dos más cercanos al puente raíz y, por lo tanto, deben configurarse como puertos raíz. Se puede confirmar la configuración del puerto mediante el comando show spanning-tree en modo EXEC privilegiado.

Haga clic en el botón Resultado del switch S1 que se muestra en la figura.

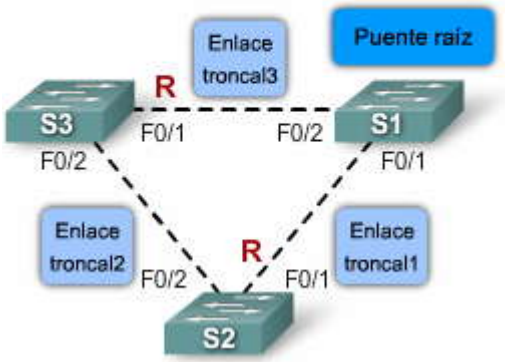
En el ejemplo, el resultado de show spanning-tree para el switch S1 revela que es el puente raíz y en consecuencia no posee puertos raíz configurados.

Haga clic en el botón Resultado del switch S2 que se muestra en la figura.
En el ejemplo, el resultado de show spanning-tree para el switch S2 muestra que el puerto de switch F0/1 está configurado como puerto raíz. El ID de raíz muestra la prioridad y la dirección MAC del switch S1.

Haga clic en el botón Resultado del switch S3 que se muestra en la figura.

En el ejemplo, el resultado de show spanning-tree para el switch S3 muestra que el puerto de switch F0/1 está configurado como puerto raíz. El ID de raíz muestra la prioridad y la dirección MAC del switch S1.

Verificar el puerto raíz




```
S1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     000A.0033.3333
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    Shr
Fa0/2            Desg FWD 19        128.2    Shr
```

No hay puertos raíz

```
S2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.0011.1111
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Root FWD 19        128.1    Shr
Fa0/2            Desg FWD 19        128.2    Shr
```

```
S3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.0022.2222
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    Shr
Fa0/2            Altn BLK 19        128.2    Shr
```

5.3.4 EÑEGIR PUERTOS DESIGNADOS Y PUERTOS NO DESIGNADOS.-

Paso 3. Elegir puertos designados y puertos no designados

Después de que el switch determina qué puerto es el raíz, los puertos restantes deben configurarse como puerto designado (DP) o puerto no designado (no DP) para finalizar la creación del spanning tree lógico sin bucles.

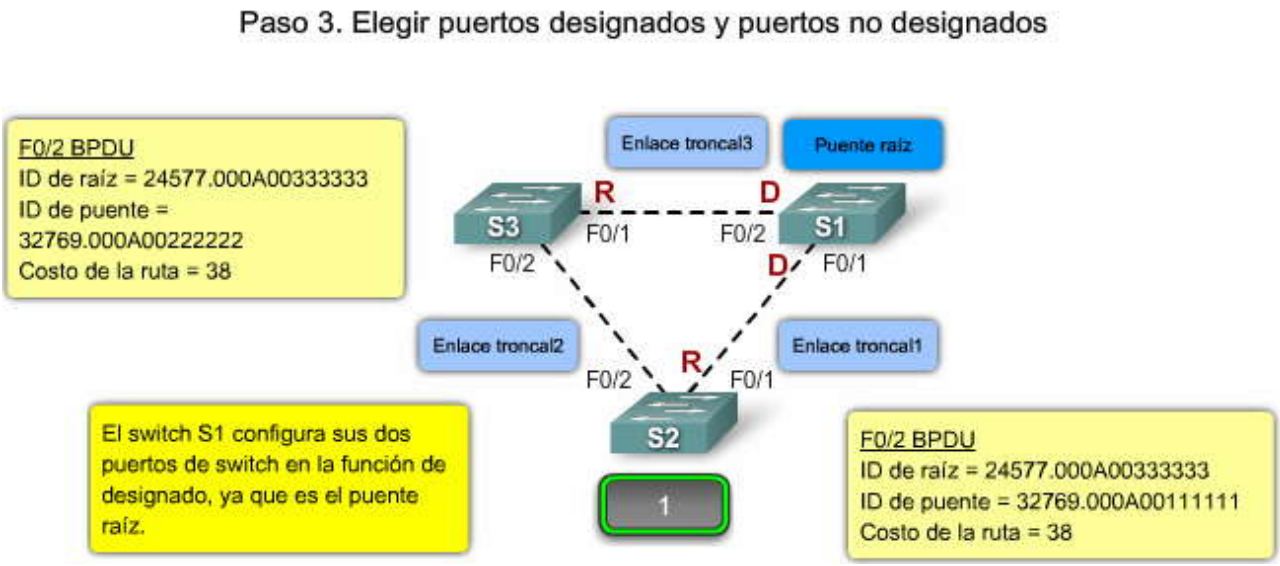
Todos los segmentos de una red conmutada sólo pueden contar conun puerto designado. Cuando dos puertos de switch que no son raíz se conectan al mismo segmento de LAN, se lleva a cabo una competencia por las funciones de puertos. Los dos switches intercambian tramas de BPDU para decidir cuál de los puertos se establececomo designado y cuál como no designado.

En general, cuando un puerto de switch se configura como designado, se basa en el BID. Sin embargo, tenga en cuenta que la primera prioridad es el menor costo de ruta hacia el puente raíz y que el BID del emisor sólo lo es cuando los costos de los puertos son iguales.

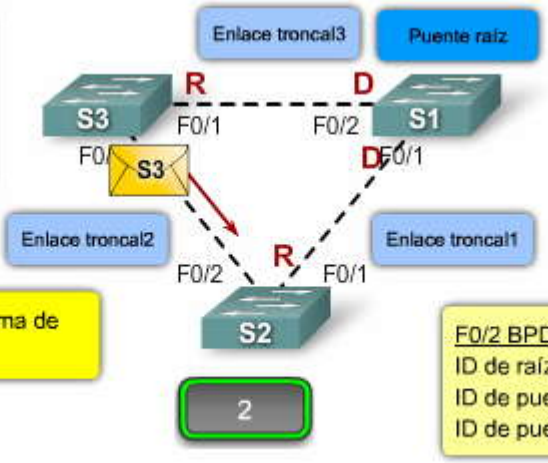
Cuando dos switches intercambian sus tramas de BPDU, examinan el BID enviado en la trama de BPDU recibida para verificar si es menor que los propios. El switch con el menor BID gana la competencia ysu puerto se configura con la función de designado. El switch restante configura su puerto de switch como no designado y, por lo tanto, en el estado de bloqueo para evitar la generación de bucles.

El proceso de determinar las funciones de los puertos seproduce de forma conjunta con la elección del puente raíz y con la designación del puerto raíz. En consecuencia, las funciones de designado y no designado pueden cambiar varias veces durante el proceso de convergencia hasta que se haya determinado el último puente raíz. El proceso completo de seleccionar el puente raíz, determinar los puertos raíz y los puertos designados y no designados se lleva a cabo dentro de los 20 segundos que transcurren durante el estado de bloqueo. Este tiempo de convergencia se basa en el temporizador de saludo de 2 segundos para las transmisiones de tramas de BPDU y el diámetro de siete switches que admite STP. La demora de antigüedad máxima de 20 segundos provee el tiempo suficiente para el diámetro de siete switches con el temporizador de saludo de 2 segundos entre transmisiones de tramas de BPDU.

Haga clic en cada paso de la figura para aprender acerca de la elección de puertos designados y no designados.



F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente =
32769.000A00222222
Costo de la ruta = 38

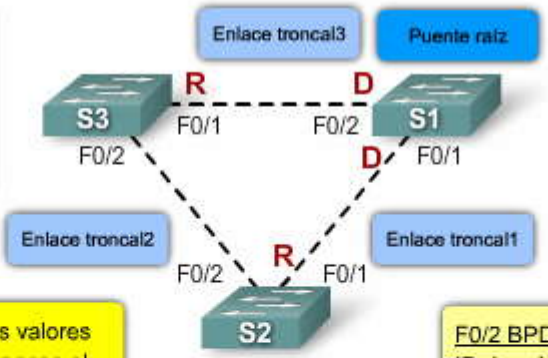


El switch S3 envía una trama de BPDU al switch S2.

2

F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00111111
ID de puente = 38

F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente =
32769.000A00222222
Costo de la ruta = 38



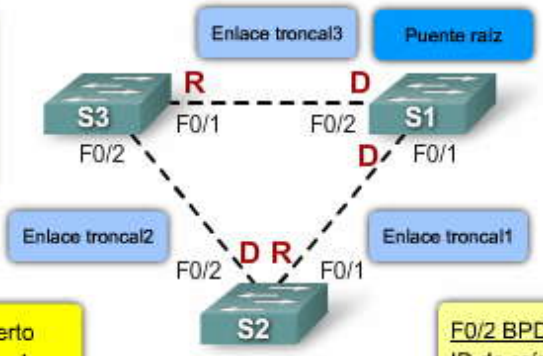
El switch S2 compara los valores de BID y determina que posee el menor valor.

3

F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00111111
Costo de la ruta = 38

F0/2 BPDU – S3
ID de puente = 32769.000A00222222
Costo de la ruta = 38

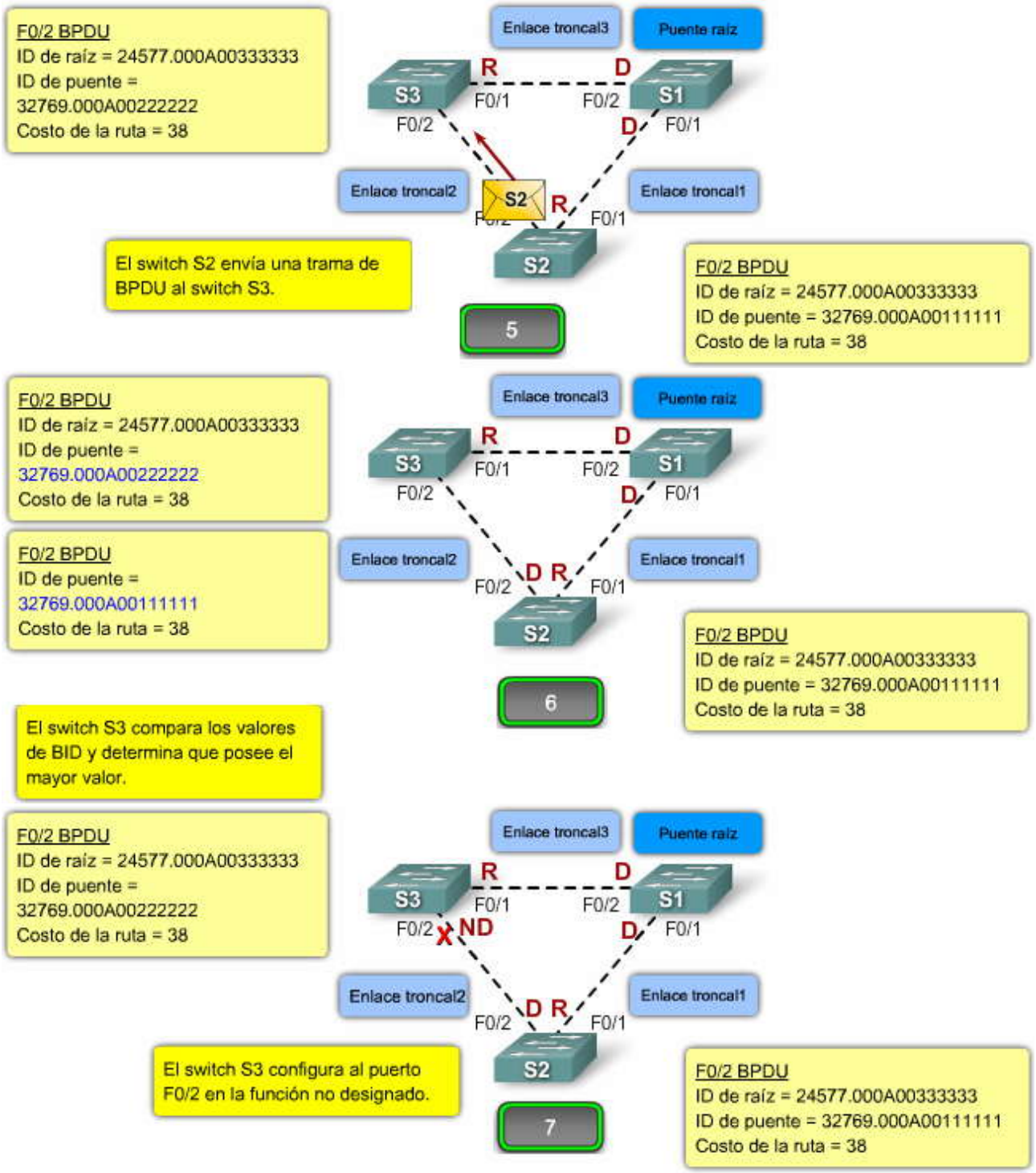
F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente =
32769.000A00222222
Costo de la ruta = 38



El switch S2 configura el puerto F0/2 en la función de designado.

4

F0/2 BPDU
ID de raíz = 24577.000A00333333
ID de puente = 32769.000A00111111
Costo de la ruta = 38



Verificar DP y no DP

Después de que se asignaron los puertos raíz, los switches determinan cuáles de los puertos restantes se configuran como designados y cuáles como no designados. Se puede verificar la configuración de los puertos designados y no designados mediante el comando show spanning-tree en modo EXEC privilegiado.

En la topología:

1. El switch S1 se identifica como puente raíz y, por lo tanto, configura sus dos puertos de switch como designados.

2. El puerto F0/1 de switch S2 y el puerto F0/1 del switch S3 son los dos más cercanos al puente raíz y se configuran como puertos raíz.

3. Los restantes, el puerto F0/2 del switch S2 y el puerto F0/2 del switch S3 deben decidir cuál de los dos será el designado y cuál será el no designado.

4. El switch S2 y el switch S3 comparan sus valores de BID para determinar cuál es el menor. El que posee el menor BID se configura como puerto designado.

5. Debido a que ambos switches cuentan con la misma prioridad, la dirección MAC se convierte en el factor de decisión.

6. Ya que el switch S2 posee una dirección MAC menor, configura su puerto F0/2 como designado.

7. En consecuencia, el switch S3 configura su puerto F0/2 como no designado para evitar la generación de bucles.

Se puede confirmar la configuración de puerto mediante el comando show spanning-tree en modo EXEC privilegiado.

Haga clic en el botón Resultado del switch S1 que se muestra en la figura.

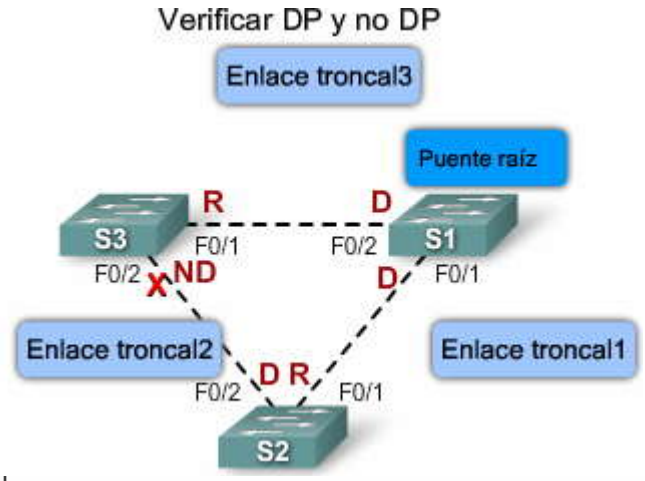
En el ejemplo, el resultado de show spanning-tree para el switch S1 revela que es el puente raíz y en consecuencia sus dos puertos se configuran como designados.

Haga clic en el botón Resultado del switch S2 que se muestra en la figura.

En el ejemplo, el resultado de show spanning-tree para el switch S2 muestra que el puerto de switch F0/2 está configurado como puerto designado.

Haga clic en el botón Resultado del switch S3 que se muestra en la figura.

En el ejemplo, el resultado de show spanning-tree para el switch S3 muestra que el puerto de switch F0/2 está configurado como puerto no designado.




```
S1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address      000A.0033.3333
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

```
S2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.0011.1111
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
S3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.0022.2222
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
```

5.3.5 CAMBIO EN LA TOPOLOGIA DE STP.-

Proceso de notificación de cambio en la topología de STP

Un switch considera que ha detectado un cambio en la topología cuando un puerto que envía se desactiva (se bloquea, por ejemplo) o cuando un puerto cambia al estado de enviar y el switch cuenta con un puerto designado. Cuando se detecta un cambio, el switch notifica al puente raíz del spanning tree. Luego, el puente raíz envía un broadcast con dicha información a toda la red.

Cuando STP funciona de forma normal, el switch continúa recibiendo tramas de BPDU de configuración desde el puente raíz en su puerto raíz. Sin embargo, nunca envía una BPDU hacia el puente raíz. Para lograr esto se introduce una BPDU especial denominada notificación de cambio en la topología (TCN). Cuando un switch necesita avisar acerca de uncambio en la topología, comienza a enviar TCN en su puerto raíz. La TCN es una BPDU muy simple que no contiene información y se envía durante el intervalo de tiempo de saludo. El switch receptor se denomina puente designado y realiza el acuse de recibo de la TCN mediante el envío inmediato de una BPDU normal con el bit de acuse de recibo de cambio en la topología (TCA). Este intercambio continúa hasta que el puente raíz responde.

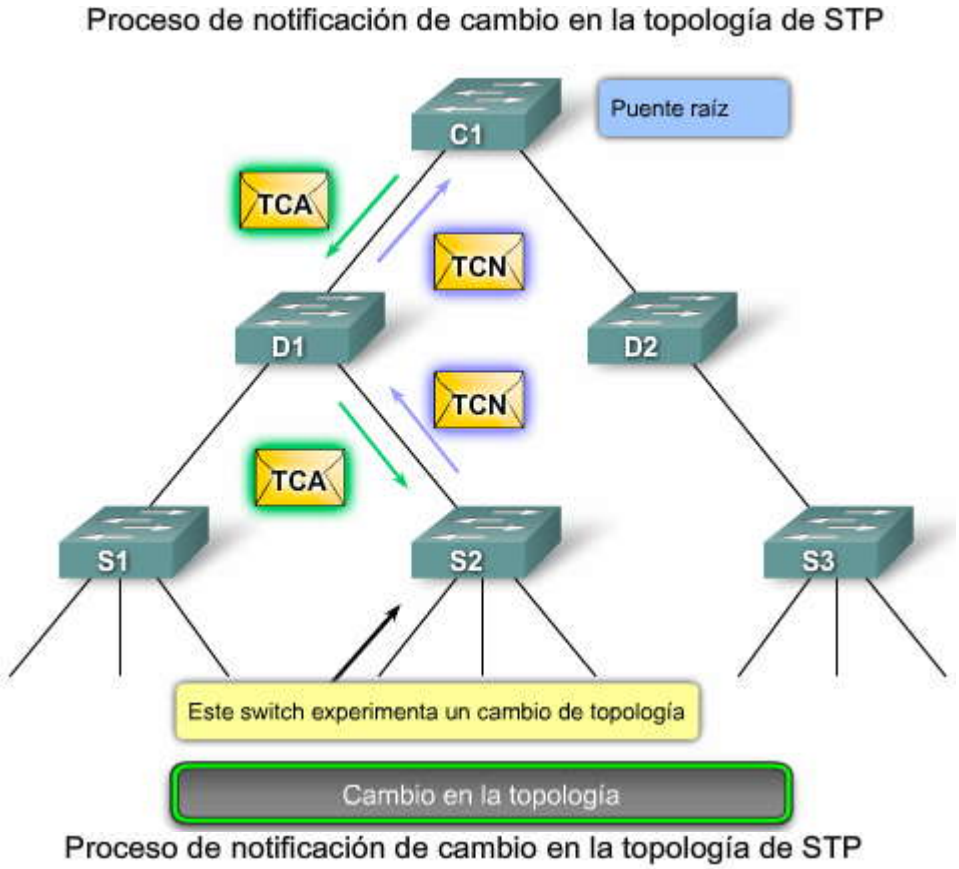
Por ejemplo, en la figura el switch S2 experimenta un cambio de topología. Envía una TCN a su puente designado, que en este caso es el switch D1. El switch D1 recibe la TCN y acusa recibo a S2 con una TCA. El switch D1 genera una TCN y la envía a su puente designado, que en este caso es el puente raíz.

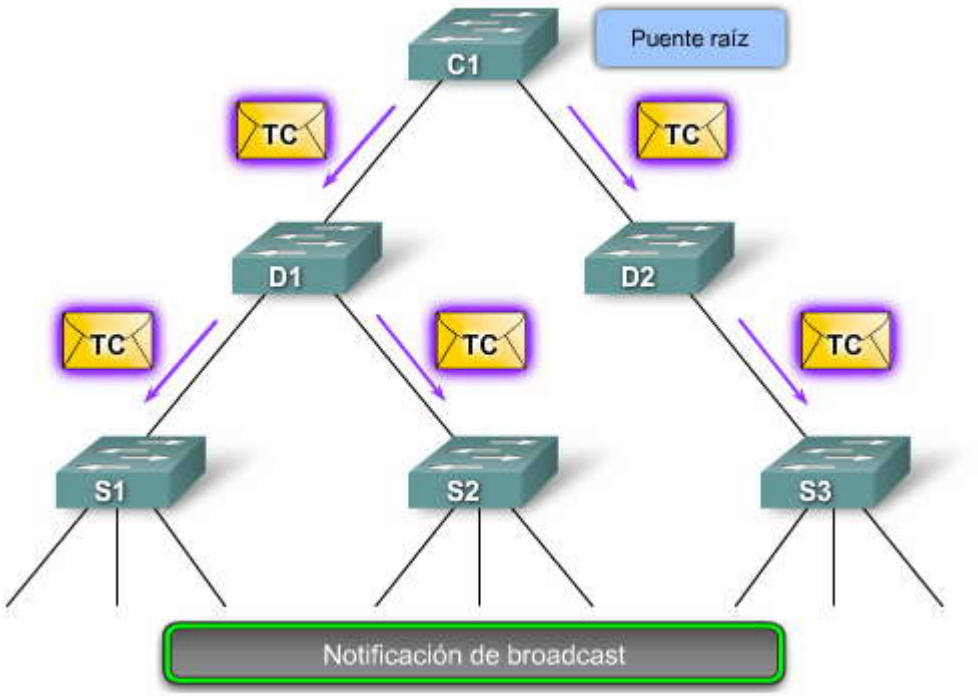
Haga clic en el botón Notificación de broadcast que se muestra en la figura.

Notificación de broadcast

Una vez que el puente raíz advierte que se ha producido un evento de cambio en la topología en la red, comienza a enviar sus BPDU de configuración con el bit de cambio de topología (TC) establecido. Estas BPDU son transmitidas por todos los switches de la red con dicho bit establecido. En consecuencia, todos los switches advierten el cambio de topología y pueden reducir su tiempo de expiración al retraso de envío. Los switches reciben las BPDU de cambio de topología tanto en los puertos en estado de enviar como de bloqueo.

La raíz establece el bit de TC durante un período igual a la suma de la antigüedad máxima y el retraso de envío (en segundos), que de manera predeterminada es 20+15=35.





5.4 PVST+, RSTP Y PVST+ RÁPIDO.-

5.4.1 VARIANTES DE CISCO Y STP.-

Al igual que con muchos estándares de redes, la evolución de STP se ha enfocado en la necesidad de crear especificaciones para toda la industria cuando los protocolos de propiedad son estándares de hecho. Cuando un protocolo de propiedad es tan predominante que todos sus competidores del mercado deben contar con soporte para el mismo, las agencias como el IEEE intervienen y crean una especificación pública. La evolución de STP ha seguido este mismo camino, como puede verse en la tabla.

Cuando se lee acerca de STP en el sitio Cisco.com, se advierte que existen muchos tipos de variantes de STP. Algunas de estas variantes son propiedad de Cisco y otras son estándares de IEEE. Aprenderá másdetalles acerca de algunas de estas

variantes de STP pero para comenzar necesita poseer un conocimiento general de cuáles son las variantes de STP más importantes. La tabla resume las descripciones siguientes de las variantes principales de STP de Cisco e IEEE.

Propiedad de Cisco

Protocolo spanning tree por VLAN (PVST): Mantiene una instancia de spanning-tree para cada VLAN configurada en la red. Utiliza el protocolo de enlace troncal ISL propiedad de Cisco que permite que un enlace troncal de la VLAN se encuentre en estado de enviar para algunas VLAN y en estado de bloqueo para otras. Debido a que PVST trata a cada VLAN como una red independiente, puede balancear la carga de tráfico de la Capa 2 mediante el envío de algunas VLAN de un enlace troncal y otras de otro enlace troncal sin generar bucles. Para PVST, Cisco desarrolló varias extensiones de propiedad del IEEE 802.1D STP original, como BackboneFast, UplinkFast y PortFast. Estas extensiones de STP de Cisco no se cubren en este curso. Para obtener más información acerca de estas extensiones, visite: http://www.cisco.com/en/US/docs/switches/lan/catalyst4000/7.4/configuration/guide/stp_enha.html.

Protocolo spanning tree por VLAN plus (PVST+): Cisco desarrolló PVST+ para proporcionar soporte a los enlaces troncales de IEEE 802.1Q. PVST+ proporciona la misma funcionalidad que PVST, incluidas las extensiones de STP propiedad de Cisco. PVST+ no cuenta con soporte en aquellos dispositivos que no son de Cisco. PVST+ incluye una mejora de PortFast denominada protección de BPDU y protección de raíz. Para obtener más información acerca de la protección de BPDU, visite:
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a008009482f.shtml.

Para obtener más información acerca de la protección de raíz, visite:
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800ae96b.shtml.

Protocolo spanning tree por VLAN rápido (PVST+ rápido): Se basa en el estándar IEEE 802.1w y posee una convergencia más veloz que STP (estándar 802.1D). PVST+ rápido incluye las extensiones propiedad de Cisco, como BackboneFast, UplinkFast y PortFast.

Estándares IEEE

Protocolo Rapid spanning tree (RSTP): Se introdujo por primera vez en 1982 como evolución de STP (estándar 802.1D). Proporciona una convergencia de spanning-tree más veloz después de un cambio de topología. RSTP implementa las extensiones de STP propiedad de Cisco, como BackboneFast, UplinkFast y PortFast en el estándar público. A partir de 2004, el IEEE incorporó RSTP a 802.1D, mediante la identificación de la especificación como IEEE 802.1D-2004. De manera que cuando se haga referencia a STP, debe pensarse en RSTP. Aprenderá más acerca de RSTP posteriormente en esta sección.

STP múltiple (MSTP): permite que se asignen VLAN múltiples a la misma instancia de spanning-tree, de modo tal que se reduce la cantidad de instancias necesarias para admitir una gran cantidad de VLAN. MSTP se inspiró en STP de instancias múltiples (MISTP) propiedad de Cisco y es una evolución de STP y RSTP. Se introdujo en el IEEE 802.1s como enmienda de la edición de 802.1Q de 1998. El estándar IEEE 802.1Q-2003 ahora incluye a MSTP. MSTP proporciona varias rutas de envío para el tráfico de datos y permite el balanceo de carga. La explicación de MSTP excede el alcance de este curso. Para obtener más información acerca de MSTP, visite:
http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_19_ea1/configuration/guide/swmstp.html.

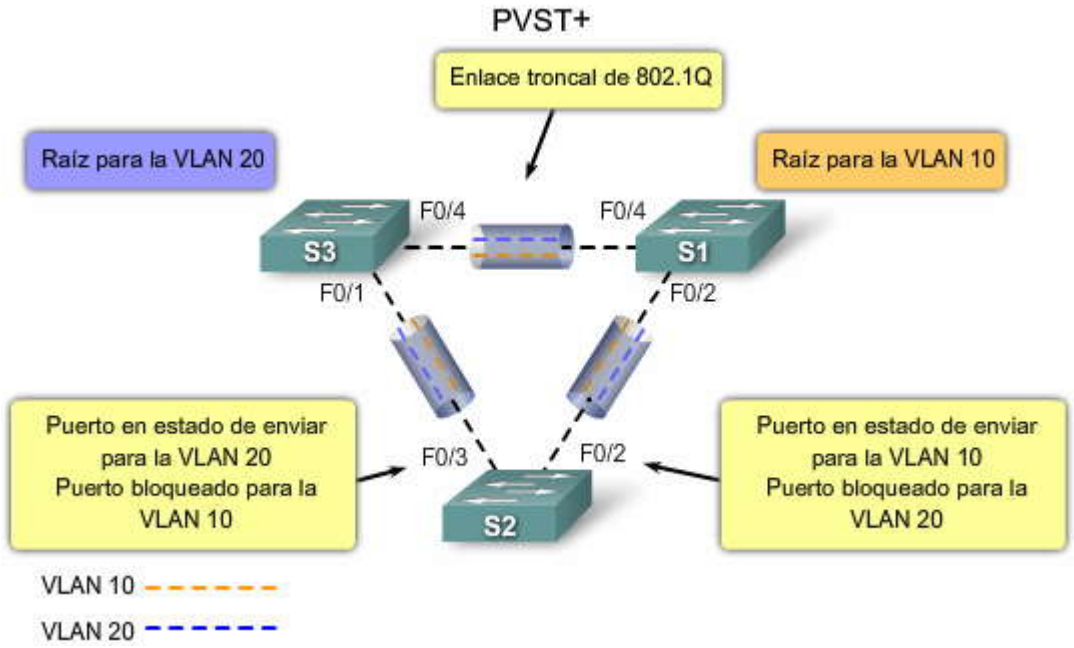
Variantes de Cisco y STP

Propiedad de Cisco	**PVST** • Utiliza el protocolo de enlace troncal ISL propiedad de Cisco • Cada VLAN cuenta con una instancia de spanning tree • Capacidad de balancear la carga de tráfico de la Capa 2 • Incluye las extensiones BackboneFast, UplinkFast y PortFast
	PVST+ • Admite ISL y enlace troncal IEEE 802.1Q • Admite las extensiones de STP propiedad de Cisco • Agrega mejoras en la protección de BPDU y en la protección de raíz
	PVST+ rápido • Basado en el estándar IEEE802.1w • Posee convergencia más veloz que 802.1D
Estándar IEEE	**RSTP** • Presentado en 1982, brinda una convergencia más veloz que 802.1D • Implementa versiones genéricas de las extensiones de STP propiedad de Cisco • IEEE incorporó RSTP dentro de 802.1D, identificando la especificación como IEEE 802.1D-2004
	MSTP • Pueden asignarse varias VLAN a una misma instancia de spanning-tree • Inspirado en el protocolo spanning tree de múltiples instancias (MISTP) de Cisco, • IEEE 802.1Q-2003 ahora incluye a MSTP

5.4.2 PVST+.-
PVST+

Cisco desarrolló PVST+ para que una red pueda ejecutar una instancia de STP para cada VLAN de la red. Con PVST+ puede bloquearse más de un enlace troncal en una VLAN y puede implementarse la carga compartida. Sin embargo, implementar PVST+ implica que todos los switches de la red se comprometan con la convergencia de la red y los puertos de switch deben ajustarse al ancho de banda adicional utilizado para cada instancia de PVST+ a fin de poder enviar sus propias BPDU.

En un entorno de PVST+ de Cisco se pueden ajustar los parámetros de spanning-tree de manera que la mitad de las VLAN puedan enviar en todos los enlaces troncales. En la figura, el puerto F0/3 del switch S2 es el puerto emisor para la VLAN 20 y F0/2 del switch S2 es el puerto emisor para la VLAN 10. Esto se logra mediante la configuración de un switch para elegirlo como puente raíz para la mitad de la cantidad total de VLAN de la red y de otro para elegirlo como puente raíz para la otra mitad de las VLAN. En la figura, el switch S3 es el puente raíz para la VLAN 20 y el switch S1 es el puente raíz para la VLAN 10. La creación de distintos switches raíz en STP por VLAN genera una red más redundante.



ID de puente en PVST+

Como recordará, en el estándar 802.1D original, un BID de 8 bytes se compone de una prioridad de puente de 2 bytes y una dirección MAC de 6 bytes de switch. No había necesidad de identificar una VLAN debido a que sólo existía un spanning tree en la red. PVST+ requiere que se ejecute una instancia de spanning tree independiente por cada VLAN. Para admitir PVST+, el campo BID de 8 bytes se modifica para transportar un ID de VLAN (VID). En la figura, el campo de prioridad de puente se reduce a 4 bits y un nuevo campo de 12 bits, el ID de sistema extendido, contiene el VID. La dirección MAC de 6 bytes permanece sin cambios.

A continuación se brindan más detalles acerca de los campos de PVST+:

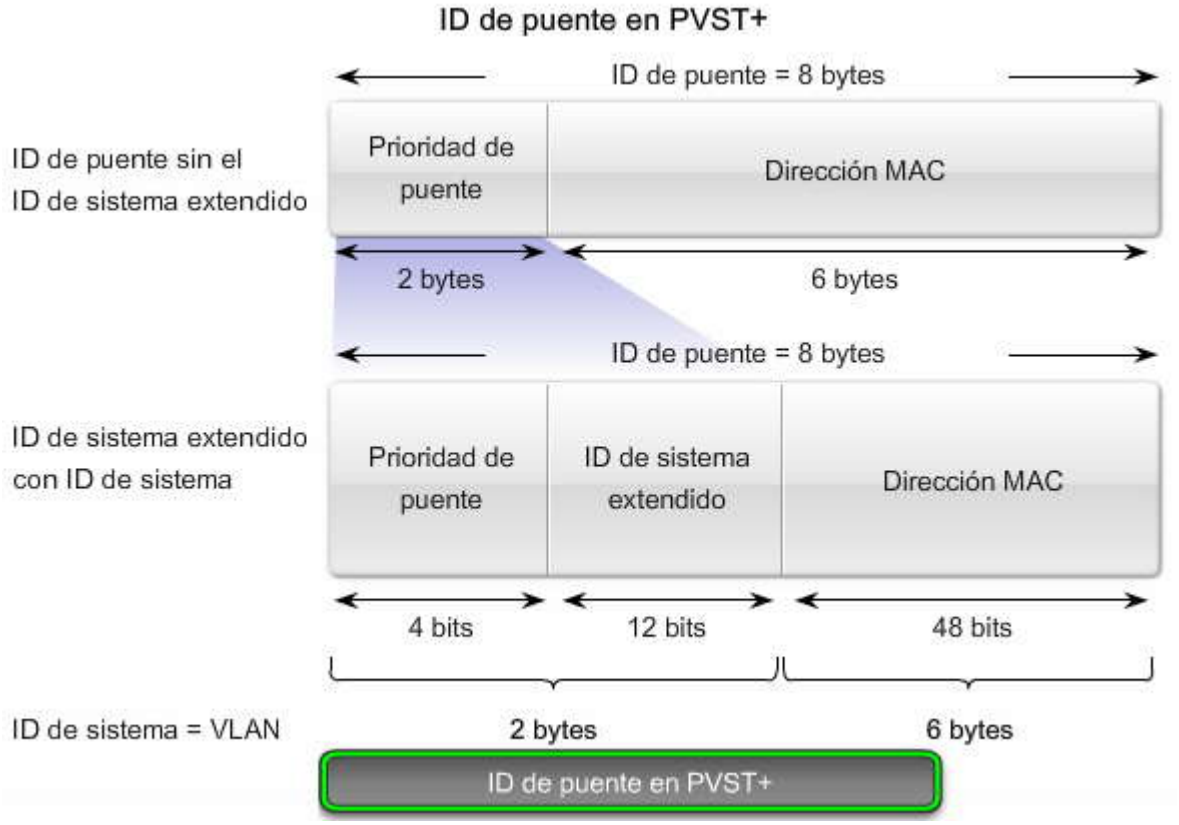
Prioridad de puente: un campo de 4 bits contiene la prioridad de puente. Debido a la cantidad de bits limitados, la prioridad se transporta en valores discretos en incrementos de 4096 en lugar de valores discretos con incrementos de 1, como sería si se dispusiera del campo de 16 bits. La prioridad predeterminada, de acuerdo al IEEE 802.1D, es 32 768, que es el valor medio.
ID de sistema extendido: un campo de 12 bits que contiene el VID para PVST+.
Dirección MAC: un campo de 6 bytes con la dirección MAC de un solo switch.

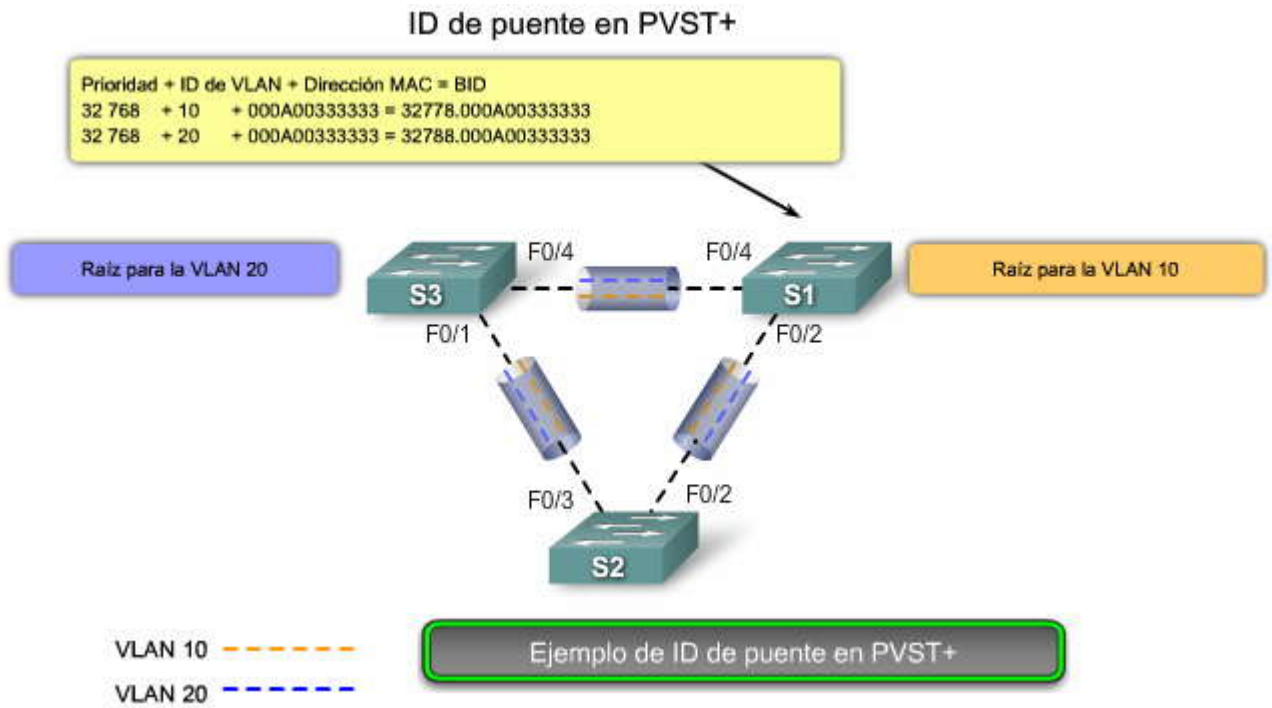
La dirección MAC es lo que identifica unívocamente al BID. Cuando la prioridad y el ID de sistema extensivo se anexan a la dirección MAC del switch, cada VLAN del switch puede representarse por un único BID.

Haga clic en el botón Ejemplo de ID de puente en PVST+ que se muestra en la figura.

En la figura se muestran los valores de prioridad, VLAN y dirección MAC para el switch S1. Se combinan para formar el BID.

Precaución: Si no se ha configurado la prioridad, cada switch posee la misma prioridad predeterminada y la elección del puente raíz para cada VLAN se basa en la dirección MAC. Por lo tanto, para asegurar que se obtendrá el puente raíz deseado, se aconseja asignar un valor de prioridad menor al switch que debería servir como puente raíz.





La tabla muestra la configuración predeterminada de spanning-tree para un switch de la serie Cisco Catalyst 2960. Observe que el modo predeterminado de spanning-tree es PVST+.

Configuración de un switch de manera predeterminada

Característica	Configuración predeterminada
Estado habilitado	Habilitado en la VLAN 1
Modo spanning-tree	PVST+ (PVST+ rápido y MSTP deshabilitados).
Prioridad de switch	32768
Prioridad de puerto en spanning tree (configurable por interfaz)	128
Costo de puerto en spanning tree (configurable por interfaz)	1000 Mb/s: 4, 100 Mb/s: 19, 10 Mb/s: 100
Prioridad de puerto en spanning tree (configurable por VLAN)	128
Costo de puerto en spanning tree (configurable por VLAN)	1000 Mb/s: 4, 100 Mb/s: 19, 10 Mb/s: 100
Temporizadores de spanning-tree	Tiempo de saludo: 2 segundos Tiempo de retraso de envío: 15 segundos Tiempo de antigüedad máxima: 20 segundos Contador de espera de transmisión: 6 BPDU

Configurar PVST+

La topología muestra tres switches con enlaces troncales 802.1Q que los conectan. Se pueden observar dos VLAN, 10 y 20, que cuentan con enlaces troncales entre sí. Esta red no se ha configurado para spanning tree. El objetivo es configurar S3 como puente raíz para la VLAN 20 y S1 como puente raíz para la VLAN 10. El puerto F0/3 de S2 es el puerto en estado de enviar para la VLAN 20 y el puerto en estado de bloqueo para la VLAN 10. El puerto F0/2 de S2 es el puerto en estado de enviar para la VLAN 10 y el puerto en estado de bloqueo para la VLAN 20. Los pasos para configurar PVST+ en este ejemplo son:

Paso 1. Seleccionar los switches que desea como puentes raíz principal y secundario para cada VLAN.

Paso 2. Configurar el switch que será puente principal para una VLAN, por ejemplo: el switch S3 es el puente principal para la VLAN 20.

Paso 3. Configurar el switch que será puente secundario para la otra VLAN, por ejemplo: el switch S3 es el puente secundario para la VLAN 10.

De forma opcional, se configura la prioridad de spanning-tree para que sea lo suficientemente baja como para que sea seleccionado como puente principal.

Haga clic en el botón Puentes raíz principal y secundario de la figura.

Configurar los puentes raíz principales

El objetivo es configurar el switch S3 como puente raíz principal para la VLAN 20 y configurar el switch S1 como puente raíz principal para la VLAN 10. Para configurar un switch para que se convierta en puente raíz para una VLAN específica, utilice el comando spanning-tree vlan vlan-ID root primary en modo de configuración global. Recuerde que se comienza con una red que no se ha configurado con spanning tree, así que se supone que todos los switches se encuentran en su configuración predeterminada. En este ejemplo, el switch S1, que cuenta con las VLAN 10 y 20 habilitadas, retiene su prioridad de STP predeterminada.

Configurar los puentes raíz secundarios

Una raíz secundaria es un switch que puede convertirse en puente raíz para una VLAN en el caso de falla en el puente raíz principal. Para configurar un switch como puente raíz secundario, utilice el comando spanning-tree vlan vlan-ID root secondary en modo de configuración global. Si se tiene en cuenta que los otros puentes de la VLAN retienen su prioridad de STP predeterminada, este switch se convierte en el puente raíz en el caso de producirse una falla en el puente raíz principal. Este comando puede ejecutarse en más de un switch para configurar varios puentes raíz de respaldo.

La gráfica muestra la sintaxis del comando del IOS de Cisco para especificar a S3 como puente raíz principal para la VLAN 20 y como puente raíz secundario para la VLAN 10. Además, el switch S1 se convierte en el puente raíz principal para la VLAN 10 y en el puente raíz secundario para la VLAN 20. Esta configuración permite el balanceo de carga en spanning tree, donde el tráfico de la VLAN 10 pasa a través del switch S1 y el tráfico de la VLAN 20 pasa a través del switch S3.

Haga clic en el botón Prioridad de switch en PVST+ que se muestra en la figura.

Prioridad de switch en PVST+

Anteriormente en este capítulo se aprendió que la configuración predeterminada utilizada para spanning tree es la adecuada para la mayoría de las redes. Esto también es cierto para PVST+ de Cisco. Existen varias formas de ajustar PVST+. La explicación de la forma en que se ajusta la implementación de PVST+ excede el alcance de este curso. Sin embargo, se puede establecer la prioridad de switch para la instancia de spanning-tree especificada. Esta configuración afecta a la posibilidad de que el switch sea seleccionado como switch raíz. Un valor menor provoca el aumento de la probabilidad de que el switch sea seleccionado. Este rango oscila entre 0 y 61 440 en incrementos de 4096. Por ejemplo: un valor de prioridad válido es 4096 x 2 = 8 192. Todos los demás valores se rechazan.

Los ejemplos muestran la sintaxis del comando del IOS de Cisco.

Haga clic en el botón Verificar que se muestra en la figura.

El comando del modo EXEC privilegiado show spanning tree active muestra los detalles de la configuración de spanning-tree sólo para las interfaces activas. El resultado que se muestra es para el switch S1 configurado con PVST+. Existe una gran cantidad de parámetros del comando del IOS de Cisco asociados con el comando show spanning tree. Para obtener una descripción completa, visite:
http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_37_se/command/reference/cli2.html#wpxref47293.

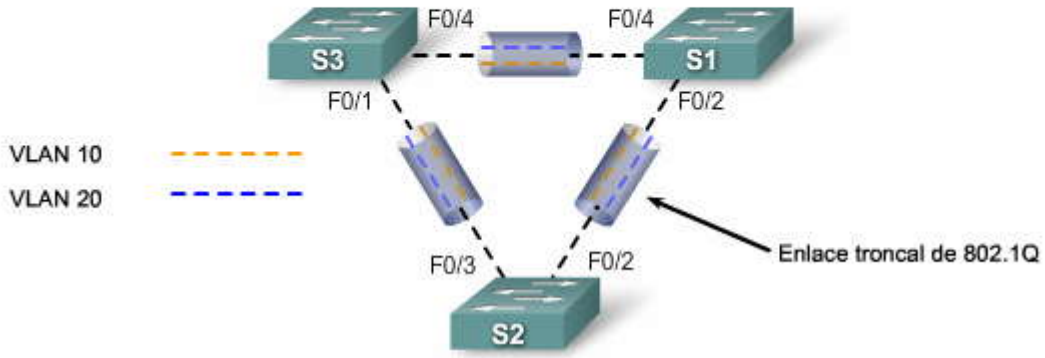
Haga clic en el botón show run de la figura.

Puede ver en el resultado que la prioridad para la VLAN 10 es 4096, la menor de las tres prioridades de la VLAN. Esta configuración de prioridades asegura que este switch sea el puente raíz principal para la VLAN 10.

Configurar PVST+

Puente raíz principal para VLAN 20
Puerto raíz secundario para VLAN 10

Puente raíz principal para VLAN 10
Puente raíz secundario para VLAN 20




```
S3(config)#spanning-tree vlan 20 root primary
```

Este comando obliga al switch S3 a ser la raíz principal para VLAN 20.

```
S3(config)#spanning-tree vlan 10 root secondary
```

Este comando obliga al switch S3 a ser la raíz secundaria para VLAN 10.

Puentes raíz principal y secundario

```
S1(config)#spanning-tree vlan 10 root primary
```

Este comando obliga al switch S1 a ser la raíz principal para VLAN 10.

```
S1(config)#spanning-tree vlan 20 root secondary
```

Este comando obliga al switch S1 a ser la raíz secundaria para VLAN 20.

```
S3(config)#spanning-tree vlan 20 priority 4096
```

Este comando establece la prioridad para el switch S3 para que sea la menor posible, lo que hace que sea más probable que el switch S3 se convierta en raíz principal para VLAN 20.

Prioridad de switch en PVST+

```
S1(config)#spanning-tree vlan 10 priority 4096
```

Este comando establece la prioridad para el switch S1 para que sea la menor posible, lo que hace que sea más probable que el switch S1 se convierta en raíz principal para VLAN 10.

```
S1#show spanning-tree active
<output omitted>
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     0019.aa9e.b000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    4106   (priority 4096 sys-id-ext 10)
              Address     0019.aa9e.b000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
<output omitted>
```

Verificar

```
S1#show run
Building configuration...

Current configuration : 1595 bytes
!
version 12.2
<output omitted>
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
<output omitted>
```

5.4.3 RSTP.-

¿Qué es RSTP?

RSTP (IEEE 802.1w) es una evolución del estándar 802.1D. Principalmente, la terminología de 802.1w STP sigue siendo la misma que la del IEEE 802.1D STP. La mayoría de los parámetros no se modifican, de modo que los usuarios familiarizados con STP puedan configurar rápidamente el nuevo protocolo.

En la figura, la red muestra un ejemplo de RSTP. El switch S1 es el puente raíz con dos puertos designados en estado de enviar. RSTP admite un nuevo tipo de puerto. El puerto F0/3 del switch S2 es un puerto alternativo en estado de descarte. Observe que no existen puertos bloqueados. RSTP no posee el estado de puerto de bloqueo. RSTP define los estados de puertos como de descarte, aprender o enviar. Aprenderá más acerca de tipos y estados de puertos posteriormente en este capítulo.

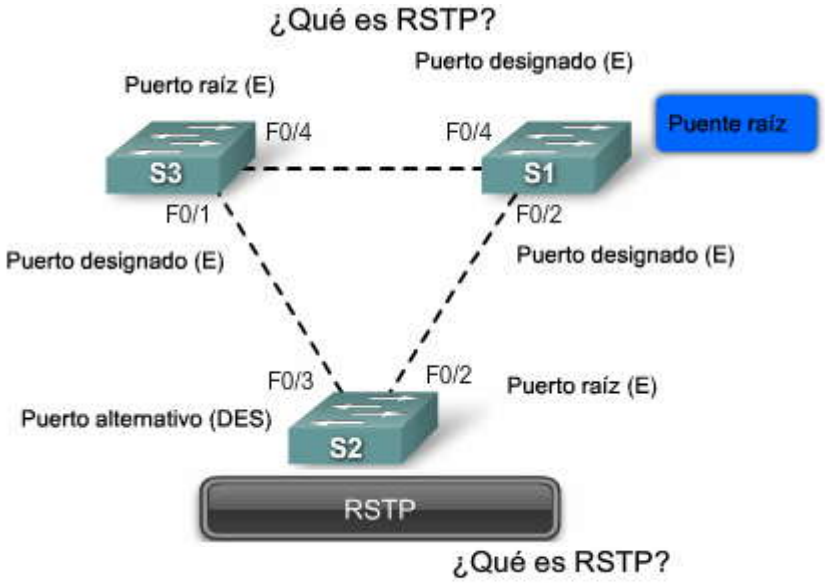
Haga clic en el botón Características de RSTP en la figura.

Características de RSTP

RSTP aumenta la velocidad de recálculo del spanning tree cuando cambia la topología de la red de la Capa 2. RSTP puede lograr una convergencia mucho más rápida en una red configurada de forma adecuada, a veces sólo en unos pocos cientos de milisegundos. RSTP redefine los tipos de puertos y sus estados. Si un puerto se configura para ser alternativo o de respaldo, puede cambiar de manera automática al estado de enviar sin esperar la convergencia de la red. A continuación se describen brevemente las características de RSTP:

RSTP es el protocolo preferido para evitar los bucles de Capa 2 en un entorno de red conmutada. Muchas de las diferencias se informaron en las mejoras de 802.1D propiedad de Cisco. Estas mejoras, como las BPDU que transportan y envían información acerca de las funciones de los puertos a los switches vecinos, no requieren configuración adicional y por lo general poseen un mejor rendimiento que las versiones anteriores propiedad de Cisco. Ahora son transparentes y están integradas al funcionamiento del protocolo.
Las mejoras al 802.1D propiedad de Cisco, como UplinkFast y BackboneFast, no son compatibles con RSTP.
RSTP (802.1w) reemplaza a STP (802.1D) a la vez que mantiene la compatibilidad retrospectiva. Mucha de la terminología de STP permanece y la mayoría de los parámetros no presentan cambios. Además, 802.1w puede volver a la versión 802.1D para inter-operar con switches antiguos por puerto. Por ejemplo: el algoritmo spanning-tree de RSTP selecciona un puente raíz exactamente de la misma forma que 802.1D.
RSTP mantiene el mismo formato de BPDU que IEEE 802.1D, excepto que el campo de versión se establece en 2 para indicar que es RSTP y todos los campos de señaladores utilizan 8 bits. Las BPDU en RSTP se explican más adelante.

RSTP puede confirmar de manera activa que un puerto puede sufrir una transición segura al estado de enviar sin depender de ninguna configuración de temporizadores.



Características de RSTP:

- Es el protocolo preferido para evitar bucles en la Capa 2 en una red conmutada.
- Integra las mejoras propiedad de Cisco de manera transparente, como las BPDU que envían propuestas y acuerdos a los switches vecinos.
- Posee mejor rendimiento que las anteriores mejoras propiedad de Cisco.
- No es compatible con algunas mejoras propiedad de Cisco, como UplinkFast y BackboneFast.
- Define estados y funciones de puerto distintos.
- Es compatible hacia atrás con 802.1D.
- Mantuvo la mayoría de los parámetros sin cambios.
- Posee el mismo formato de BPDU que IEEE 802.1D.
- No requiere los temporizadores de 802.1D.

Características de RSTP

BPDU en RSTP

RSTP (802.1w) utiliza BPDU tipo 2, versión 2, de manera que un puente en RSTP puede comunicar a 802.1D en cualquier enlace compartido o con cualquier switch que ejecute 802.1D. RSTP envía BPDU y completa el byte señalizador de una manera ligeramente distinta que en 802.1D:

La información de protocolo puede expirar de forma inmediata en un puerto si no se reciben saludos durante tres tiempos de saludo consecutivos, 6 segundos de manera predeterminada, o si expira el temporizador de antigüedad máxima.
Debido a que las BPDU se utilizan como un mecanismo de actividad, tres BPDU perdidas de forma consecutiva indican la pérdida de la conectividad entre un puente y su raíz vecino o puente designado. La rápida expiración de la información permite que las fallas se detecten muy rápidamente.

Nota: Al igual que STP, un puente en RSTP envía una BPDU con su información actual en todos los períodos de tiempo de saludo (2 segundos de manera predeterminada), aún si el puente de RSTP no recibe ninguna BPDU del puente raíz.

RSTP utiliza el byte de señalización de la BPDU versión 2 como se muestra en la figura:

Los bits 0 y 7 se utilizan para notificación de cambio en la topología y acuse de recibo de la misma forma que en 802.1D.
Los bits 1 y 6 se utilizan para el proceso de Acuerdo de propuesta (para la convergencia rápida).
Los bits del 2 al 5 contienen la función y el estado del puerto que origina la BPDU.
Los bits 4 y 5 se utilizan para codificar la función del puerto mediante un código de 2 bits.

BPDU en RSTP

BPDU en RSTP Versión 2

Campo	Longitud en bytes
ID de protocolo=0x0000	2
ID de versión de protocolo= 0x02	1
Tipo de BPDU= 0x02	1
Señaladores	1
ID de raíz	8
Costo de la ruta raíz	4
ID de puente	8
ID del puerto	2
Antigüedad del mensaje	2
Antigüedad máxima	2
Tiempo de saludo	2
Retraso de envío	2

Campo señalador

Bit del campo	Bit
Cambio en la topología	0
Propuesta	1
Función de puerto Puerto desconocido Puerto alternativo o de respaldo Puerto raíz Puerto designado	2-3 00 01 10 11
Aprender	4
Enviar	5
Acuerdo	6
Acuse de recibo de cambio de topología	7

5.4.4 PUERTOS DE EXTREMO.-

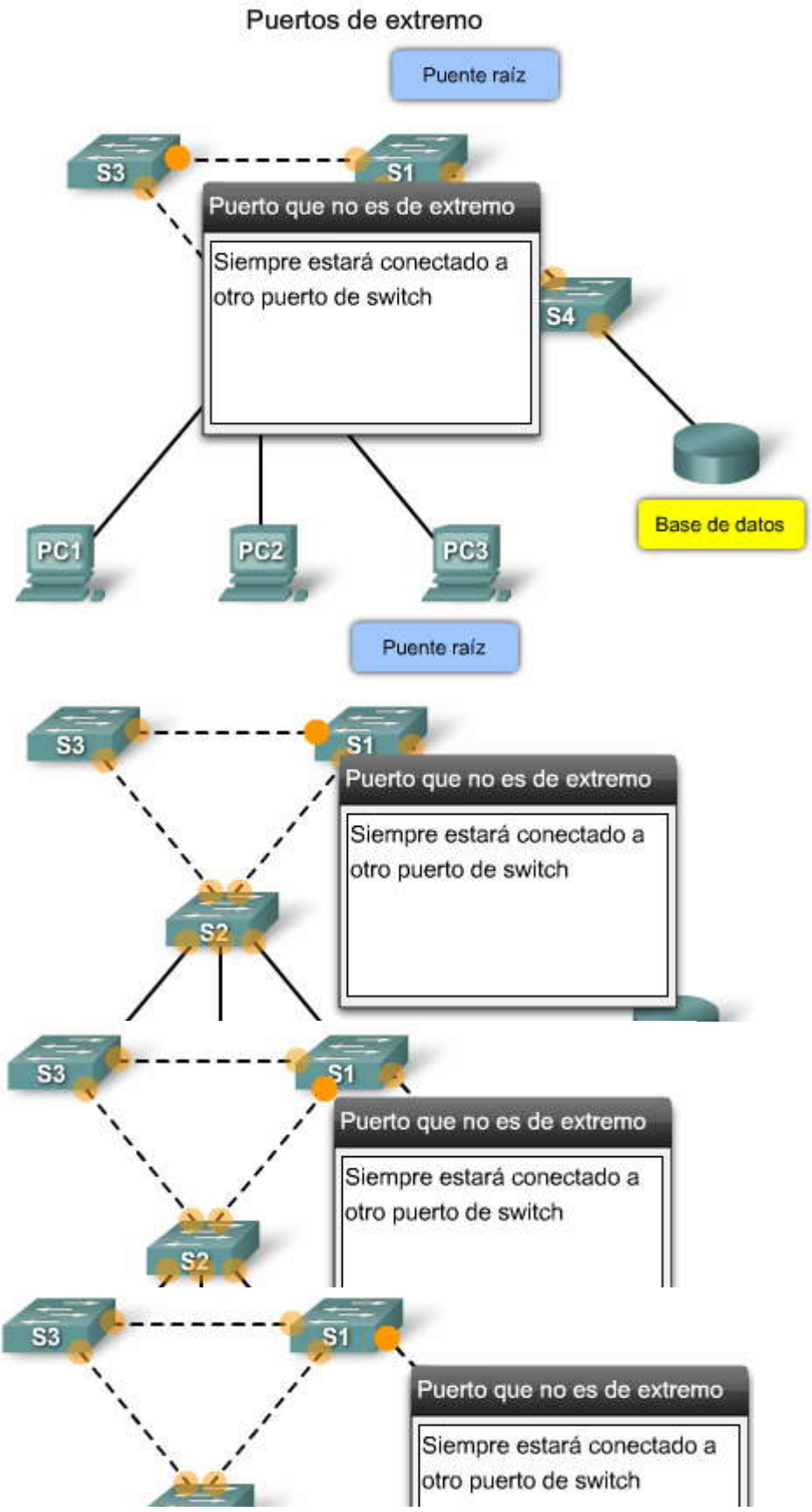
Puertos de extremo

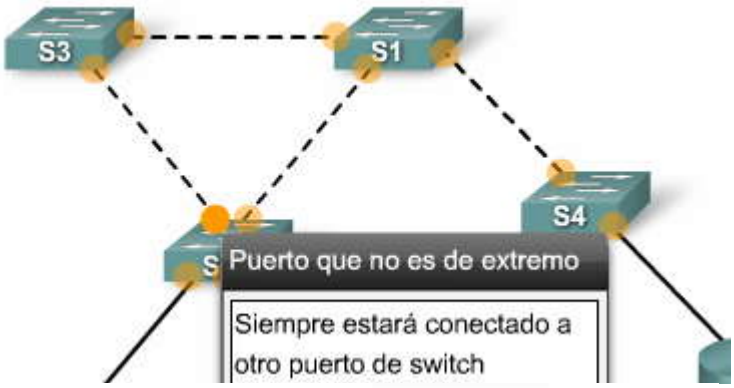
Un puerto de extremo en RSTP es un puerto de switch que nunca se conecta con otro dispositivo de switch. Sufre la transición al estado de enviar de manera inmediata cuando se encuentra habilitado.

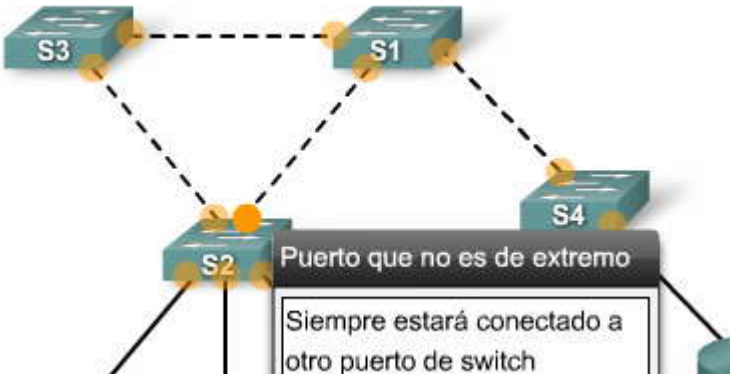
El concepto de puerto de extremo es muy conocido entre los usuarios de spanning-tree de Cisco, ya que corresponde a la función de PortFast en la que todos los puertos conectados directamente a estaciones finales anticipan que no hay dispositivos de switch conectados a los mismos. Los puertos de PortFast sufren la transición al estado de enviar de STP de forma inmediata, lo que permite evitar el uso de los estados de escuchar y aprender, que consumen tiempo. Ni los puertos de extremo ni los puertos con PortFast habilitado generan cambios de topología cuando el puerto experimenta una transición al estado habilitado o deshabilitado.

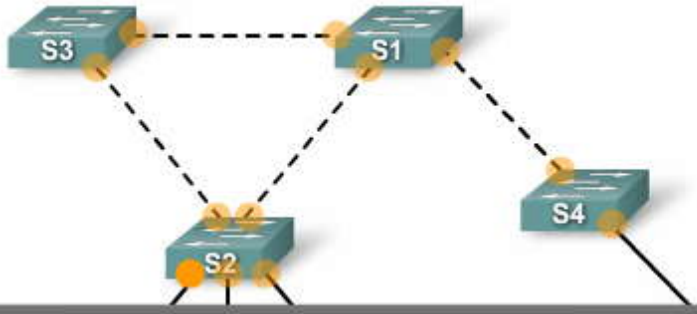
A diferencia de PortFast, un puerto de extremo de RSTP que recibe una BPDU pierde su estado de puerto de extremo de forma inmediata y se convierte en un puerto normal de spanning-tree.

La implementación de RSTP de Cisco mantiene la palabra clave PortFast mediante el comando **spanning-tree portfast** para la configuración del puerto de extremo. Esto permite que la transición de red total a RSTP sea más transparente. La configuración de un puerto de extremo para que se conecte a otro switch puede tener implicancias negativas para RSTP cuando se encuentra en estado sincronizado, ya que puede generarse un bucle temporal, lo que posiblemente provocará una demora en la convergencia de RSTP debido a la contención de BPDU con el tráfico de bucles.


Puertos de extremo
Puente raíz
S3
S1
Puerto que no es de extremo
Siempre estará conectado a otro puerto de switch
S4
Base de datos
PC1
PC2
PC3
Puente raíz
S3
S1
Puerto que no es de extremo
Siempre estará conectado a otro puerto de switch
S2
S3
S1
Puerto que no es de extremo
Siempre estará conectado a otro puerto de switch
S2
S3
S1
Puerto que no es de extremo
Siempre estará conectado a otro puerto de switch

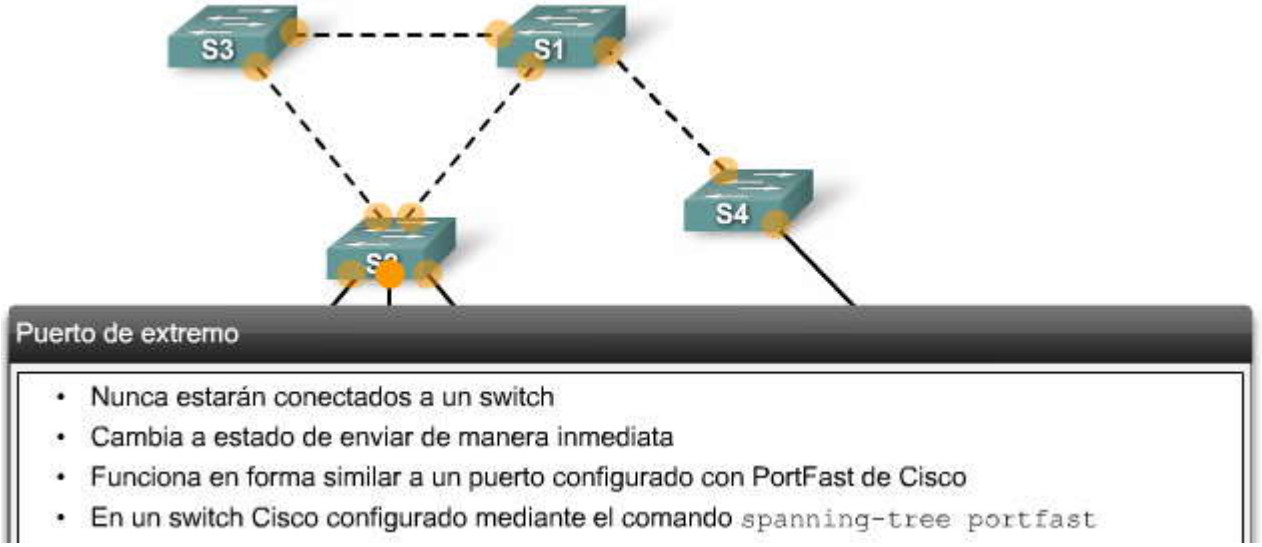


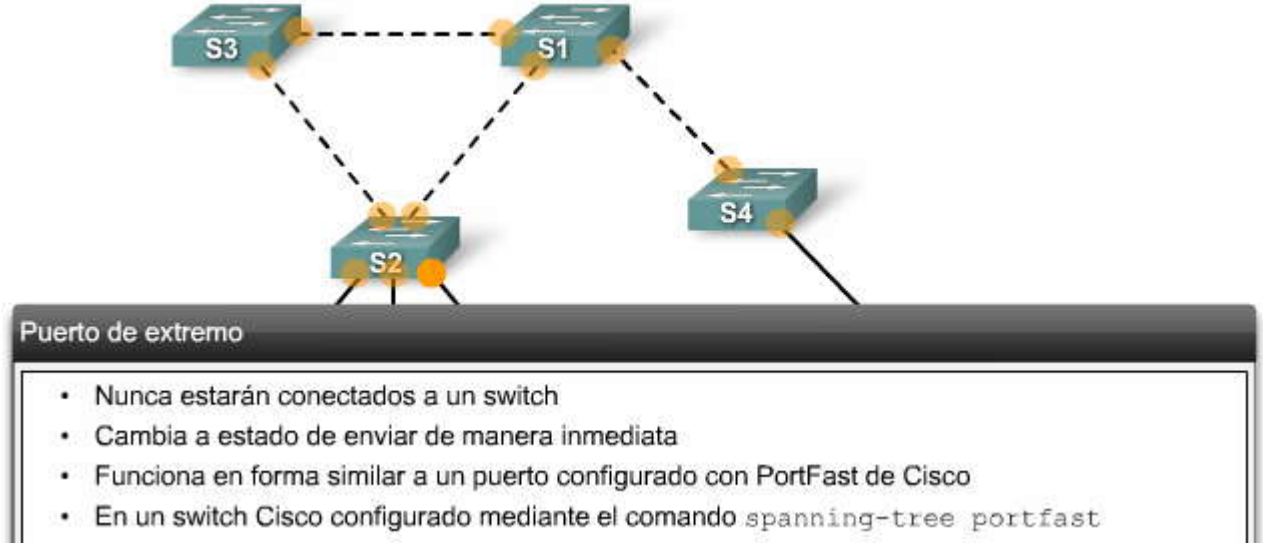




Puerto de extremo

- Nunca estarán conectados a un switch
- Cambia a estado de enviar de manera inmediata
- Funciona en forma similar a un puerto configurado con PortFast de Cisco
- En un switch Cisco configurado mediante el comando `spanning-tree portfast`





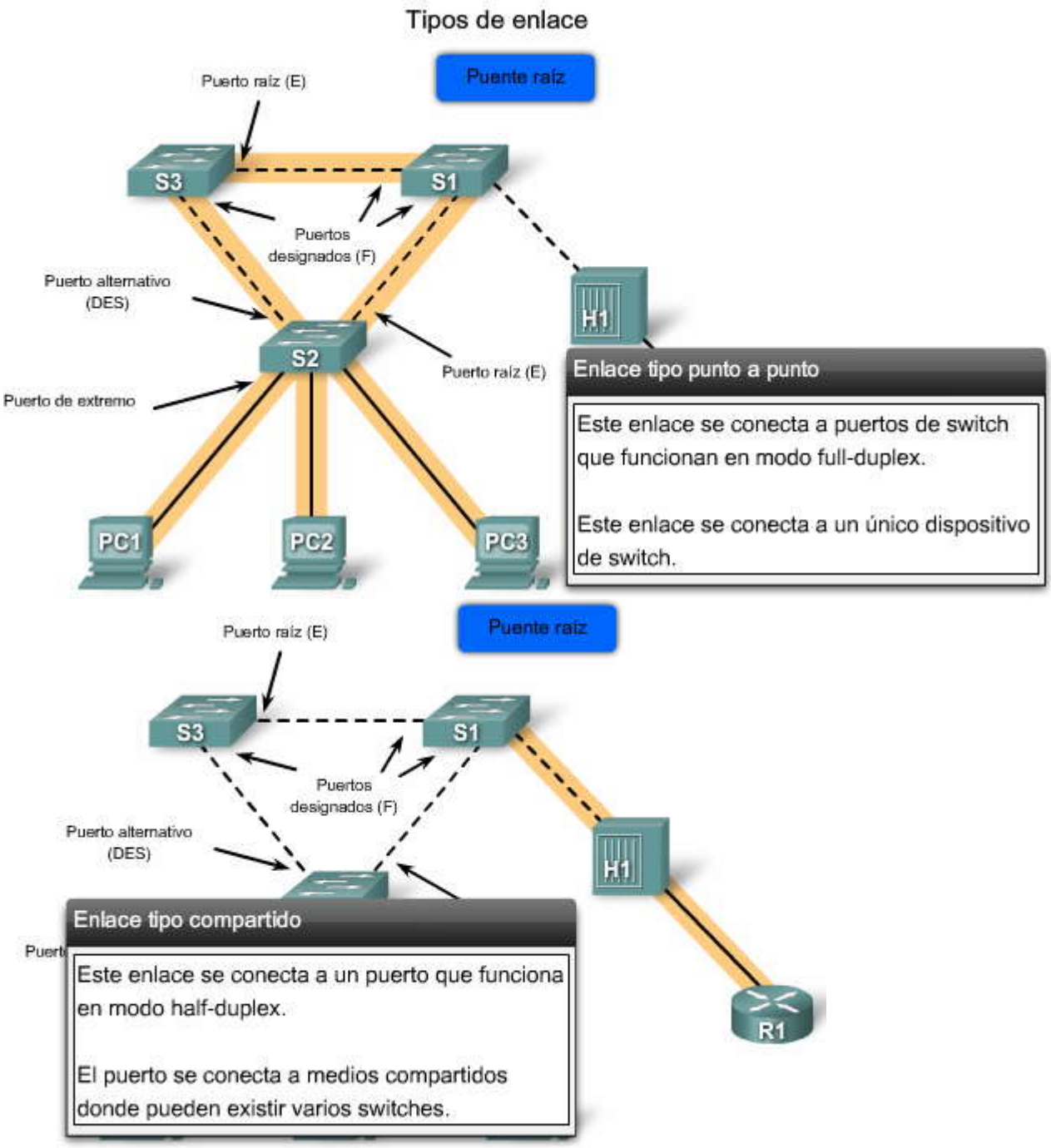
5.4.5 TIPOS DE ENLACE.-

Tipos de enlaces

El tipo de enlace proporciona una categorización para cada puerto que participa de RSTP. El tipo de enlace puede predeterminar la función activa que cumple el puerto mientras espera por la transición inmediata al estado de enviar si se satisfacen ciertas condiciones. Estas condiciones son distintas para los puertos de extremo y para los puertos que no son de extremo. Los puertos que no son de extremo se categorizan en dos tipos de enlaces, punto a punto y compartido. El tipo de enlace se determina de forma automática pero puede sobrescribirse con una configuración de puerto explícita.

Los puertos de extremo, equivalentes a los puertos con PortFast habilitado y los enlaces punto a punto son los candidatos para la transición rápida al estado de enviar. Sin embargo, antes de considerar el parámetro tipo de enlace,RSTP debe determinar la función del puerto. Aprenderá más acerca de las funciones de puertos a continuación, pero por ahora tenga en cuenta lo siguiente:

Los puertos raíz no utilizan el parámetro tipo de enlace. Los puertos raíz son capaces de realizar una transición rápida al estado de enviar siempre que el puerto se encuentre sincronizado.
Los puertos alternativos y de respaldo no utilizan el parámetro tipo de enlace en la mayoría de los casos.
Los puertos designados son los que más utilizan el parámetro tipo de enlace. La transición rápida al estado de enviar para el puerto designado se produce sólo si el parámetro tipo de enlace indica un enlace punto a punto.



5.4.6 ESTADOS Y FUNCIONES DE LOS PUERTOS EN RSTP.-

Estados de los puertos en RSTP

RSTP proporciona una convergencia rápida después de una falla o durante el restablecimiento de un switch, puerto de switch o enlace. Un cambio de topología en RSTP produce una transición en los estados de puertos de switch adecuados a través de intercambios de señales explícitas o del proceso y sincronización de propuesta y acuerdo. Aprenderá más acerca del proceso de propuesta y acuerdo más adelante.

Con RSTP, la función de un puerto es independiente del estado del mismo. Por ejemplo: un puerto designado puede encontrarse en estado de descarte de forma temporal, aun si su estado final es el de enviar. La figura muestra los tres posibles estados de puertos en RSTP: descarte, aprender y enviar.

Haga clic en el botón Descripciones que se muestra en la figura.

La tabla de la figura describe las características de cada uno de los tres estados de puertos en RSTP. En todos los estados, el puerto acepta y procesa las tramas de BPDU.

Haga clic en el botón Puertos de STP y RSTP que se muestra en la figura.

La tabla de la figura compara los estados de puertos en STP y en RSTP. Recuerde que en los estados de puertos de STP de bloqueo, escuchar y deshabilitado no se envían tramas. Estos estados de puertos se han unido en el estado de puerto de descarte en RSTP.

Estados de los puertos en RSTP

Estado del puerto	Acción
Descarte	Este estado puede verse tanto en la topología activa estable como durante la sincronización y los cambios de topología. El estado de descarte evita el envío de tramas de datos, además de "romper" la continuidad de un bucle de la Capa 2.
Aprender	Este estado puede verse tanto en la topología activa estable como durante la sincronización y los cambios de topología. El estado aprender acepta tramas de datos para llenar la tabla MAC en un intento por limitar la transmisión de tramas de unicast desconocidas.
Enviar	Este estado sólo puede verse en las topologías activas estables. Los puertos de switch en estado enviar determinan la topología. Después de un cambio de topología, o durante la sincronización, el envío de tramas de datos se produce sólo después del proceso de propuesta y acuerdo.

Descripciones

Estados de los puertos en RSTP

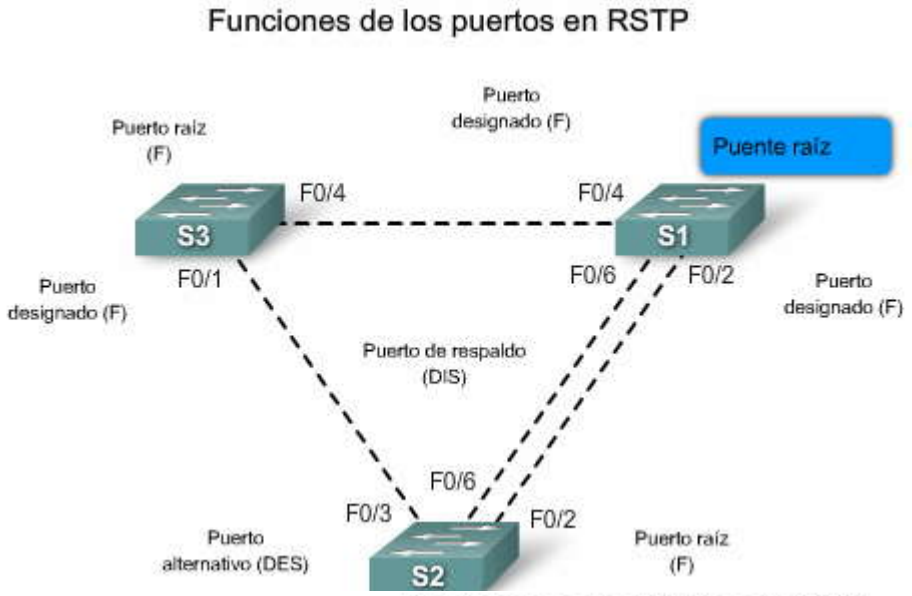
Estado de puerto operativo	Estado del puerto en STP	Estado del puerto en RSTP
Habilitado	Bloqueo	Descarte
Habilitado	Escuchar	Descarte
Habilitado	Aprender	Aprender
Habilitado	Enviar	Enviar
Deshabilitado	Deshabilitado	Descarte

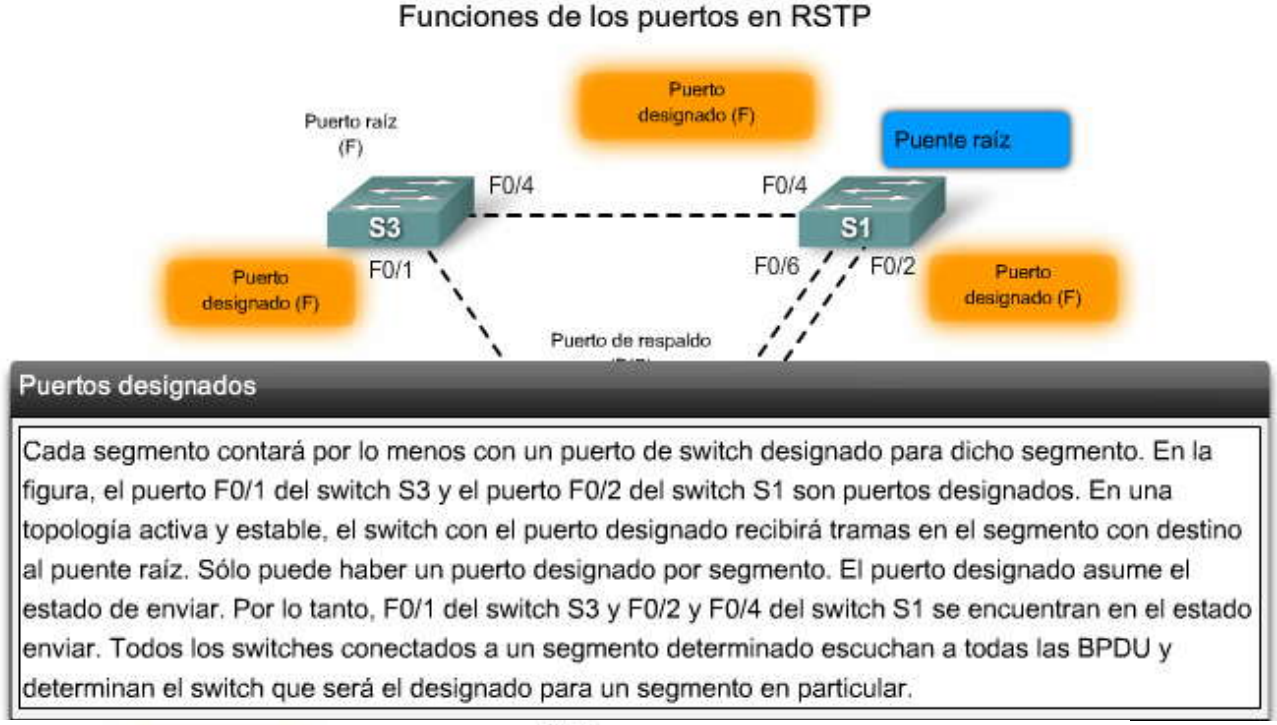
Puertos en STP y en RSTP

Funciones de los puertos en RSTP

La función del puerto define el objetivo principal de un puerto de switch y la forma en que gestiona las tramas de datos. Las funciones y los estados de los puertos pueden experimentar transiciones de forma independiente.La creación de funciones de puertos adicionales permite que RSTP defina un puerto de switch de reserva antes de una falla o un cambio de topología. El puerto alternativo pasa al estado de enviar si existe una falla en el puerto designado para el segmento.

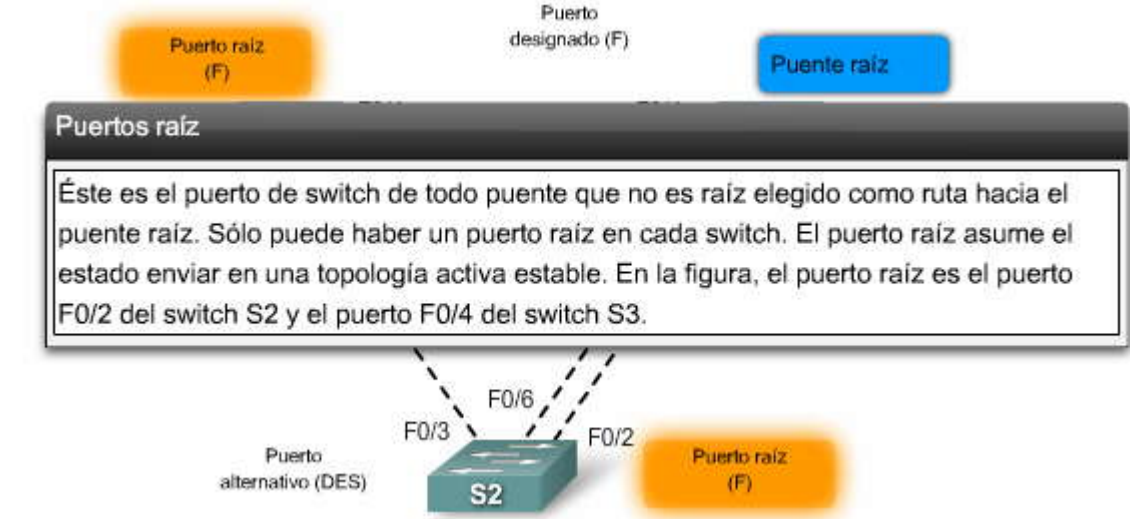
Desplace el mouse por las funciones de los puertos en la figura para aprender más acerca de cada función del puerto en RSTP.





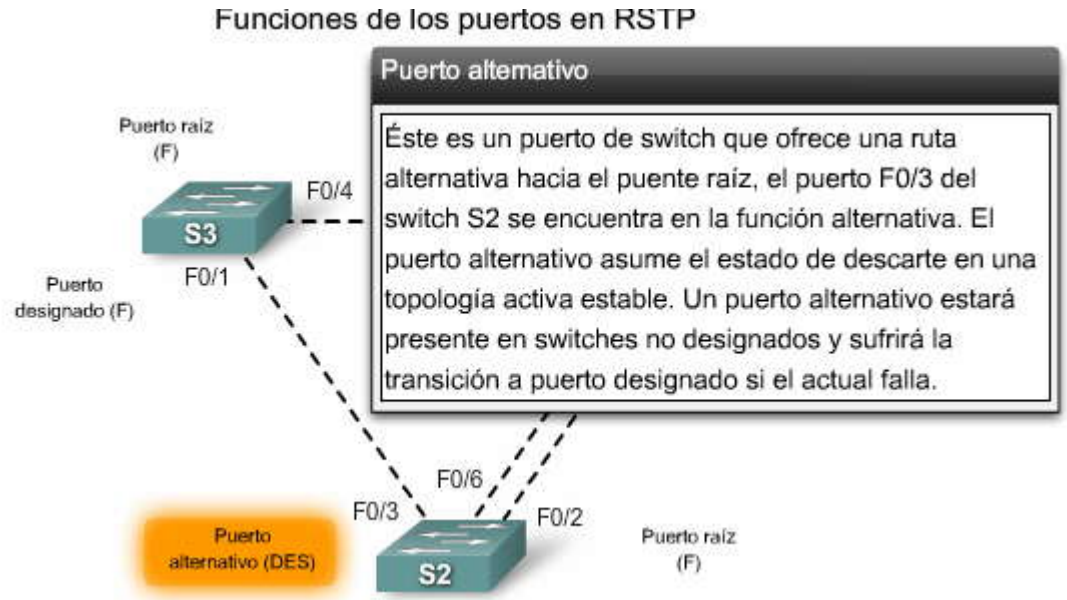
Puertos designados

Cada segmento contará por lo menos con un puerto de switch designado para dicho segmento. En la figura, el puerto F0/1 del switch S3 y el puerto F0/2 del switch S1 son puertos designados. En una topología activa y estable, el switch con el puerto designado recibirá tramas en el segmento con destino al puente raíz. Sólo puede haber un puerto designado por segmento. El puerto designado asume el estado de enviar. Por lo tanto, F0/1 del switch S3 y F0/2 y F0/4 del switch S1 se encuentran en el estado enviar. Todos los switches conectados a un segmento determinado escuchan a todas las BPDU y determinan el switch que será el designado para un segmento en particular.



Puertos raíz

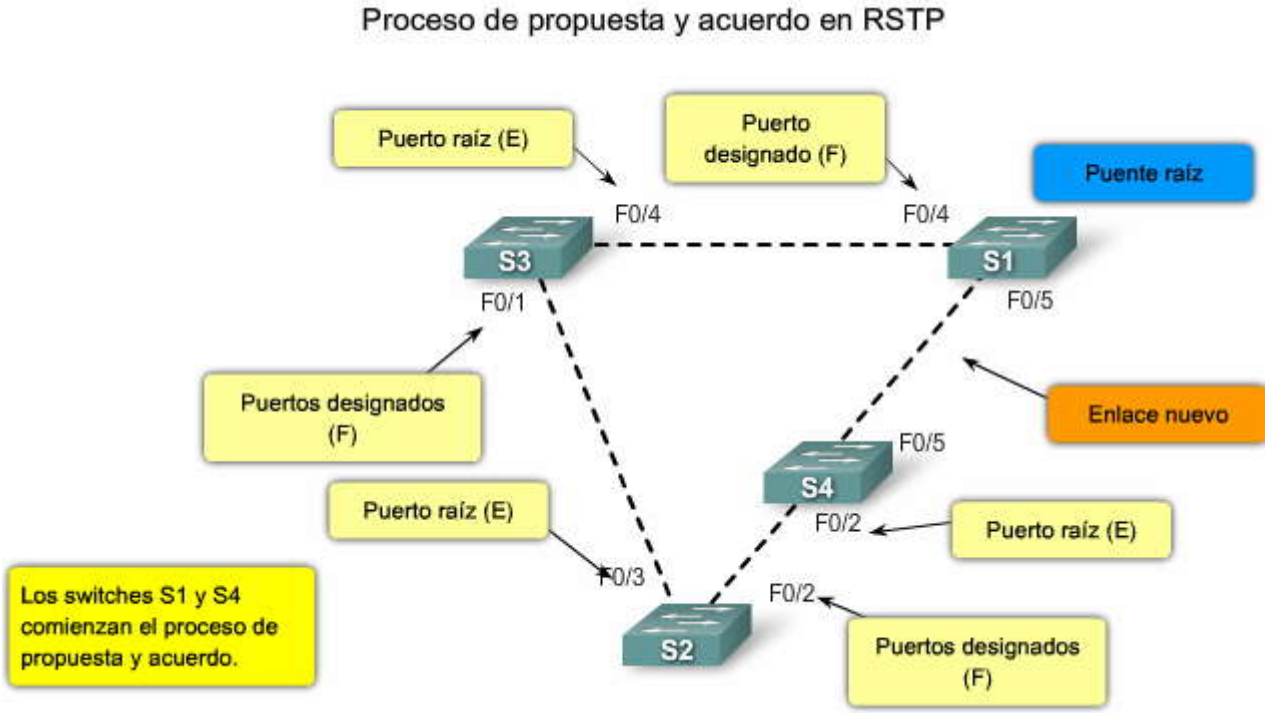
Éste es el puerto de switch de todo puente que no es raíz elegido como ruta hacia el puente raíz. Sólo puede haber un puerto raíz en cada switch. El puerto raíz asume el estado enviar en una topología activa estable. En la figura, el puerto raíz es el puerto F0/2 del switch S2 y el puerto F0/4 del switch S3.

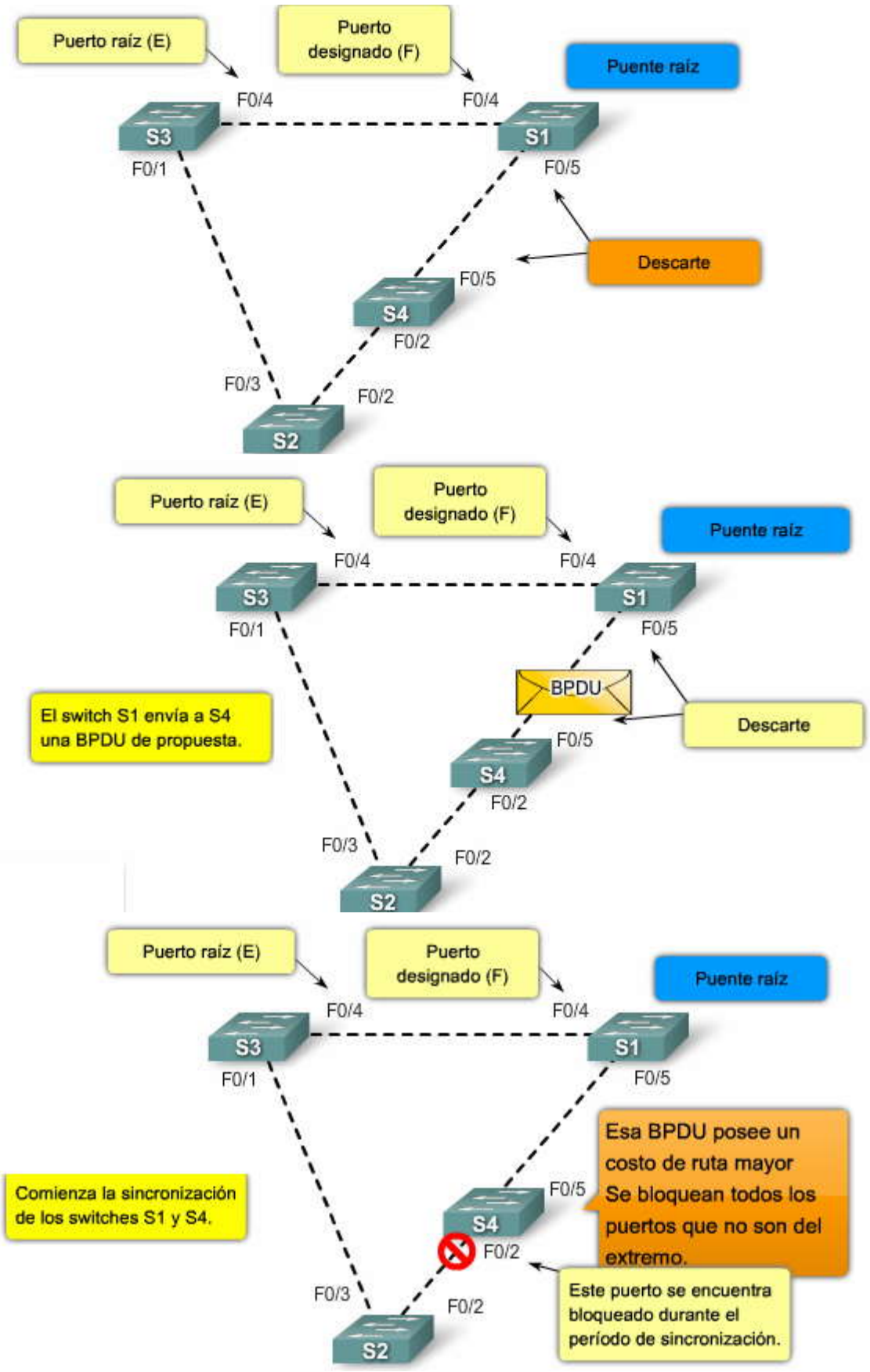


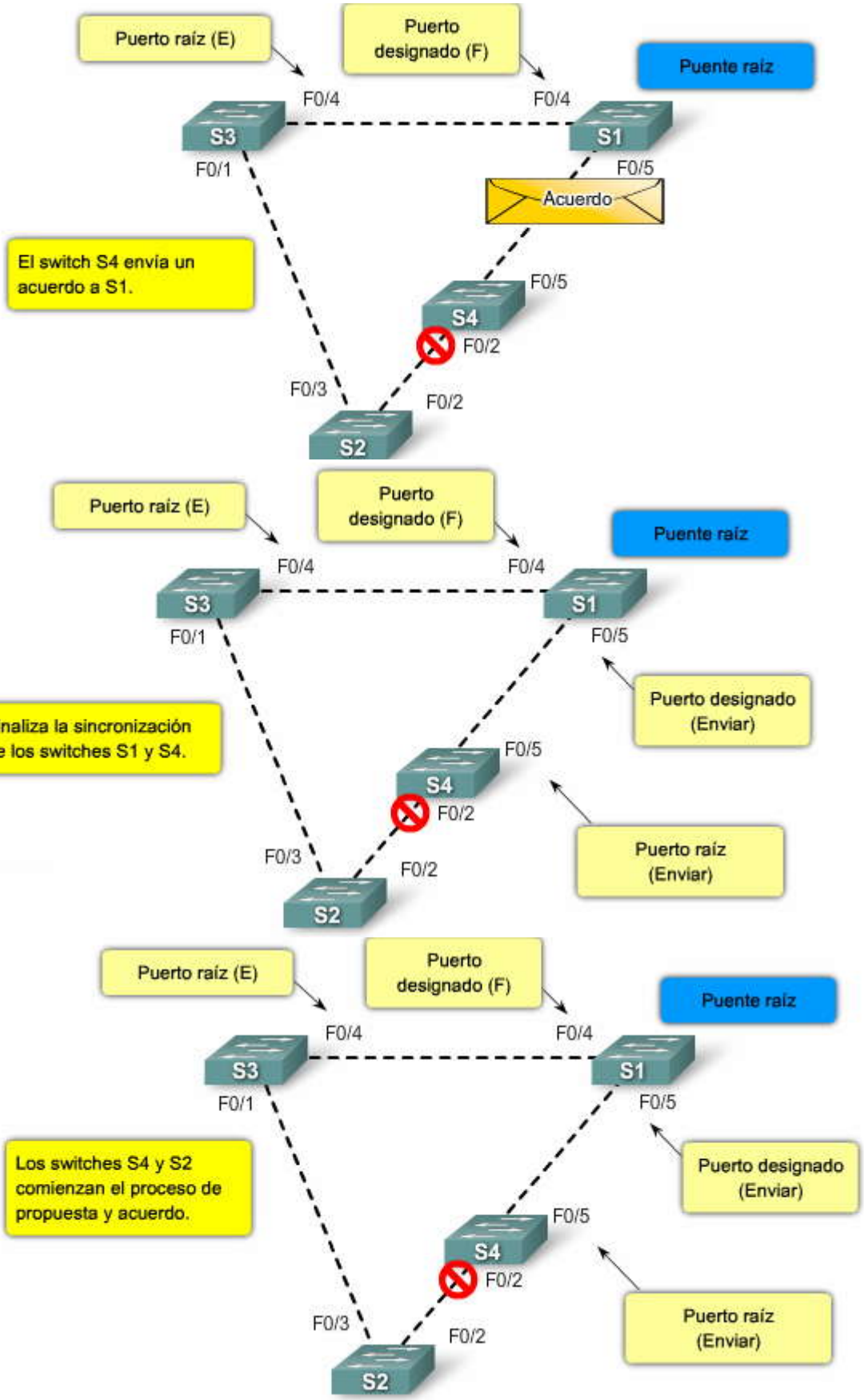
Proceso de propuesta y acuerdo en RSTP

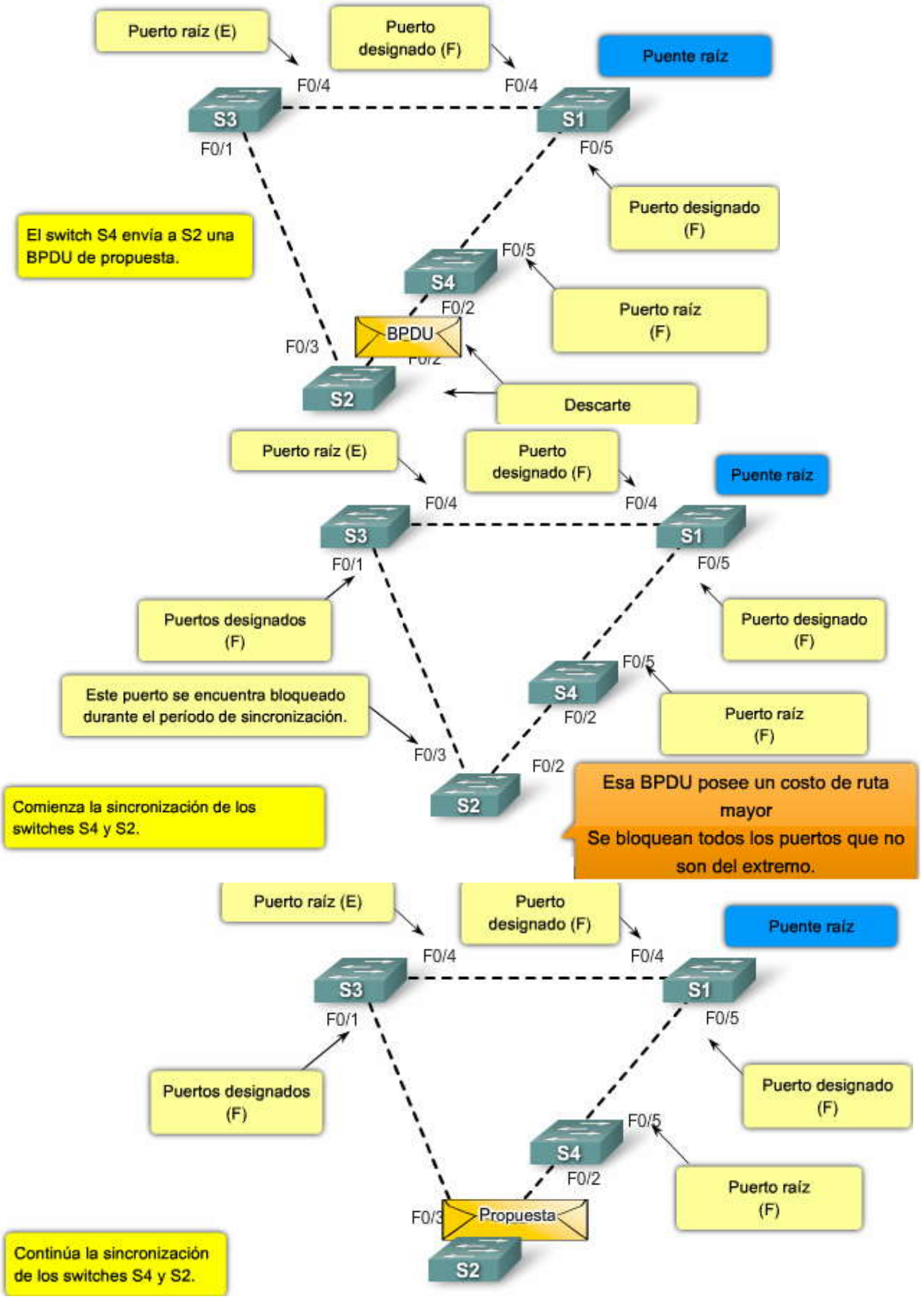
En STP IEEE 802.1D, una vez que el puerto fue seleccionado por spanning tree para convertirse en puerto designado, debe esperar el equivalente a dos veces el retraso de envío antes de pasar el puerto al estado de enviar. RSTP agiliza el proceso de recálculo de forma significativa después de un cambio de topología, ya que converge enlace por enlace y no depende de que los temporizadores expiren antes de que los puertos experimenten la transición. La transición rápida al estado de enviar sólo puede lograrse en los puertos de extremo y en los enlaces punto a punto. En RSTP, esta condiciónse corresponde con el puerto designado en estado de descarte.

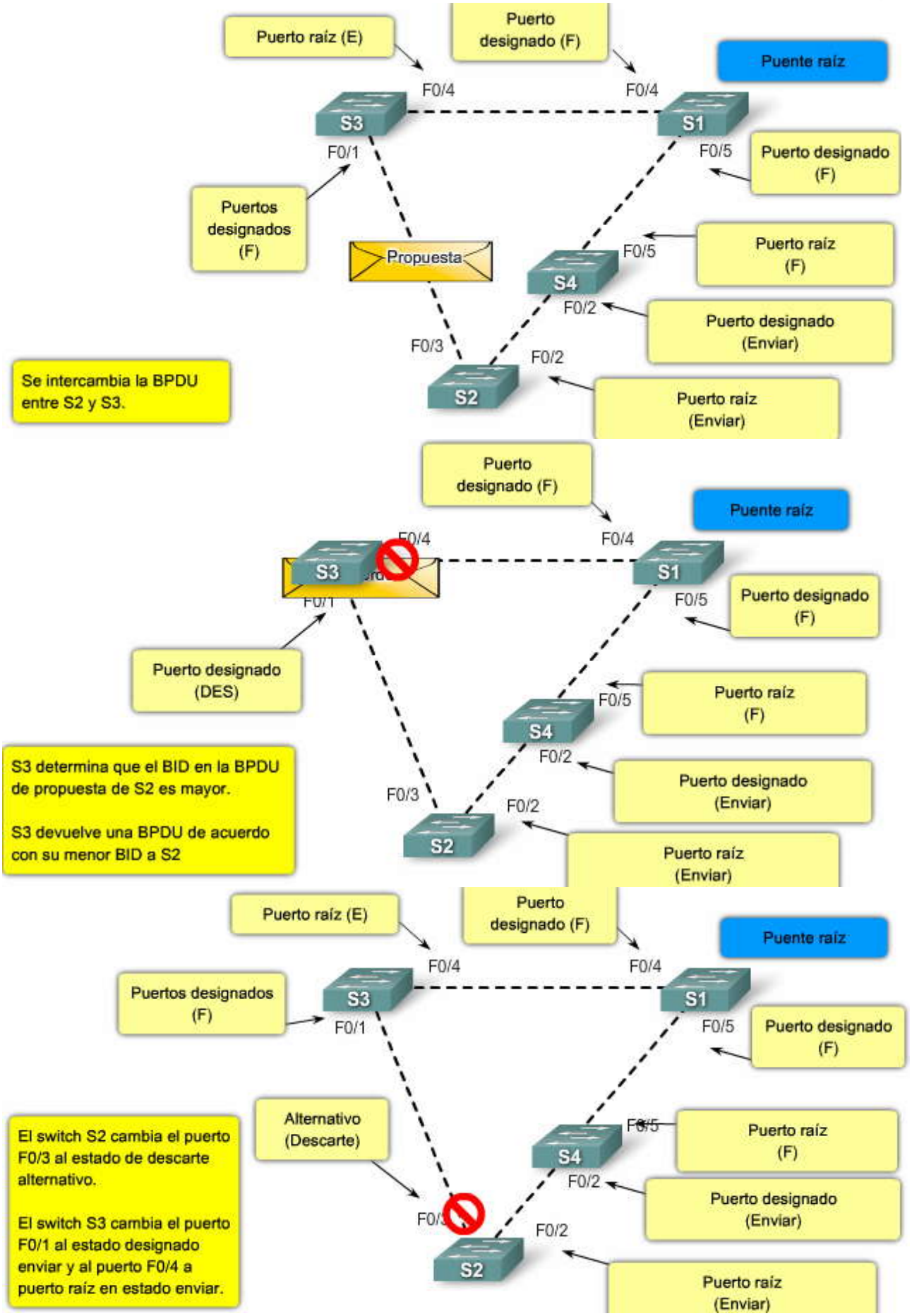
Haga clic en el botón Reproducir de la figura para iniciar la animación.

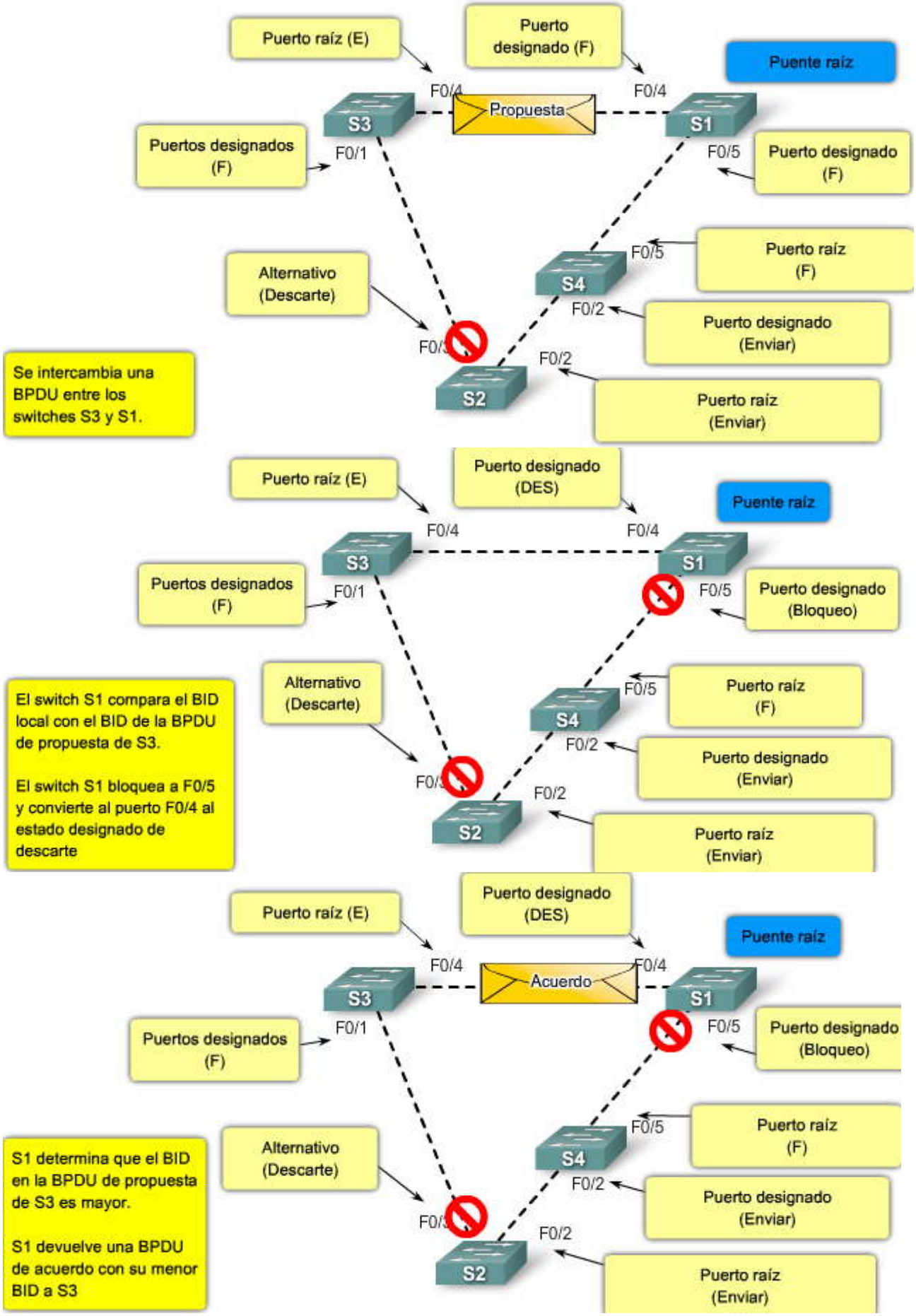


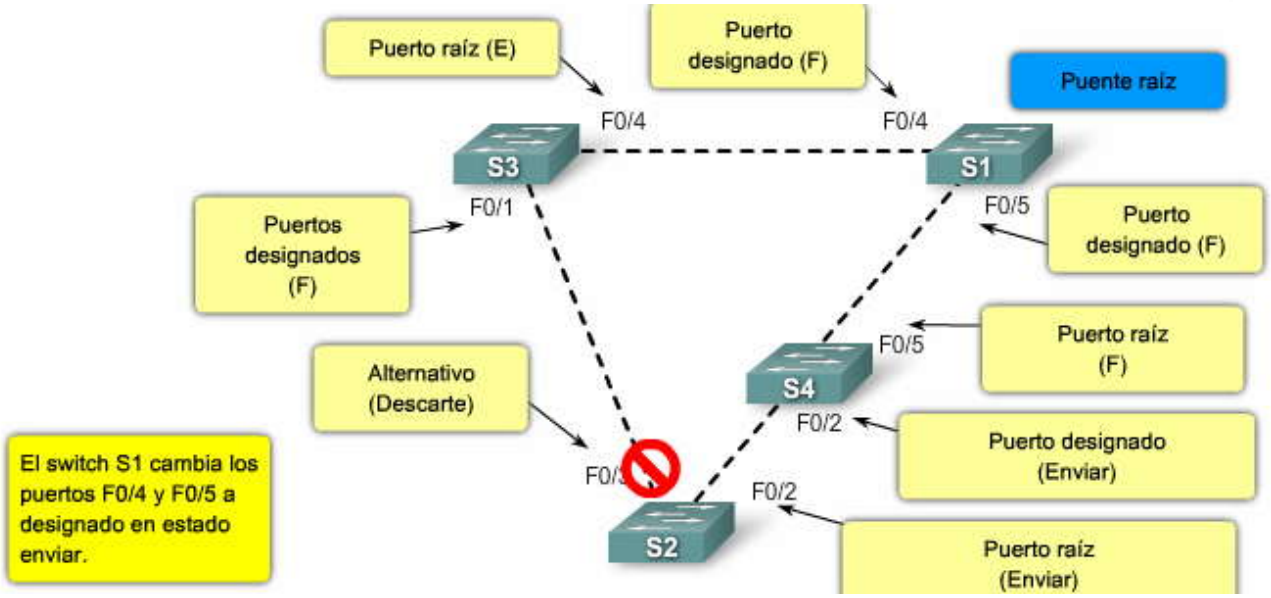

Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
Descarte
F0/5
S4
F0/2
F0/3
F0/2
S2
Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
BPDU
El switch S1 envía a S4 una BPDU de propuesta.
Descarte
F0/5
S4
F0/2
F0/3
F0/2
S2
Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
Esa BPDU posee un costo de ruta mayor
Se bloquean todos los puertos que no son del extremo.
Comienza la sincronización de los switches S1 y S4.
F0/5
S4
F0/2
Este puerto se encuentra bloqueado durante el período de sincronización.
F0/3
F0/2
S2


Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
Acuerdo
El switch S4 envía un acuerdo a S1.
F0/5
S4
F0/2
F0/3
F0/2
S2
Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
Puerto designado (Enviar)
Finaliza la sincronización de los switches S1 y S4.
F0/5
S4
F0/2
Puerto raíz (Enviar)
F0/3
F0/2
S2
Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
Puerto designado (Enviar)
Los switches S4 y S2 comienzan el proceso de propuesta y acuerdo.
F0/5
S4
F0/2
Puerto raíz (Enviar)
F0/3
F0/2
S2


Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
Puerto designado (F)
El switch S4 envía a S2 una BPDU de propuesta.
F0/5
S4
F0/2
Puerto raíz (F)
BPDU
F0/3
S2
Descarte
Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
Puertos designados (F)
Puerto designado (F)
F0/5
Este puerto se encuentra bloqueado durante el período de sincronización.
S4
F0/2
Puerto raíz (F)
F0/3
F0/2
S2
Esa BPDU posee un costo de ruta mayor
Se bloquean todos los puertos que no son del extremo.
Comienza la sincronización de los switches S4 y S2.
Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
Puertos designados (F)
Puerto designado (F)
F0/5
S4
F0/2
Puerto raíz (F)
F0/3
Propuesta
S2
Continúa la sincronización de los switches S4 y S2.


Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/1
F0/5
Puerto designado (F)
Puertos designados (F)
Propuesta
S4
F0/5
Puerto raíz (F)
F0/2
Puerto designado (Enviar)
F0/3
F0/2
S2
Puerto raíz (Enviar)
Se intercambia la BPDU entre S2 y S3.
Puerto designado (F)
Puente raíz
F0/4
F0/4
S3
S1
F0/5
Puerto designado (F)
Puerto designado (DES)
S4
F0/5
Puerto raíz (F)
F0/2
Puerto designado (Enviar)
S3 determina que el BID en la BPDU de propuesta de S2 es mayor.
S3 devuelve una BPDU de acuerdo con su menor BID a S2
F0/3
F0/2
S2
Puerto raíz (Enviar)
Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
Puertos designados (F)
S3
S1
F0/1
F0/5
Puerto designado (F)
Alternativo (Descarte)
S4
Puerto raíz (F)
F0/2
Puerto designado (Enviar)
El switch S2 cambia el puerto F0/3 al estado de descarte alternativo.
El switch S3 cambia el puerto F0/1 al estado designado enviar y al puerto F0/4 a puerto raíz en estado enviar.
F0/2
S2
Puerto raíz (Enviar)


Puerto raíz (E)
Puerto designado (F)
Puente raíz
F0/4
F0/4
Propuesta
S3
S1
Puertos designados (F)
F0/1
F0/5
Puerto designado (F)
Alternativo (Descarte)
F0/5
Puerto raíz (F)
S4
F0/2
Puerto designado (Enviar)
F0/
F0/2
S2
Puerto raíz (Enviar)
Se intercambia una BPDU entre los switches S3 y S1.
Puerto raíz (E)
Puerto designado (DES)
Puente raíz
F0/4
F0/4
S3
S1
Puertos designados (F)
F0/1
F0/5
Puerto designado (Bloqueo)
Alternativo (Descarte)
F0/5
Puerto raíz (F)
S4
F0/2
Puerto designado (Enviar)
F0/
F0/2
S2
Puerto raíz (Enviar)
El switch S1 compara el BID local con el BID de la BPDU de propuesta de S3.
El switch S1 bloquea a F0/5 y convierte al puerto F0/4 al estado designado de descarte
Puerto raíz (E)
Puerto designado (DES)
Puente raíz
F0/4
F0/4
Acuerdo
S3
S1
Puertos designados (F)
F0/1
F0/5
Puerto designado (Bloqueo)
Alternativo (Descarte)
F0/5
Puerto raíz (F)
S4
F0/2
Puerto designado (Enviar)
F0/
F0/2
S2
Puerto raíz (Enviar)
S1 determina que el BID en la BPDU de propuesta de S3 es mayor.
S1 devuelve una BPDU de acuerdo con su menor BID a S3



5.4.7 CONFIGURACION DE STP PARA EVITAR PROBLEMAS.-

PVST+ rápido es una implementación de Cisco de RSTP. Admite spanning tree para cada VLAN y es la variante rápida de STP para utilizar en redes de Cisco. La topología de la figura posee dos VLAN: 10 y 20. La configuración final implementará PVST+ rápido en el switch S1, que es el puente raíz.

Pautas para la configuración

Es de utilidad volver a ver algunas de las pautas de configuración de spanning tree. Si desea volver a ver la configuración predeterminada de spanning-tree para un switch 2960 de Cisco, consulte la sección Configuración de un switch de manera predeterminada en la parte inicial de este capítulo. Tenga en cuenta esas pautas a la hora de implementar PVST+ rápido.

Los comandos de PVST+ rápido controlan la configuración de las instancias de spanning-tree en una VLAN. Una instancia de spanning-tree se genera cuando se asigna una interfaz a una VLAN y se elimina cuando la última interfaz se traslada a otra VLAN. También se pueden configurar los parámetros de switch y puerto en STP antes de crear una instancia de spanning-tree. Estos parámetros se aplican cuando se genera un bucle y se crea una instancia de spanning-tree. Sin embargo, asegúrese de que al menos un switch de cada bucle de la VLAN ejecute spanning tree, ya que de otra manera puede producirse una tormenta de broadcast.

El switch Cisco 2960 admite PVST+, PVST+ rápido y MSTP, pero sólo una versión puede permanecer activa para todas las VLAN en todo momento.

Para obtener detalles sobre la configuración de las funciones del software de STP en un switch de la serie Cisco 2960 series, visite el sitio de Cisco:

http://www.cisco.com/en/US/products/ps6406/products_configuration_guide_chapter09186a0080875377.html.

Haga clic en el botón Comandos de configuración en la figura.

La figura muestra la sintaxis del comando del IOS de Cisco necesaria para configurar PVST+ rápido en un switch de Cisco. También se pueden configurar otros parámetros.

Nota: Si se conecta un puerto configurado con el comando spanning-tree link-type point-to-point a un puerto remoto mediante un enlace punto a punto y el puerto local se convierte en designado, el switch negocia con el puerto remoto y cambia rápidamente el puerto local al estado de enviar.

Nota: Cuando un puerto se configura con el comando clear spanning-tree detected-protocols y el mismo está conectado a un puerto de un switch antiguo de IEEE 802.1D, el software IOS de Cisco vuelve a iniciar el proceso de migración de protocolo en todo el switch. Este paso es opcional, pese a que se recomienda como práctica estándar, aún si el switch designado detecta que el switch ejecuta PVST+ rápido.

Para obtener detalles completos sobre todos los parámetros asociados con los comandos del IOS de Cisco, visite: http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_37_se/command/reference/cli3.html.

Haga clic en el botón Ejemplo de configuración que se muestra en la figura.

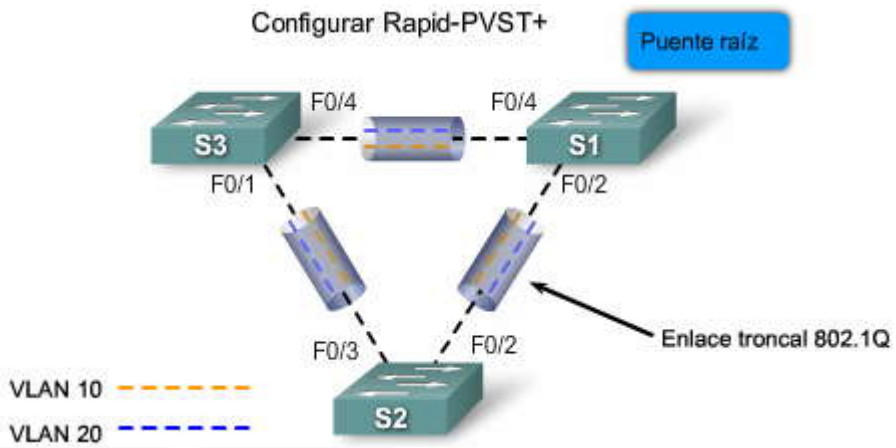
La configuración de ejemplo muestra los comandos de PVST+ rápido habilitados en el switch S1.

Haga clic en el botón Verificar que se muestra en la figura.

El comando show spanning-tree vlan vlan-id muestra la configuración de la VLAN 10 en el switch S1. Observe que la prioridad de BID se establece en 4 096. El BID se configuró mediante el comando spanning-tree vlan vlan-id priority valor de prioridad.

Haga clic en el botón show run que se muestra en la figura.

En el ejemplo, el comando show running-configuration se utiliza para verificar la configuración de PVST+ rápido en S1.



Comandos de configuración

Sintaxis de comando del IOS de Cisco	
Ingresar el modo de configuración global.	`configure terminal`
Configurar el modo rapid PVST+ spanning-tree.	`spanning-tree mode rapid-pvst`
Especificar una interfaz a configurar e ingresar el modo de configuración de interfaz. El rango del ID de la VLAN ID es de 1 a 4094. El rango del canal del puerto es de 1 a 6.	`interface`
Especificar que el tipo de enlace para este puerto es punto a punto.	`spanning-tree link-type point-to-point`
Volver al modo EXEC privilegiado.	`end`
Borrar todos los STP detectados.	`clear spanning-tree detected-protocols`

Ejemplo de configuración

```
S1#configure terminal
S1(config)#spanning-tree mode rapid-pvst
S1(config)#interface f0/2
S1(config-if)#spanning-tree link-type point-to-point
S1(config-if)#end
S1#clear spanning-tree detected-protocols
```

Verificar

```
S1# show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    4106
              Address     0019.aa9e.b000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    4106   (priority 4096 sys-id-ext 10)
              Address     0019.aa9e.b000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
Interface        Role Sta Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg LRN 19        128.2    P2p
Fa0/4            Desg LRN 19        128.4    P2p
<output truncated>
```

```
S1# show run
```

show run

```
<Output omitted>

spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
<output omitted>
```

5.4.8 RESOLUCION DE PROBLEMAS DE FUNCIONAMIENTO DE STP.-

Conozca dónde se encuentra la raíz

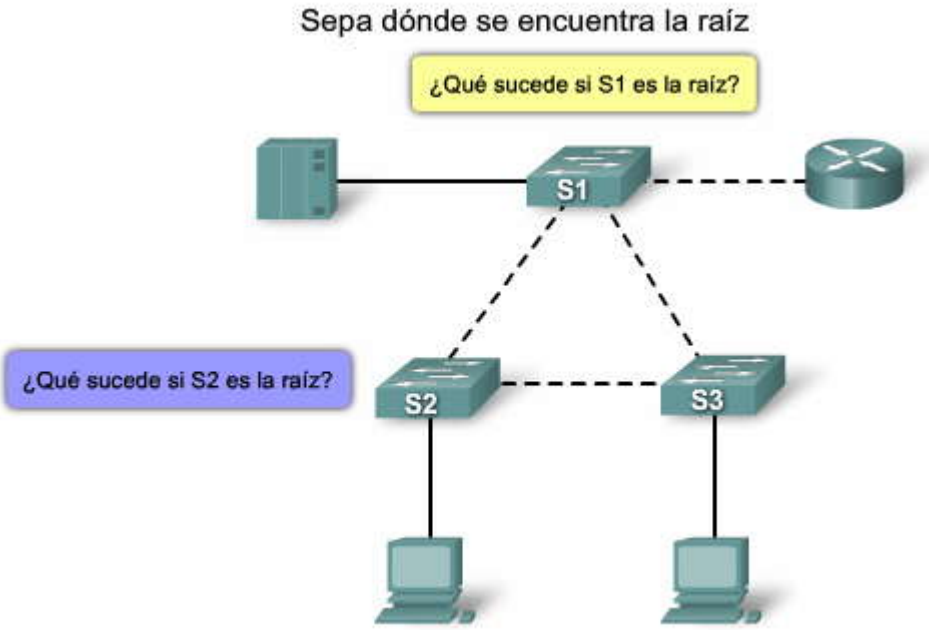
Ahora sabe que la función principal del STA es evitar los bucles que producen los enlaces redundantes en redes de puentes. STP funciona en la Capa 2 del modelo OSI. STP puede fallar en algunos casos específicos. La resolución de problemas puede ser muy complicada y depende del diseño de la red. Es por eso que se recomienda que lleve a cabo la parte más importante de la resolución de problemas antes de que ocurran los mismos.

Es muy común que la información acerca de la ubicación de la raíz no esté disponible a la hora de resolver los problemas. No permita que la decisión del puente raíz dependa de STP. Por lo general, para cada VLAN se puede identificar cuál es el switch que mejor puede funcionar como raíz. En general, elija un switch poderoso en el medio de la red. Si coloca el puente raíz en el centro de la red con una conexión directa a los servidores y routers, se reduce la distancia promedio desde los clientes a los servidores y routers.

La figura muestra:

Si el switch S2 es la raíz, el enlace desde S1 a S3 se encuentra bloqueado en S1 o en S3. En este caso, los hosts que se conectan al switch S2 pueden acceder al servidor y al router en dos saltos. Los hosts que se conectan al puente S3 pueden acceder al servidor y al router en tres saltos. La distancia promedio es de dos saltos y medio.
Si el switch S1 es la raíz, el router y el servidor son alcanzables en dos saltos para los dos hosts que se conectan a S2 y S3. La distancia promedio ahora es de dos saltos.

La lógica detrás de este ejemplo simple se traslada a topologías más complejas.
Nota: Para cada VLAN, configure el puente raíz y el puente raíz de respaldo a través de prioridades menores.



Para facilitar la solución de problemas en STP, planifique la organización de los enlaces redundantes. En redes no jerárquicas puede necesitar ajustar el parámetro de costo de STP para decidir los puertos que deben bloquearse. Sin embargo, este ajuste por lo general no es necesario si cuenta con un diseño jerárquico y con un puente raízbien ubicado.

Nota: Para cada VLAN, debe conocer los puertos que deben bloquearse en la red estable. Tenga a mano un diagrama de red que muestre de forma clara todos los bucles físicos de la red y cuáles son los puertos bloqueados que eliminan esos bucles.

Conocer la ubicación de los enlaces redundantes lo ayudará a identificar los bucles de puenteo accidentales y sus causas. Además, si conoce la ubicación de los puertos bloqueados podrá determinar la ubicación del error.

Minimizar la cantidad de puertos bloqueados

La única acción crítica que STP lleva a cabo es el bloqueo de puertos. Un único puerto bloqueado que por error pasa al estado de enviar puede impactar de forma negativa en gran parte de la red. Una buena forma de limitar el riesgo inherente al uso de STP es reducir el número de puertos bloqueados al mínimo posible.

Depuración de VTP

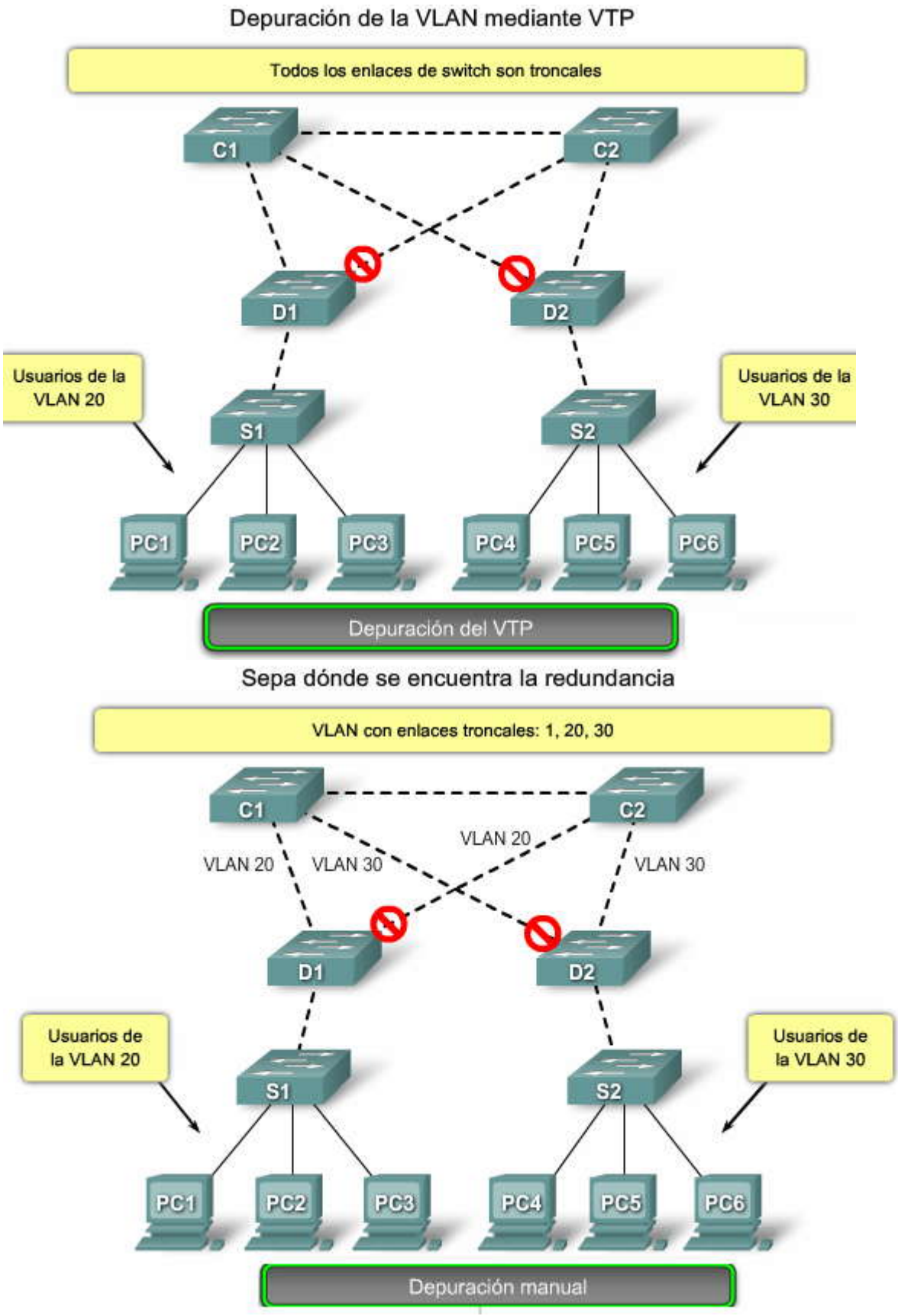
No se requieren más de dos enlaces redundantes entre dos nodos de una red conmutada. Sin embargo, la configuración mostrada en la figura es muy común. Los switches de distribución poseen una conexión doble a dos switches del núcleo, C1 y C2. Los usuarios de los switches S1 y S2 que se conectan a los switches de distribución se encuentran sólo en un subconjunto de las VLAN disponibles en la red. En la figura, los usuarios que se conectan al switch D1 se encuentran todos en la VLAN 20, el switch D2 conecta a los usuarios a la VLAN 30. De manera predeterminada, los enlaces troncales transportan todas las VLAN definidas en el dominio de VTP. Sólo el switch D1 recibe tráfico de broadcast y multicast innecesario para la VLAN 20, pero también cuenta con uno de sus puertos bloqueados para la VLAN 30. Existen tres rutas redundantes entre los switches C1 y C2 de la capa núcleo. Esta redundancia tiene como consecuencia más puertos bloqueados y una más alta probabilidad de bucles.

Nota: Depure todas las VLAN que no necesite en sus enlaces troncales.

Haga clic en el botón Depuración manual que se muestra en la figura.

Depuración manual

La depuración de VTP puede ayudar pero esta función no es necesaria en el núcleo de la red. En la figura, sólo se utiliza una VLAN de acceso para conectar los switches de distribución al núcleo. En este diseño, sólo hay un puerto bloqueado por VLAN. Además, con este diseño se pueden eliminar todos los enlaces redundantes en un solo paso si desconecta C1 o C2.



Utilice la conmutación de Capa 3

La conmutación de Capa 3 implica que el enrutamiento se lleva a cabo a la velocidad de la conmutación. Un router realiza dos funciones principales:

Construye una tabla de envíos. En general, el router intercambia información con sus pares mediante los protocolos de enrutamiento.

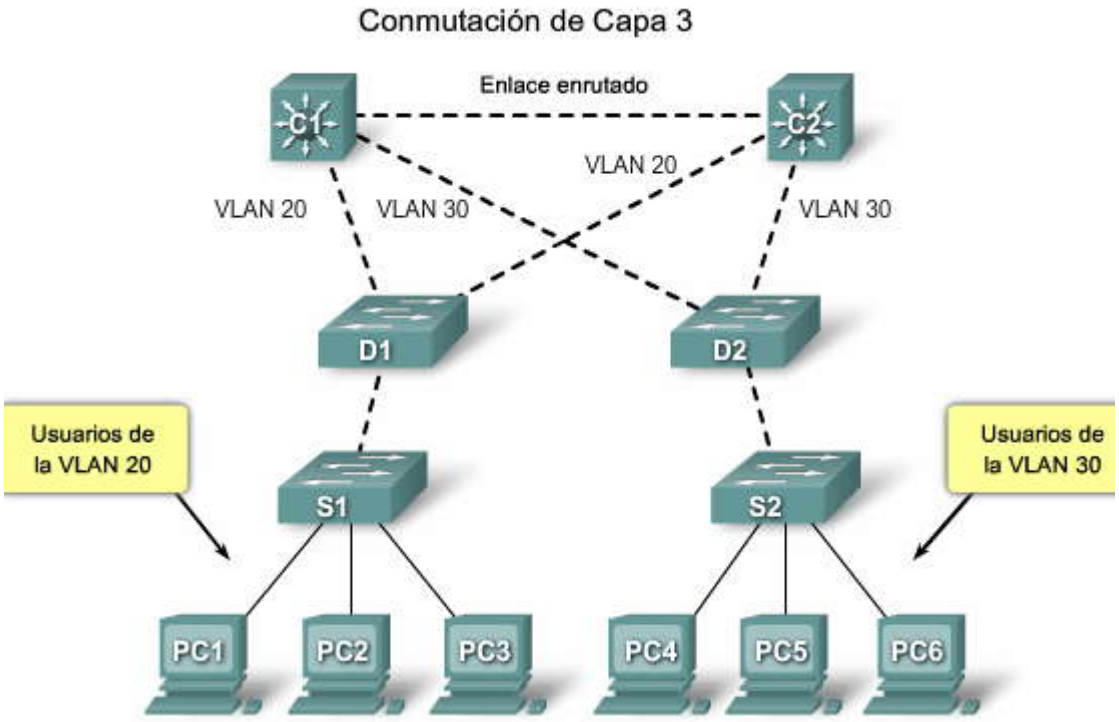
Recibe paquetes y los envía a la interfaz correcta en base a la dirección de destino.

Los switches Cisco de nivel superior de la Capa 3 ahora pueden realizar esta segunda función a la misma velocidad que la función de conmutación de Capa 2. En la figura:

No existe penalización de velocidad para el salto de enrutamiento y en un segmento adicional entre C1 y C2.
El switch C1 del núcleo y el switch C2 del núcleo corresponden a la Capa 3. La VLAN 20 y la VLAN 30 ya no poseen puentes entre C1 y C2, de manera que no existe la posibilidad de bucles.

La redundancia aún está presente, con dependencia en los protocolos de enrutamiento de la Capa 3. El diseño asegura que la convergencia sea más rápida que en STP.

STP ya no bloquea los puertos, de manera que no existe la posibilidad de bucles de puenteo.
Al establecer la VLAN según la conmutación de Capa 3 permite que la velocidad sea tan alta como si se contara con puenteo dentro de la VLAN.



Puntos finales

Mantenga STP aun si no es necesario

Asumiendo que ha eliminado todos los puertos bloqueados de la red y que no existe redundancia física, se recomienda altamente no deshabilitar STP.

En general, STP no es muy exigente para el procesador, la conmutación de paquetes no involucra a la CPU en la mayoría de los switches Cisco. Además, las pocas BPDU que se envían en cada enlace no reducen de forma significativa el ancho de banda disponible. Sin embargo, si un técnico comete un error de conexión en un panel de conexión y genera un bucle de manera accidental, la red sufrirá un impacto negativo. En general, deshabilitar STP en una red conmutada no vale el riesgo.

Mantenga el tráfico fuera de la VLAN administrativa y no permita que una única VLAN se expanda por toda la red

En general, un switch de Cisco posee una única dirección IP que lo conecta a una VLAN, conocida como VLAN administrativa. En esta VLAN, el switch se comporta como un host IP genérico. En particular, todo paquete de broadcast o multicast se envía a la CPU. Una tasa alta de tráfico de broadcast o multicast en la VLAN administrativa puede impactar de forma adversa en la CPU y en su capacidad para procesar las BPDU vitales. Por lo tanto, mantenga el tráfico de usuario fuera de la VLAN administrativa.

Hasta hace poco tiempo no existía manera de eliminar la VLAN 1 de un enlace troncal en una implementación de Cisco. En general, la VLAN 1 cumple la función de VLAN administrativa, donde todos los switches son accesibles en la misma subred IP. Pese a que es de utilidad, esta configuración puede ser peligrosa, ya que un bucle de puenteo en la VLAN 1 afecta a todos los enlaces troncales, lo que puede hacer que toda la red deje de funcionar. Por supuesto, el mismo problema se repite independientemente de la VLAN que se utilice. Intente segmentar los dominios de puenteo mediante los switches de alta velocidad de la Capa 3.

Nota: A partir de la versión 12.1(11b)E del software IOS de Cisco, se puede eliminar la VLAN 1 de los enlaces troncales. La VLAN 1 aún existe pero bloquea el tráfico, lo que evita la posibilidad de bucles.

PUNTOS FINALES

Mantenga STP incluso si no es necesario.
No deshabilite STP.
STP no es muy exigente para el procesador.
Las pocas BPDU enviadas a cada enlace no reducen el ancho de banda.
Pero una red de puentes sin STP puede dejar de funcionar en una fracción de segundo.

Mantenga el tráfico fuera de la VLAN administrativa.
Una tasa alta de tráfico de broadcast o multicast en la VLAN administrativa produce un efecto adverso sobre la capacidad de la CPU para procesar las BPDU vitales.
Mantenga el tráfico de usuario fuera de la VLAN administrativa.

No permita que una única VLAN se expanda por toda la red.
La VLAN 1 sirve como VLAN administrativa, donde todos los switches son accesibles en la misma subred IP.
Un bucle de puenteo en la VLAN 1 afecta a todos los enlaces troncales y la red puede dejar de funcionar.
Segmente los dominios de puenteo mediante los switches de alta velocidad de la Capa 3.

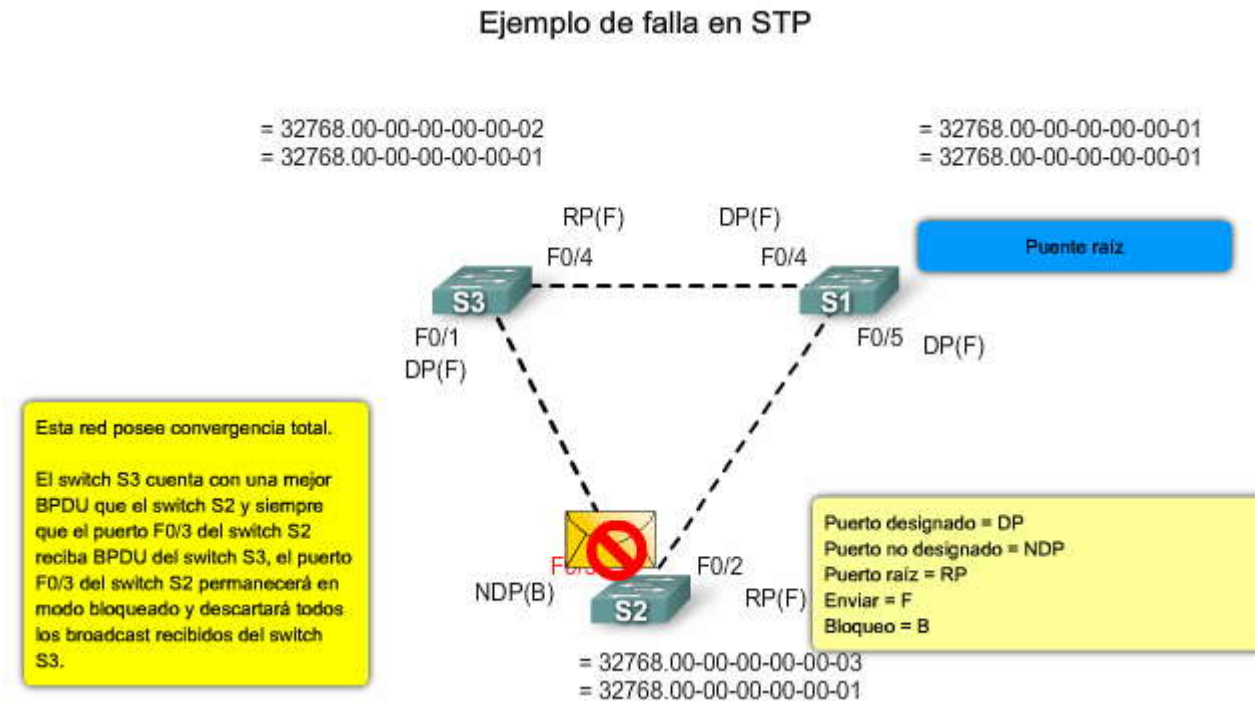
5.4.9 RESOLUCION DE PROBLEMAS DE FUNCIONAMIENTO STP

Falla del switch o del enlace

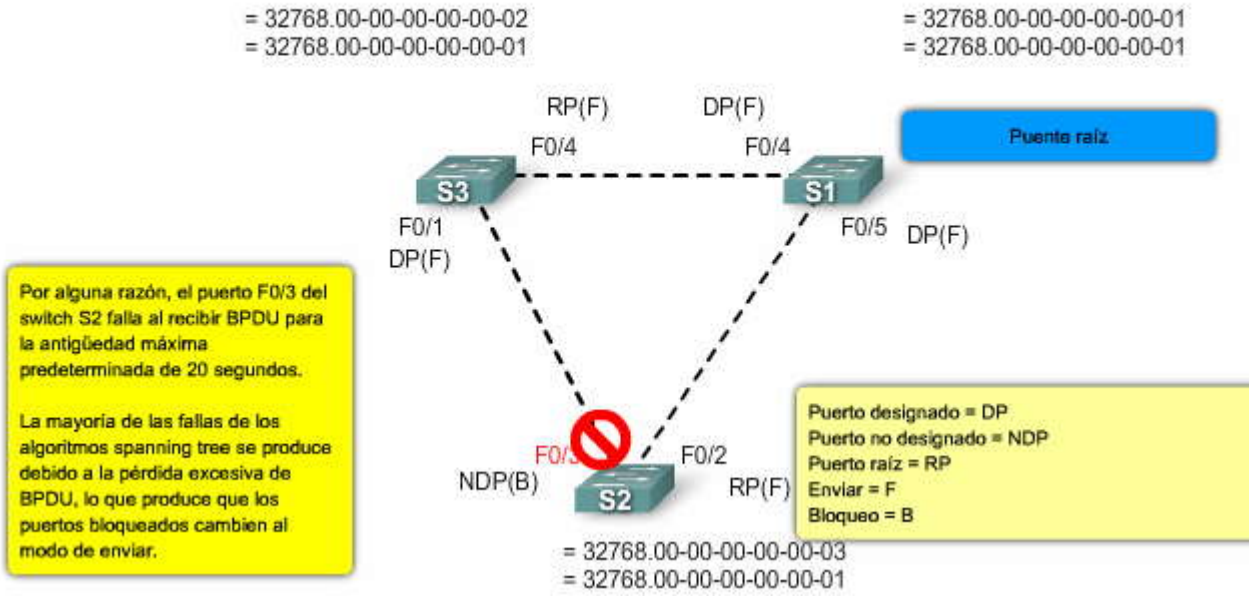
En la animación se puede ver que cuando falla un puerto de una red configurada con STP, se puede producir una tormenta de broadcast.

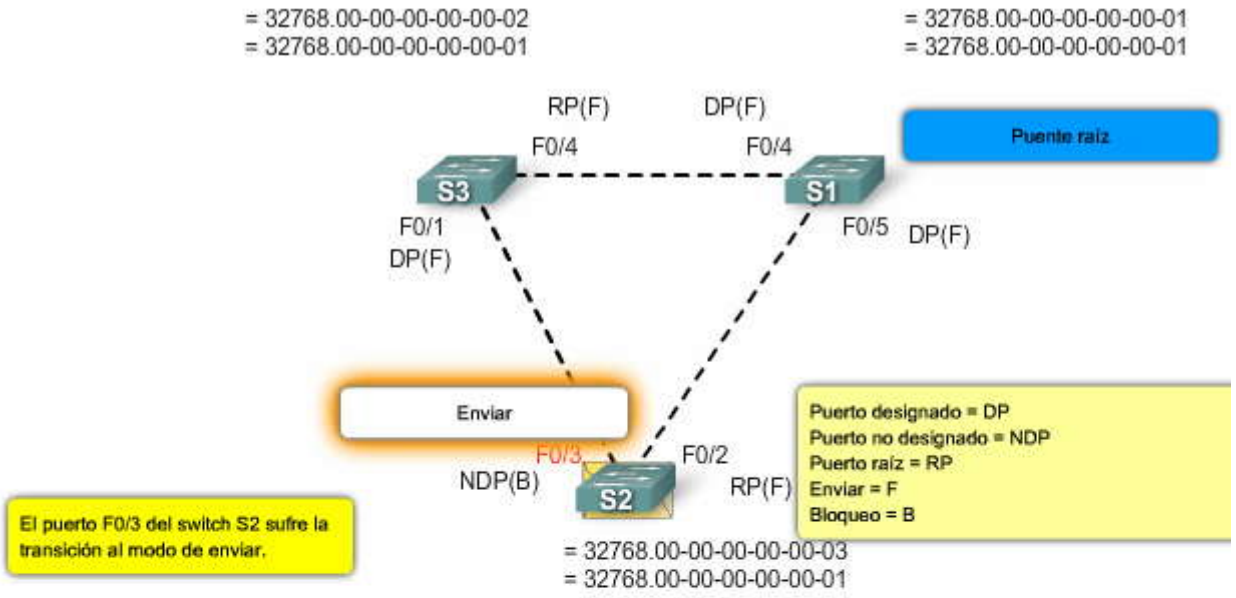
En el estado inicial de la situación de falla en STP, el switch S3 posee un BID menor que S2; en consecuencia el puerto designado entre S3 y S2 es el puerto S0/1 del switch S3. Se considera que el switch S3 posee una "mejor BPDU" que el switch S2.

Haga clic en el botón Reproducir de la figura para ver la falla en STP.

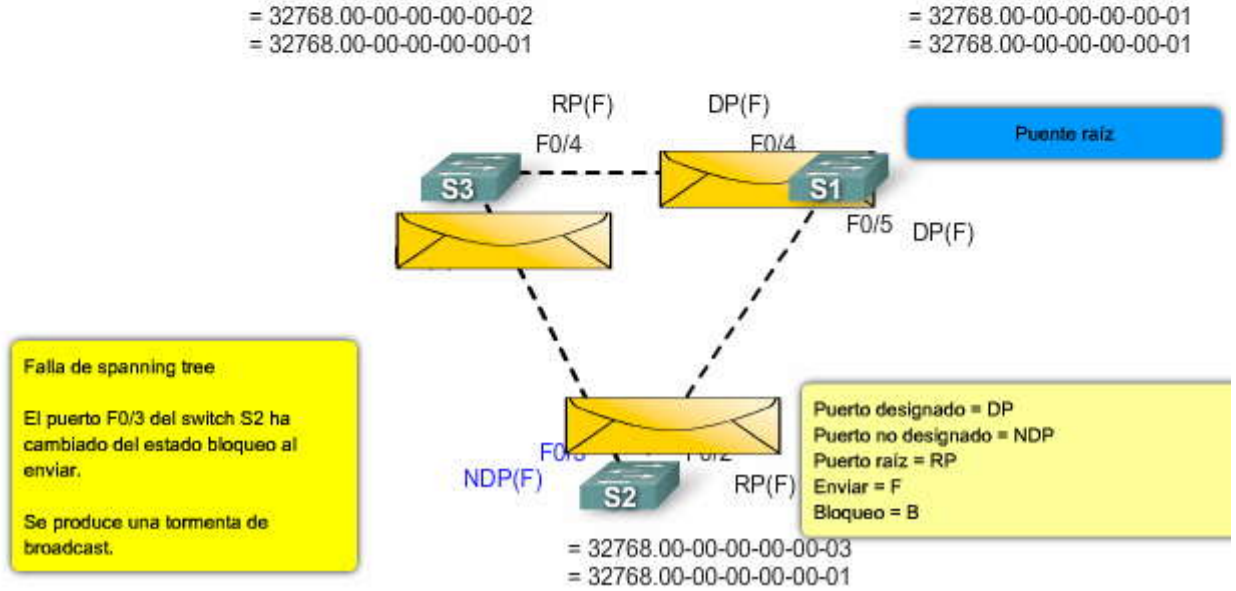


Ejemplo de falla en STP





Ejemplo de falla en STP



Resolución de problemas ante una falla

Desafortunadamente, no existe ningún procedimiento sistemático para la resolución de problemas ante una falla con STP. Esta sección resume algunas de las acciones disponibles. La mayoría de los pasos se aplican para la resolución de problemas relacionados con los bucles de puenteo en general. Puede utilizar un enfoque más convencional para identificar otras fallas de STP que provocan la pérdida de la conectividad. Por ejemplo: puede explorar la ruta que sigue el tráfico que está experimentando el problema.

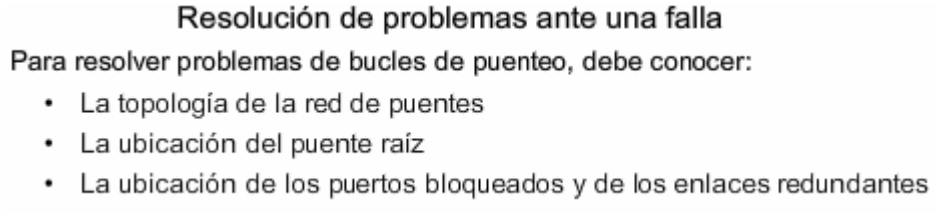
Nota: Es posible que el acceso dentro de la banda no se encuentre disponible durante un bucle de puenteo. Por ejemplo: es posible que no pueda hacer Telnet a los dispositivos de la infraestructura durante una tormenta de broadcast. Por lo tanto, puede necesitar la conectividad fuera de banda, como el acceso de consola.

Antes de llevar a cabo la resolución de problemas de un bucle de puenteo, debe conocer al menos estos factores:

Topología de la red de puentes
Ubicación del puente raíz
Ubicación de los puertos bloqueados y de los enlaces redundantes

Este conocimiento es esencial. Para saber lo que debe repararse en la red, necesita saber cómo se vela red cuando funciona de forma correcta. La mayoría de los pasos de la resolución de problemas sólo utiliza los comandos show para intentar identificar situaciones de error. El conocimiento de la red ayuda a enfocarse en los puertos fundamentales en los dispositivos clave.

El resto de este tema se enfoca brevemente en dos problemas comunes de spanning tree, un error de configuración de PortFast y los inconvenientes relacionados con el diámetro de la red. Para aprender más acerca de otros inconvenientes con STP, visite: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800951ac.shtml.



Error de configuración de PortFast

En general, sólo se habilita PortFast en un puerto o interfaz que se conecta a un host. Cuando se enciende el enlace en dicho puerto, el puente salta las primeras etapas del STA y directamente pasa al modo enviar.

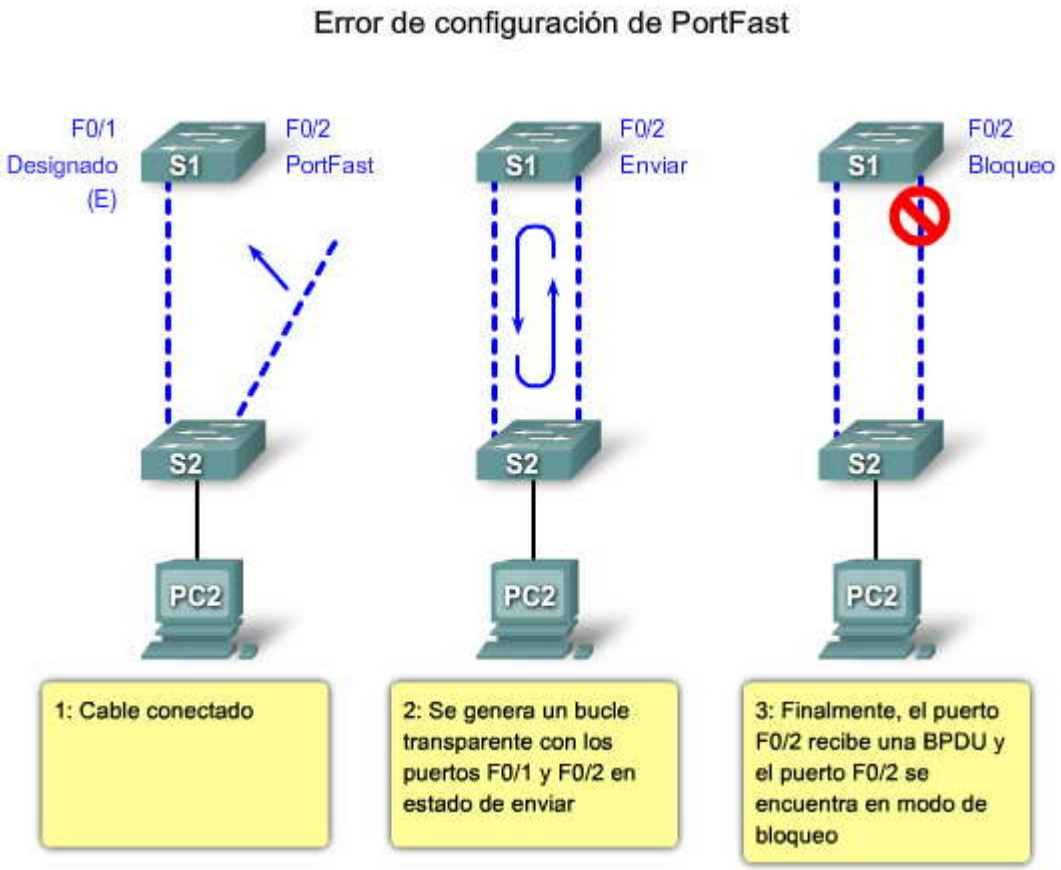
Precaución: No utilice PortFast en puertos de switch o interfaces que se conectan a otros switches, hubs o routers. De otra forma, puede generar un bucle en la red.

En este ejemplo, el puerto F0/1 del switch S1 ya se encuentra enviando. El puerto F0/2 se ha configurado de forma errónea con la función PortFast. Por lo tanto, cuando se conecta la segunda conexión desde el switch S2 a F0/2 de S1, el puerto pasa a modo enviar de manera automática y genera un bucle.
Eventualmente, uno de los switches enviará una BPDU y provocará la transición de un puerto al modo de bloqueo.
Sin embargo, existe un problema con este tipo de bucle de transición. Si el tráfico atrapado en el bucle es muy intenso, el switch puede tener problemas al intentar transmitir de forma adecuada la BPDU que detiene el bucle. Este problema puede demorar la convergencia de manera considerable o, en algunos casos extremos, puede hacer que lared deje de funcionar.

Aun con una configuración de PortFast, el puerto o interfaz continúa participando en el STP. Si un switch con una prioridad de puente menor que la del puente raíz activo actual se conecta a un puerto o interfaz con PortFast configurado, el mismo puede resultar elegido como puente raíz. Este cambio de puente raíz puede afectar de forma adversa a la topología de STP activa y puede hacer que la red no esté óptima. Para evitar esta situación, la mayoría de los switches Catalyst que ejecutan el software IOS de Cisco cuenta con una función denominada protección de BPDU. La protección de BPDU deshabilita un puerto o interfaz configurados con PortFast si los mismos reciben una BPDU.

Para obtener más información acerca del uso de PortFast en switches que ejecutan el software IOS de Cisco, consulte el documento "Using PortFast and Other Commands to Fix Workstation Startup Connectivity Delays," disponible en: http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a00800b1500.shtml.

Para obtener más información acerca del uso de la protección de BPDU en switches que ejecutan el software IOS de Cisco, visite: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a008009482f.shtml.



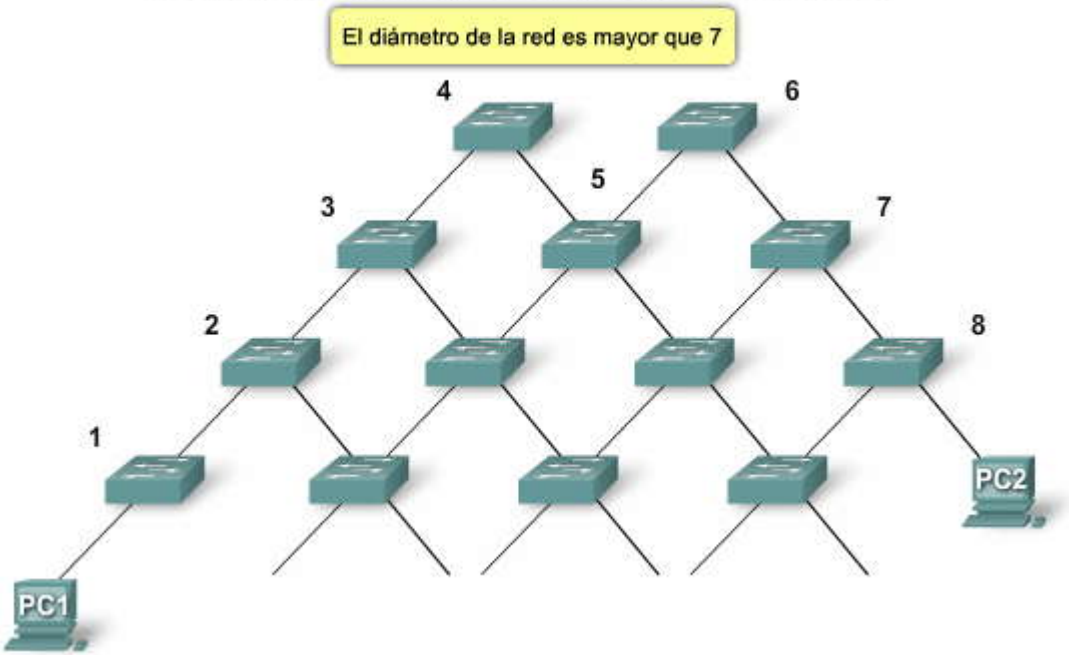
Inconvenientes relacionados con el diámetro de la red

Otro inconveniente del cual no existe demasiada información se relaciona con el diámetro de la red conmutada. Los valores conservadores predeterminados para los temporizadores de STP imponen un diámetro máximo de red de siete.En la figura, este diseño crea un diámetro de red de ocho. El diámetro de red máximo restringe la distancia que puede existir entre los switches de la red. En este caso, no puede haber más de ocho saltos entre dos switches distintos. Parte de esta restricción se obtiene del campo de antigüedad que transporta la BPDU.

Cuando una BPDU se propaga desde el puente raíz hacia las hojas del árbol, el campo de antigüedad se incrementa cada vez que la misma atraviesa un switch. Eventualmente, el switch descarta la BPDU cuando el campo de antigüedad llega a la antigüedad máxima. Si la raíz se encuentra demasiado lejos de algunos switches de la red, las BPDU se descartan. Este inconveniente afecta a la convergencia del spanning tree.

Se debe tener mucho cuidado si se planea cambiar los valores predeterminados de los temporizadores de STP. Se corre peligro si se intenta agilizar la convergencia de esta manera. Un cambio de temporizador de STP impacta en el diámetro de la red y en la estabilidad de STP. Se puede cambiar la prioridad del switch para seleccionar el puente raíz y el parámetro de costo o prioridad de puerto para controlar la redundancia y el balanceo de carga.

Inconvenientes relacionados con el diámetro de la red



Actividad 1

Estados de los puertos de STP y RSTP

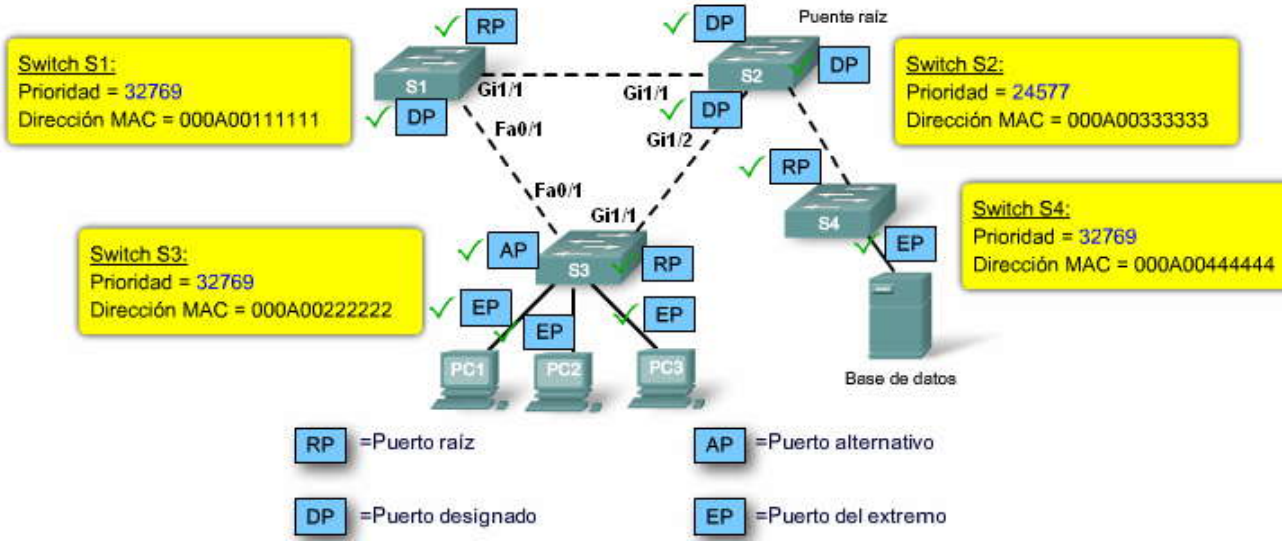
Actividad

Arrastre y coloque los nombres de los estados de los puertos de STP y RSTP que coincidan con el funcionamiento del estado de puerto. Se utilizan todas las respuestas. Algunas respuestas se pueden usar más de una vez.

Operación del estado de puerto	Estado del puerto en STP	Estado del puerto en RSTP
Habilitado	✓ Bloqueo	✓ Descarte
Habilitado	✓ Escuchar	✓ Descarte
Habilitado	✓ Aprender	✓ Aprender
Habilitado	✓ Enviar	✓ Enviar
Deshabilitado	✓ Deshabilitado	✓ Descarte

Escuchar | Aprender | Bloqueo

Deshabilitado | Descarte | Enviar



CAPITULO VI – "ENRUTAMIENTO INTER VLAN"

6.0 INTRODUCCIÓN DEL CAPITULO.-

6.0.1 INTRODUCCIÓN.-

En los capítulos anteriores de este curso analizamos cómo utilizar las VLAN y enlaces troncales para segmentar una red. Limitar el ámbito de cada dominio de broadcast en la LAN mediante la segmentación de la VLAN proporciona mejor rendimiento y seguridad a través de la red. También aprendió cómo se utiliza el VTP para compartir la información de la VLAN a través de múltiples switches en un ambiente de LAN, para simplificar la administración de las VLAN. Ahora que tiene una red con muchas y diferentes VLAN, la siguiente pregunta es: "¿cómo permitimos que se comuniquen los dispositivos en VLAN separadas?"

En este capítulo, aprenderá sobre el enrutamiento inter VLAN y cómo se utiliza para permitir la comunicación de los dispositivos en VLAN separadas. Aprenderá diferentes métodos para lograr el enrutamiento inter VLAN, y las ventajas y desventajas de cada uno. Además aprenderá cómo las distintas configuraciones de la interfaz dd router facilitan el enrutamiento inter VLAN. Finalmente, analizará los problemas potenciales que podría enfrentar al implementar el enrutamiento inter VLAN y cómo identificarlos y corregirlos.

En este capítulo aprenderá a:

- Explicar cómo el tráfico de la red está enrutado entre las VLAN en una red convergente.
- Configurar el enrutamiento inter VLAN en un router para permitir la comunicación entre dispositivos de usuario final en VLAN separadas.
- Resolver los problemas de conectividad inter VLAN más comunes.

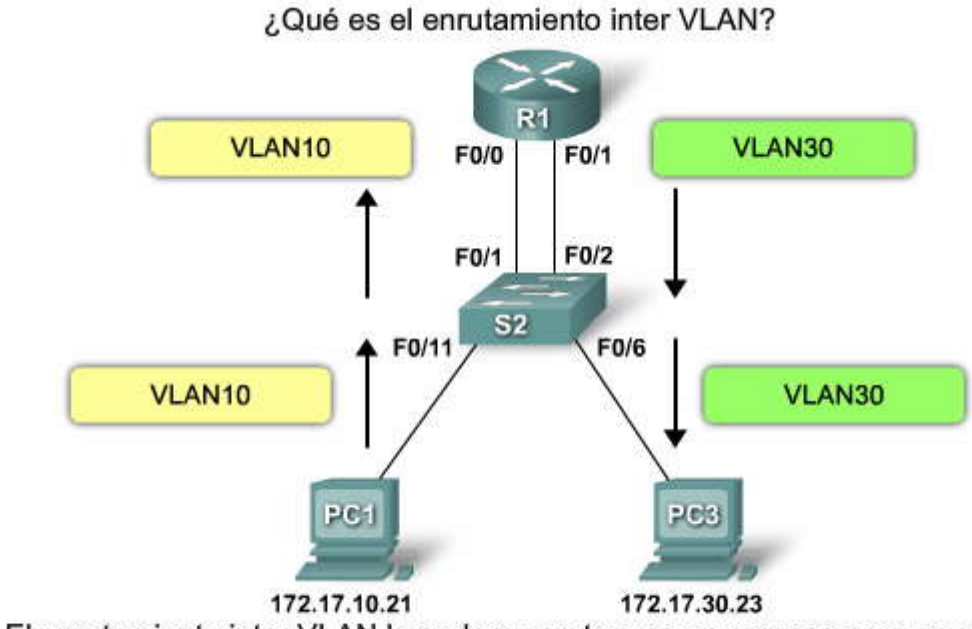
6.1 ENRUTAMIENTO INTER VLAN.-

6.1.1 INTRODUCCION AL ENRUTAMIENTO INTER VLAN.-

Ahora que ya conoce cómo configurar las VLAN en un switch de redes, el siguiente paso es permitir a los dispositivos conectados a las distintas VLAN comunicarse entre sí. En un capítulo anterior, aprendió que cada VLAN es un dominio de broadcast único. Por lo tanto, de manera predeterminada, las computadoras en VLAN separadas no pueden comunicarse. Existe una manera para permitir que estas estaciones finales puedan comunicarse; esta manera se llama enrutamiento inter VLAN. En este tema aprenderá qué es el enrutamiento inter VLAN y algunas de las diferentes maneras de lograr un enrutamiento inter VLAN en una red.

En este capítulo, nos concentramos en un tipo de enrutamiento inter VLAN mediante un router separado conectado a una infraestructura de switch. Definimos al enrutamiento inter VLAN como un proceso para reenviar el tráfico de la red desde una VLAN a otra mediante un router. Las VLAN están asociadas a subredes IP únicas en la red. Esta configuración de subred facilita el proceso de enrutamiento en un ambiente de múltiples VLAN. Cuando utiliza un router para facilitar el enrutamiento inter VLAN, las interfaces del router pueden conectarse a VLAN separadas. Los dispositivos en dichas VLAN envían el tráfico a través del router hasta llegar a otras VLAN.

Como puede ver en la figura, el tráfico de PC1 en la VLAN10 está enrutado a través del router R1 para llegar a PC3 en la VLAN30.



El enrutamiento inter VLAN basado en routers es un proceso para reenviar el tráfico de la red desde una VLAN a otra mediante un router.

Tradicionalmente, el enrutamiento de la LAN utiliza routers con interfaces físicas múltiples. Es necesario conectar cada interfaz a una red separada y configurarla para una subred diferente.

En una red tradicional que utiliza VLAN múltiples para segmentar el tráfico de la red en dominios de broadcast lógicos, el enrutamiento se realiza mediante la conexión de diferentes interfaces físicas del router a diferentes puertos físicos del switch. Los puertos del switch conectan al router en modo de acceso; en el modo de acceso, diferentes VLAN estáticas se asignan a cada interfaz del puerto. Cada interfaz del switch estaría asignada a una VLAN estática diferente. Cada interfaz del router puede entonces aceptar el tráfico desde la VLAN asociada a la interfaz del switch que se encuentra conectada, y el tráfico puede enrutarse a otras VLAN conectadas a otras interfaces.

Haga clic en el botón Reproducir que se muestra en la figura para ver el enrutamiento inter VLAN tradicional.

Como puede verse en la animación:

1. PC1 en la VLAN10 se está comunicando con PC3 en la VLAN30 a través del router R1.

2. PC1 y PC3 están en VLAN diferentes y tienen direcciones IP en subredes diferentes.

3. El router R1 tiene una interfaz separada configurada para cada una de las VLAN.

4. PC1 envía el tráfico unicast destinado a PC3 al switch S2 en la VLAN10, donde luego se lo reenvía por la interfaz troncal al switch S1.

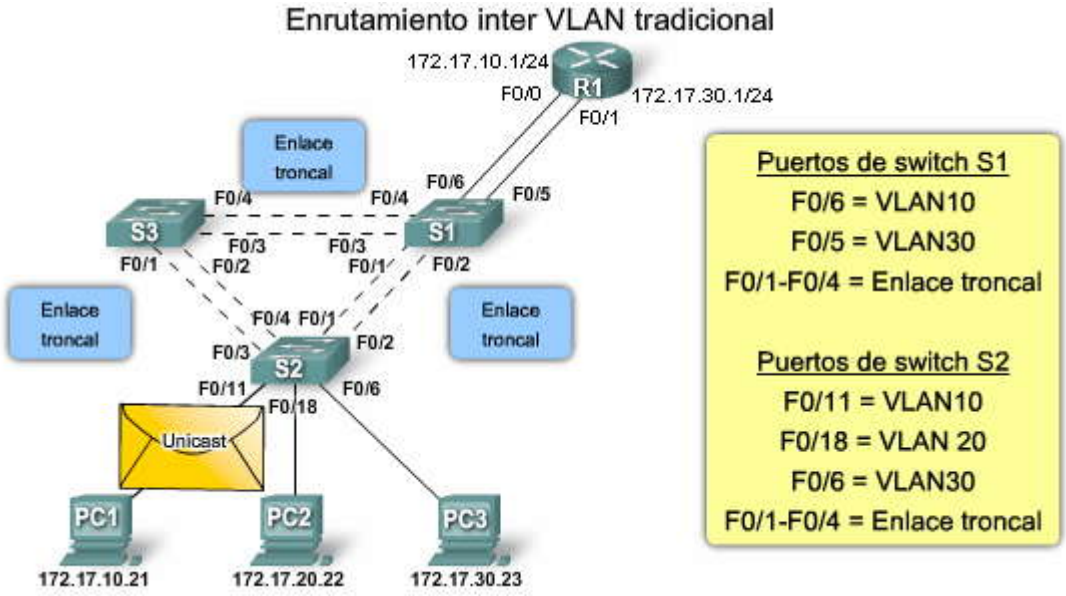
5. El switch S1 luego reenvía el tráfico unicast al router R1 en la interfaz F0/0.

6. El router enruta el tráfico unicast a través de la interfaz F0/1, que está conectada a la VLAN30.

7. El router reenvía el tráfico unicast al switch S1 en la VLAN 30.

8. El switch S1 luego reenvía el tráfico unicast al switch S2 a través del enlace troncal, luego, el switch S2 puede reenviar el tráfico unicast a PC3 en la VLAN30.

En este ejemplo el router se configuró con dos interfaces físicas separadas para interactuar con las distintas VLAN y realizar el enrutamiento.



El enrutamiento inter VLAN tradicional requiere de interfaces físicas múltiples en el router y en el switch. Sin embargo, no todas las configuraciones del enrutamiento inter VLAN requieren de interfaces físicas múltiples. Algunos software del router permiten configurar interfaces del router como enlaces troncales. Esto abre nuevas posibilidades para el enrutamiento inter VLAN.

"Router-on-a-stick" es un tipo de configuración de router en la cual una interfaz física única enruta el tráfico entre múltiples VLAN en una red. Como puede ver en la figura, el router se conecta al switch S1 mediante una conexión de red física y única.

La interfaz del router se configura para funcionar como enlace troncal y está conectada a un puerto del switch configurado en modo de enlace troncal. El router realiza el enrutamiento inter VLAN al aceptar el tráfico etiquetado de la VLAN en la interfaz troncal proveniente del switch adyacente y enrutar en forma interna entre las VLAN, mediante subinterfaz. El router luego reenvía el tráfico enrutado de la VLAN etiquetada para la VLAN de destino, por la misma interfaz física.

Las subinterfaces son interfaces virtuales múltiples, asociadas a una interfaz física. Estas interfaces están configuradas en software en un router configurado en forma independiente con una dirección IP y una asignación de VLAN para funcionar en una VLAN específica. Las subinterfaces están configuradas para diferentes subredes quecorresponden a la asignación de la VLAN, para facilitar el enrutamiento lógico antes de que la VLAN etiquete las tramas de datos y las reenvíe por la interfaz física. Aprenderá más acerca de las interfaces y subinterfaces en el siguiente tema.

Haga clic en el botón Reproducir que se muestra en la figura para ver cómo un router-on-a-stick realiza la función de enrutamiento.

Como puede verse en la animación:

1. PC1 en la VLAN10 se está comunicando con PC3 en la VLAN30 a través del router R1 mediante una interfaz del router física y única.

2. PC1 envía el tráfico unicast al switch S2.

3. El switch S2 luego etiqueta el tráfico unicast como originado en la VLAN10 y lo reenvía por el enlace troncal al switch S1.

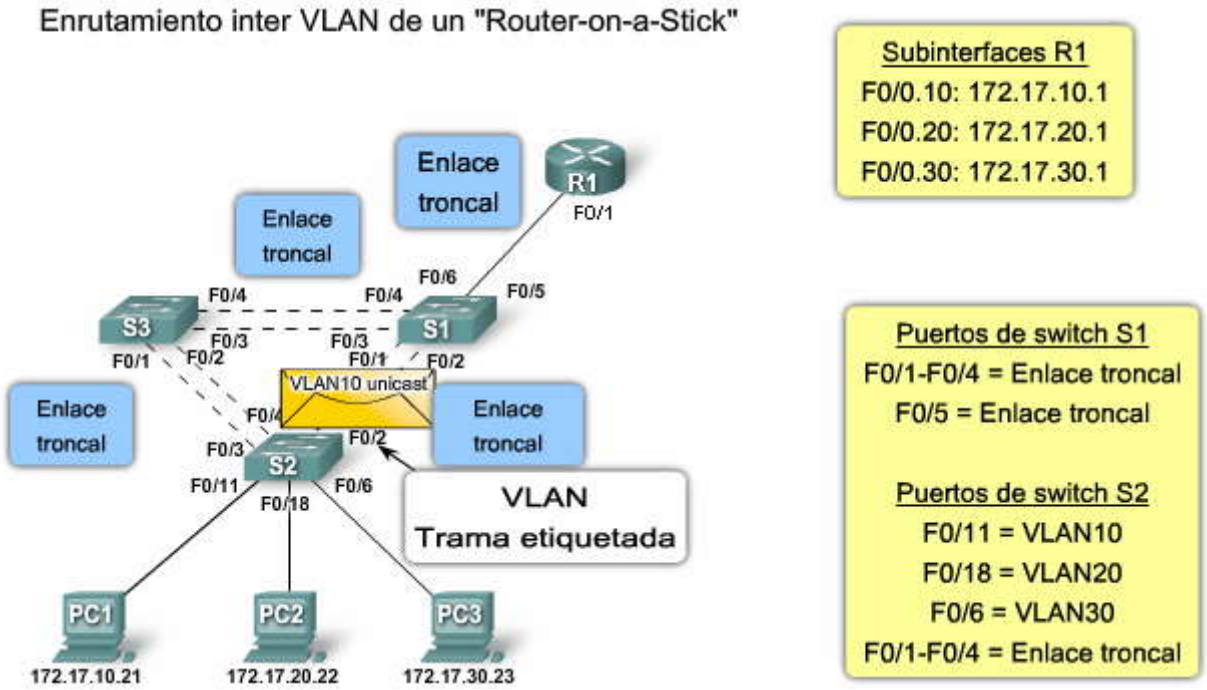
4. El switch S1 reenvía el tráfico etiquetado fuera de la otra interfaz troncal en el puerto F0/5 a la interfaz en el router R1.

5. El router R1 acepta el tráfico unicast etiquetado en la VLAN10 y lo enruta a la VLAN30 mediante las subinterfaces configuradas.

6. El tráfico unicast es etiquetado con la VLAN30 y enviado fuera de la interfaz del router al switch S1.

7. El switch S1 reenvía el tráfico unicast etiquetado fuera del otro enlace troncal al switch S2.

8. El switch S2 elimina la etiqueta de la VLAN de la trama de unicast y reenvía la trama a PC3 en el puerto F0/6.



Algunos switches pueden realizar funciones de Capa 3, reemplazando la necesidad de utilizar routers dedicados para realizar el enrutamiento básico en una red. Los switches multicapas pueden realizar el enrutamiento inter VLAN.

Haga clic en el botón Reproducir que se muestra en la figura para ver cómo tiene lugar un enrutamiento inter VLAN basado en switches.

Como puede verse en la animación:

1. PC1 en la VLAN10 se está comunicando con PC3 en la VLAN30 a través del switch S1 mediante interfaces VLAN configuradas para cada VLAN.

2. PC1 envía el tráfico unicast al switch S2.

3. El switch S2 luego etiqueta el tráfico unicast como originado en la VLAN10 a medida que lo reenvía por el enlace troncal al switch S1.

4. El switch S1 elimina la etiqueta de la VLAN y reenvía el tráfico unicast a la interfaz VLAN10.

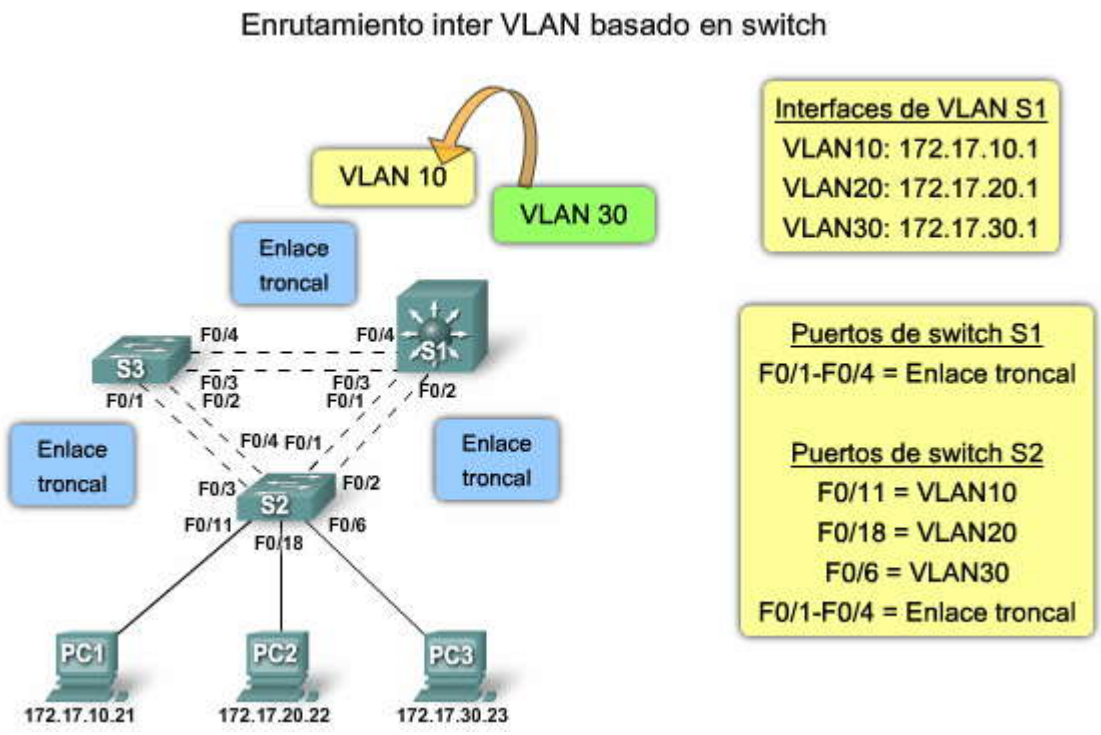
5. El switch S1 enruta el tráfico unicast a la interfaz VLAN30.

6. El switch S1 luego vuelve a etiquetar el tráfico unicast con la VLAN30 y lo reenvía por el enlace troncal al switch S2.

7. El switch S2 elimina la etiqueta de la VLAN de la trama de unicast y reenvía la trama a PC3 en el puerto F0/6.

Para habilitar un switch multicapa para realizar funciones de enrutamiento, es necesario configurar las interfaces VLAN en el switch con las direcciones IP correspondientes que coincidan con la subred a la cual la VLAN está asociada en la red. El switch multicapa también debe tener el IP routing habilitado. El switching multicapa es complejo y va más allá del ámbito de este curso. Para obtener una buena descripción general del switching multicapa, visite: http://cisco.com/en/US/docs/ios/12_0/switch/configuration/guide/xcmls.html.

La configuración del enrutamiento inter VLAN en un switch multicapa va más allá del alcance de este curso. Sin embargo, el currículo CCNP abarca el concepto ampliamente. Además, para explorar información adicional, visite: http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a008019e74e.shtml.



6.1.2 INTERFACES Y SUBINTERFACES.-

Tal como se explicó, existen varias opciones de enrutamiento inter VLAN. Cada una utiliza una configuración de router diferente para realizar la tarea de enrutamiento entre VLAN. En este tema, observaremos cómo cada tipo de configuración de interfaz del router enruta entre las VLAN, y sus ventajas y desventajas. Comenzaremos por revisar el modelo tradicional.

Uso del router como gateway

El enrutamiento tradicional requiere de routers que tengan interfaces físicas múltiples para facilitar el enrutamiento inter VLAN. El router realiza el enrutamiento al conectar cada una de sus interfaces físicas a una VLAN única. Además, cada interfaz está configurada con una dirección IP para la subred asociada con la VLAN conectada a ésta. Al configurar las direcciones IP en las interfaces físicas, los dispositivos de red conectados a cada una de las VLAN pueden comunicarse con el router utilizando la interfaz física conectada a la misma VLAN. En esta configuración los dispositivos de red pueden utilizar el router como un gateway para acceder a los dispositivos conectados a las otras VLAN.

El proceso de enrutamiento requiere del dispositivo de origen para determinar si el dispositivo de destino es local o remoto con respecto a la subred local. El dispositivo de origen realiza esta acción comparando las direcciones de origen y destino con la máscara de subred. Una vez que se determinó que la dirección de destino está en una red remota, el dispositivo de origen debe identificar si es necesario reenviar el paquete para alcanzar el dispositivo de destino. El dispositivo de origen examina la tabla de enrutamiento local para determinar si es necesario enviar los datos. Generalmente, los dispositivos utilizan los gateways predeterminados como destino para todo el tráfico que necesita abandonar la subred local. El gateway predeterminado es la ruta que el dispositivo utiliza cuando no tiene otra ruta explícitamente definida hacia la red de destino. La interfaz del router en la subred local actúa como el gateway predeterminado para el dispositivo emisor.

Una vez que el dispositivo de origen determinó que el paquete debe viajar a través de la interfaz del router local en la VLAN conectada, el dispositivo de origen envía una solicitud de ARP para determinar la dirección MAC de la interfaz del router local. Una vez que el router reenvía la respuesta ARP al dispositivo de origen, éste puede utilizar la dirección MAC para finalizar el entramado del paquete, antes de enviarlo a la red como tráfico unicast.

Dado que la trama de Ethernet tiene la dirección MAC de destino de la interfaz del router, el switch sabe exactamente a qué puerto del switch reenviar el tráfico unicast para alcanzar la interfaz del router en dicha VLAN. Cuando la trama llega al router, el router elimina la información de la dirección MAC de origen y destino para examinar la dirección IP de destino del paquete. El router compara la dirección de destino con las entradas en la tabla de enrutamiento para determinar si es necesario reenviar los datos para alcanzar el destino final. Si el router determina que la red de destino es una red conectada en forma local, como sería el caso en el enrutamiento inter VLAN, el router envía una solicitud de ARP fuera de la interfaz conectada físicamente a la VLAN de destino. El dispositivo de destino responde al router con la dirección MAC, la cual luego utiliza el router para entramar el paquete. El router envía el tráfico unicast al switch, que lo reenvía por el puerto donde se encuentra conectado el dispositivo de destino.

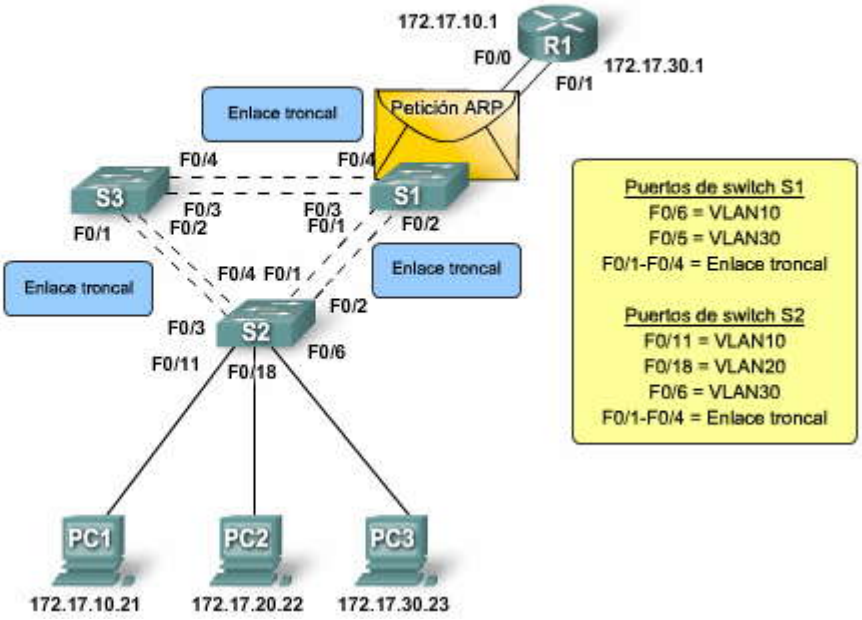
Haga clic en el botón Reproducir que se muestra en la figura para ver cómo se realiza el enrutamiento tradicional.

Aunque existen muchos pasos en el proceso de enrutamiento inter VLAN cuando dos dispositivos en diferentes VLAN se comunican a través de un router, el proceso completo se produce en una fracción de segundo.

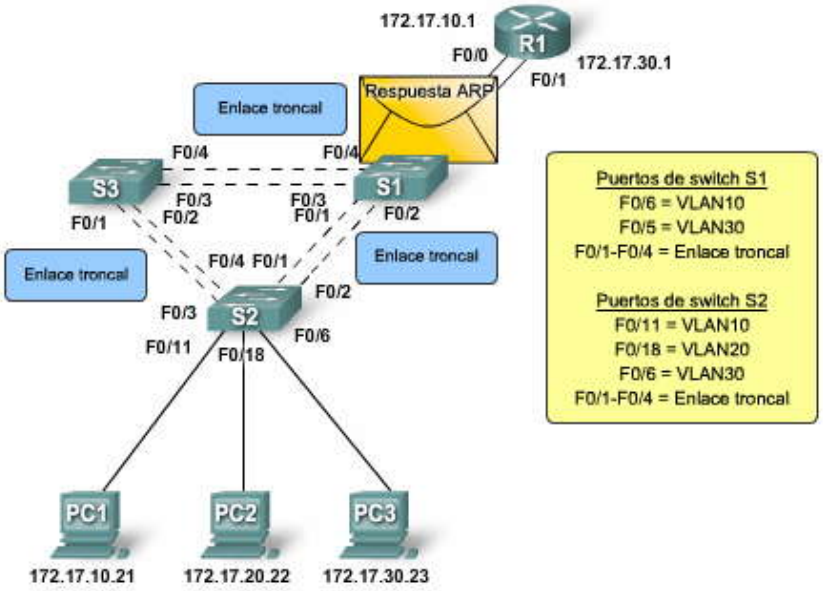
Interfaces del router y enrutamiento entre VLAN

La PC1 envía un broadcast de petición de ARP en la VLAN10 para determinar su dirección MAC de gateway. Recuerde que el gateway para esta PC será la interfaz más próxima al router. El broadcast de petición de ARP se reenvía por el switch S2 a todos los puertos asignados a VLAN10, y el enlace troncal se conecta al switch S1.

La trama de broadcast de petición de ARP se etiqueta con VLAN10 a medida que atraviesa el enlace troncal entre los switches S2 y S1. El switch S1 elimina la etiqueta VLAN y reenvía la trama por los puertos configurados para VLAN10, incluso el puerto F0/6 que está conectado al router R1.



El router R1 envía una respuesta ARP con la dirección MAC física de la interfaz F0/0 de vuelta a la PC1.



La PC1 entrama los datos y los reenvía como tráfico unicast al router R1 a través de los switches S2 y S1. Una vez que el router R1 acepta la trama, elimina las direcciones MAC de origen y destino originales y examina la dirección IP de destino para determinar dónde reenviar el paquete.

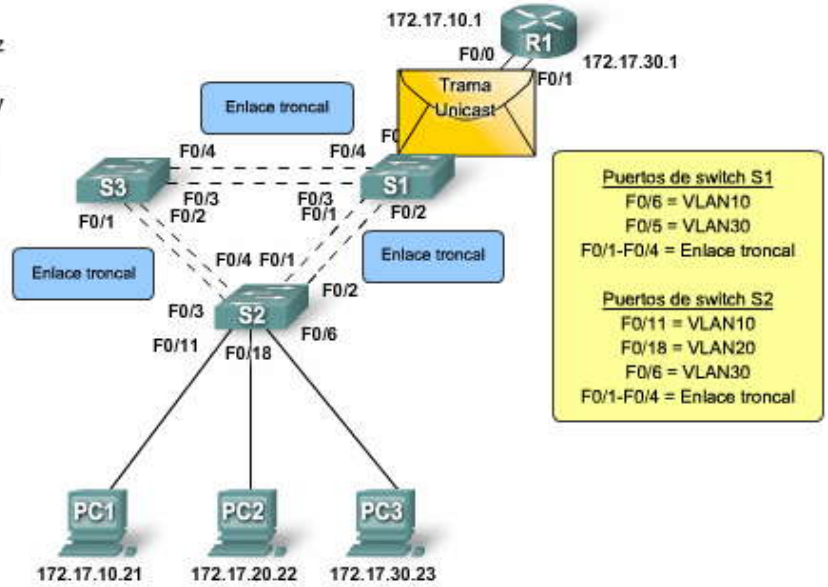
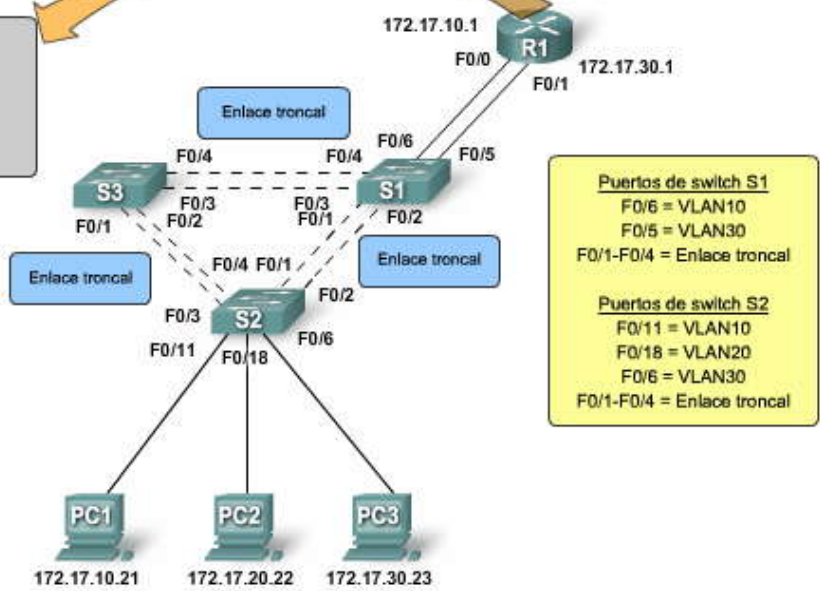
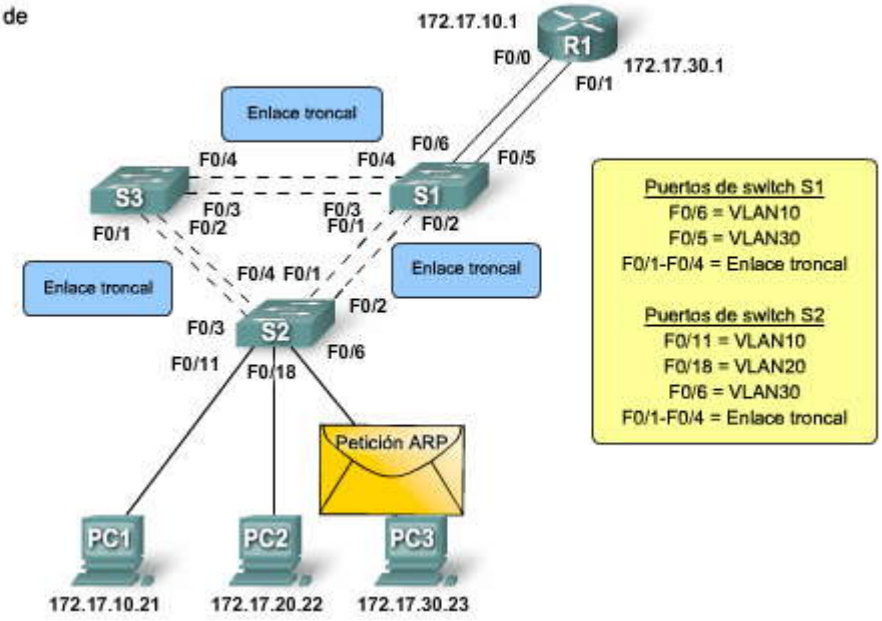


Tabla de enrutamiento
172.17.30.0 is directly connected, FastEthernet0/0.30
172.17.10.0 is directly connected, FastEthernet0/0.10

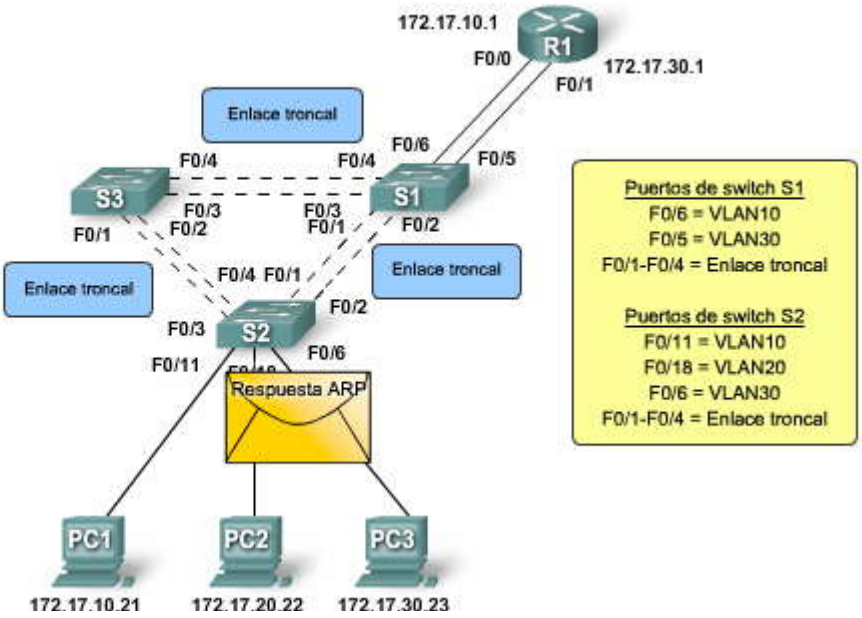
El router R1 compara la dirección con las rutas configuradas en su tabla de enrutamiento local. El router R1 identifica que la red de destino está conectada de forma local a la interfaz F0/1, de manera que prosigue a enviar una petición de ARP para la PC3 en la VLAN30.



El broadcast de petición de ARP atraviesa el switch S1 y el S2 saliendo de todos los puertos configurados para VLAN30, donde llega a la PC3.

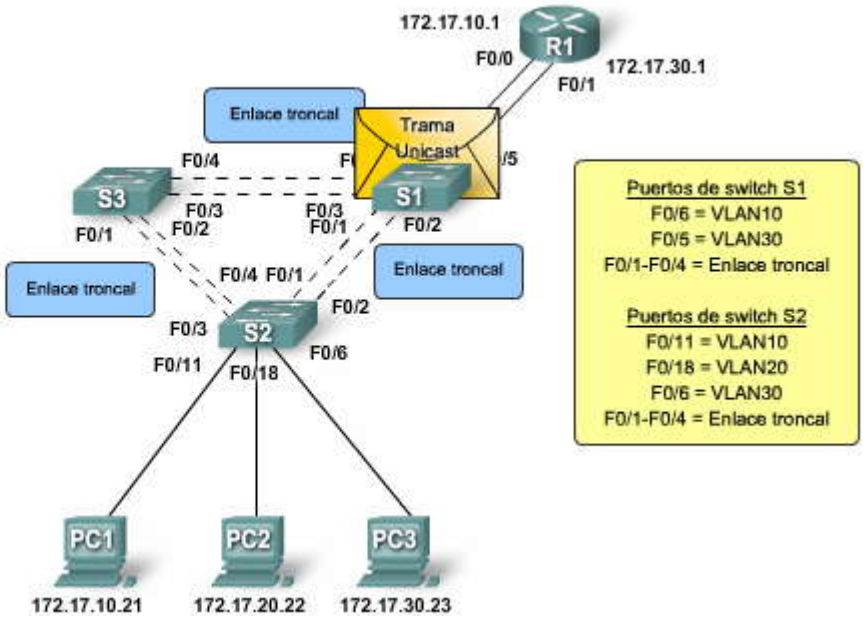


La PC3 luego envía una respuesta de ARP de vuelta al router R1 con su dirección MAC local.



Una vez que el router R1 ha recibido la respuesta de ARP, el router entonces entrama el paquete con las nuevas direcciones MAC de destino y origen y reenvía la trama a la VLAN local, VLAN30.

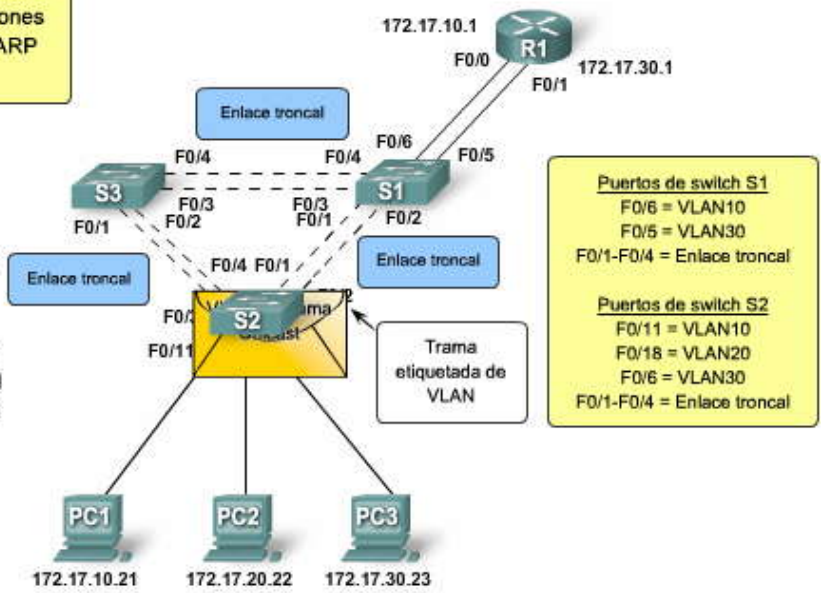
El switch S1 reenvía la trama al switch S2 donde sale por el puerto F0/6 a PC3.



NOTA: No se necesitan los ARP debido a que R1 y PC3 ya conocen las direcciones MAC entre ellas del intercambio de ARP anterior.

La PC3 necesita responder a la PC1 para confirmar que recibió los datos enviados desde la PC1.

Como la PC3 ya tiene la dirección MAC de la interfaz F0/1 del router R1 de la petición de ARP anterior que el router envío, no necesita reenviar una petición de ARP antes de que pueda entramar el paquete que está enviando a la PC1. La PC3 envía el paquete entramado destinado para la PC1 al router R1 con la dirección MAC de destino de la interfaz F0/1 en el router R1 en VLAN30.



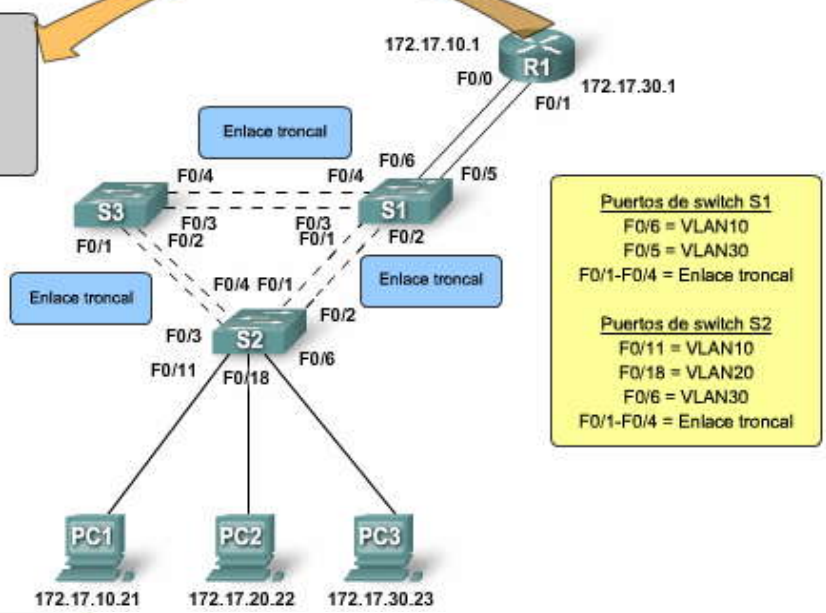
Puertos de switch S1
F0/6 = VLAN10
F0/5 = VLAN30
F0/1-F0/4 = Enlace troncal

Puertos de switch S2
F0/11 = VLAN10
F0/18 = VLAN20
F0/6 = VLAN30
F0/1-F0/4 = Enlace troncal

Tabla de enrutamiento
172.17.30.0 is directly connected, FastEthernet0/0.30
172.17.10.0 is directly connected, FastEthernet0/0.10

El router R1 recibe la trama y elimina la dirección de origen y destino original para examinar la dirección IP de destino, la dirección IP de PC1, para determinar dónde reenviar el paquete.

El router R1 determina que la interfaz F0/0 local está conectada a la subred correcta y determina que debe usar esa interfaz física para enviar el paquete de regreso a la PC1.

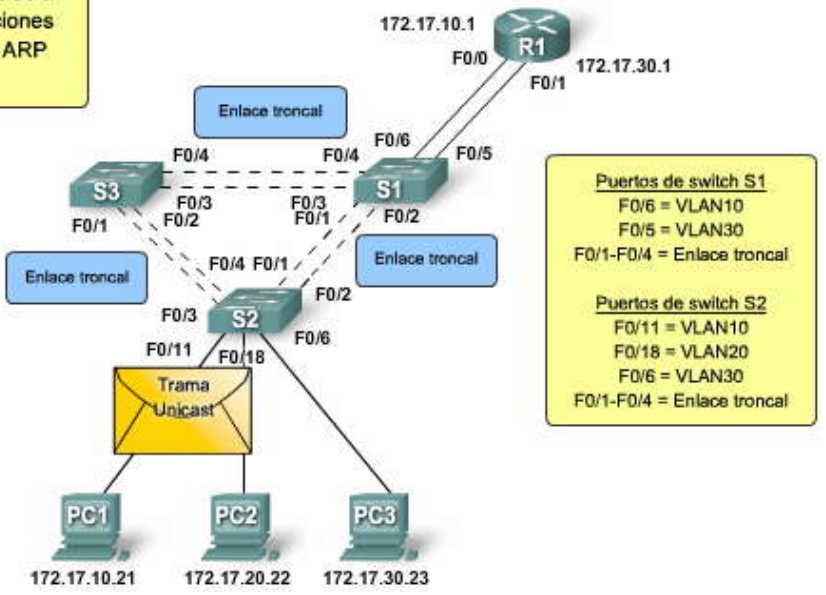


Puertos de switch S1
F0/6 = VLAN10
F0/5 = VLAN30
F0/1-F0/4 = Enlace troncal

Puertos de switch S2
F0/11 = VLAN10
F0/18 = VLAN20
F0/6 = VLAN30
F0/1-F0/4 = Enlace troncal

NOTA: No se necesitan los ARP debido a que R1 y PC1 ya conocen las direcciones MAC entre ellas del intercambio de ARP anterior.

El router R1 entrama el paquete con la dirección MAC de destino de PC1, que todavía recuerda del intercambio de ARP original entre la PC1 y el router R1. El router R1 luego reenvía la trama al switch S1, que luego la reenvía al switch S2, donde la trama es finalmente enviada de regreso a la PC1.



Puertos de switch S1
F0/6 = VLAN10
F0/5 = VLAN30
F0/1-F0/4 = Enlace troncal

Puertos de switch S2
F0/11 = VLAN10
F0/18 = VLAN20
F0/6 = VLAN30
F0/1-F0/4 = Enlace troncal

Configuración de la interfaz

Haga clic en el botón Configuración de la interfaz que se muestra en la figura para ver un ejemplo de las interfaces del router que se están configurando.

Las interfaces del router se configuran de manera similar a las interfaces VLAN en los switches. En el modo de configuración global, conmute al modo configuración de la interfaz para la interfaz específica que desea configurar.

Como muestra el ejemplo, la interfaz F0/0 está configurada con la dirección IP 172.17.10.1 y la máscara de subred 255.255.255.0 utiliza el comando **ip address 172.17.10.1 255.255.255.0.**

Para habilitar una interfaz del router, es necesario ingresar el comando **no shutdown** para la interfaz. Observe que también se configuró la interfaz F0/1. Después de asignar ambas direcciones IP a cada una de las interfaces físicas, el router puede realizar el enrutamiento.

Haga clic en el botón Tabla de enrutamiento que se muestra en la figura para ver un ejemplo de una tabla de enrutamiento en un router Cisco.

Tabla de enrutamiento

Como puede ver en el ejemplo, la tabla de enrutamiento tiene dos entradas, una para la red 172.17.10.0 y la otra para la red 172.17.30.0. Observe la letra C a la izquierda de cada entrada de ruta. Esta letra indica que la ruta es local para una interfaz conectada, que también está identificada en la entrada de ruta. En base al resultado en este ejemplo, si el tráfico estuviera destinado para la subred 172.17.30.0, el router debería reenviar el tráfico fuera de la interfaz F0/1.

El enrutamiento inter VLAN tradicional que utiliza interfaces físicas tiene una limitación. A medida que aumenta la cantidad de VLAN en una red, el enfoque físico de tener una interfaz del router por VLAN se vuelve rápidamente dificultoso debido a las limitaciones del hardware de un router. Los routers tienen una cantidad limitada de interfaces físicas que pueden utilizar para conectar las distintas VLAN. Las redes grandes con muchas VLAN deben utilizar enlace troncal de VLAN para asignar múltiples VLAN a una interfaz del router única, para funcionar dentro de las restricciones de hardware de los routers dedicados.

Configuración de la interfaz

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f0/0
R1(config-if)#ip address 172.17.10.1 255.255.255.0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R1(config-if)#interface f0/1
R1(config-if)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
R1(config-if)#end
%SYS-5-CONFIG I: Configured from console by console
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 2 subnets
C       172.17.30.0 is directly connected, FastEthernet0/1
C       172.17.10.0 is directly connected, FastEthernet0/0
```

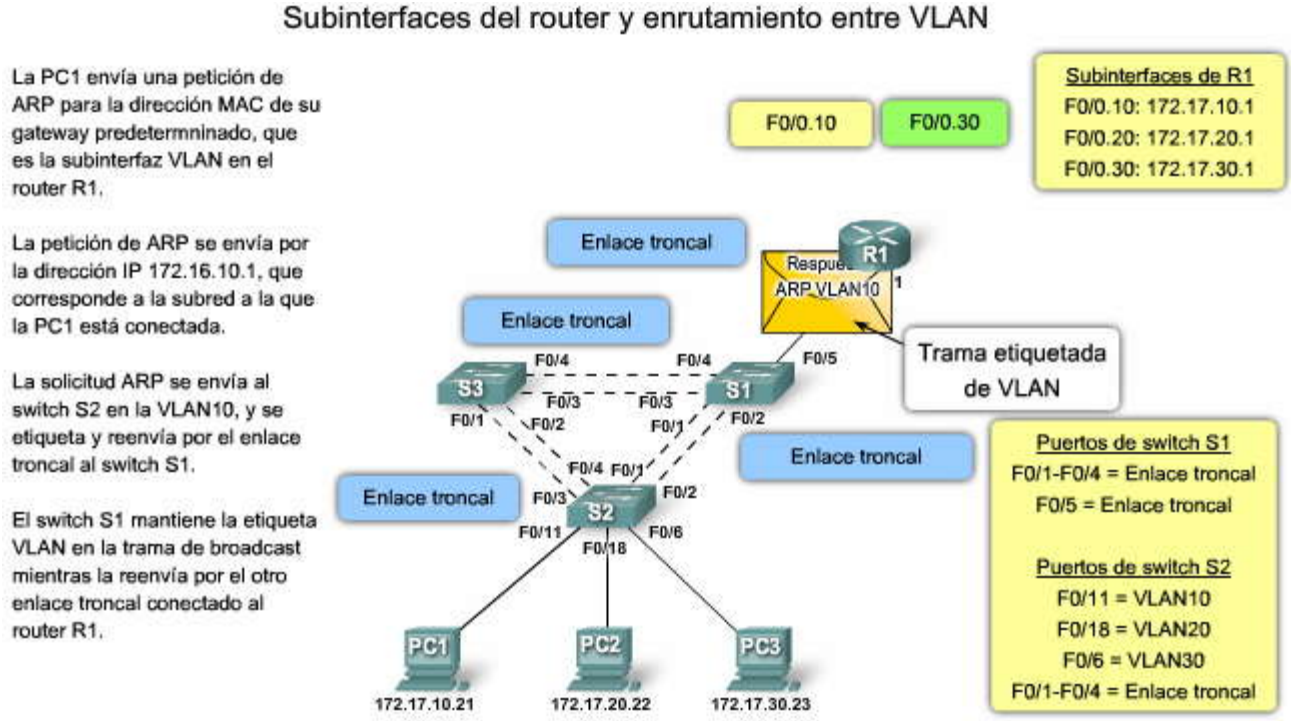
Para superar las limitaciones de hardware del enrutamiento inter VLAN basado eninterfaces físicas del router, se utilizan subinterfaces virtuales y enlaces troncales, como en el ejemplo del router-on-a-stick descrito anteriormente. Las subinterfaces son interfaces virtuales basadas en software asignadas a interfaces físicas. Cada subinterfaz se configura con su propia dirección IP, máscara de subred y asignación de VLAN única, permitiendo que una interfaz física única sea parte en forma simultánea de múltiples redes lógicas. Esto resulta útil cuando se realiza el enrutamiento inter VLAN en redes con múltiples VLAN y pocas interfaces físicas del router.

Al configurar el enrutamiento inter VLAN mediante el modelo router-on-a-stick, la interfaz física del router debe estar conectada al enlace troncal en el switch adyacente. Las subinterfaces se crean para cada VLAN/subred única en la red. A cada subinterfaz se le asigna una dirección IP específica a la subred de la cual será parte y se configura en tramas con etiqueta de la VLAN para la VLAN con la cual interactuará la interfaz. De esa manera, el router puede mantener separado el tráfico de cada subinterfaz a medida que atraviesa el enlace troncal hacia el switch.

Funcionalmente, el modelo router-on-a-stick para el enrutamiento inter VLAN es el mismo que se utiliza para el modelo de enrutamiento tradicional, pero en lugar de utilizar las interfaces físicas para realizar el enrutamiento, se utilizan las subinterfaces de una interfaz única.

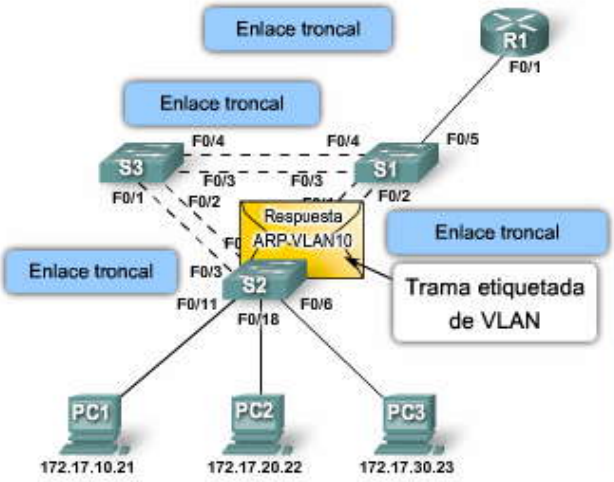
Analicemos un ejemplo. En la figura, PC1 desea comunicarse con PC3. PC1 está en la VLAN10 y PC3 está en la VLAN30. Para que PC1 se comunique con PC3, PC1 necesita tener los datos enrutados a través del router R1 mediante las subinterfaces configuradas.

Haga clic en el botón Reproducir que se muestra en la figura para ver cómo se utilizan las subinterfaces para enrutar entre las VLAN.



El router R1 examina la etiqueta VLAN en el broadcast y reconoce que fue enviada en la VLAN10.

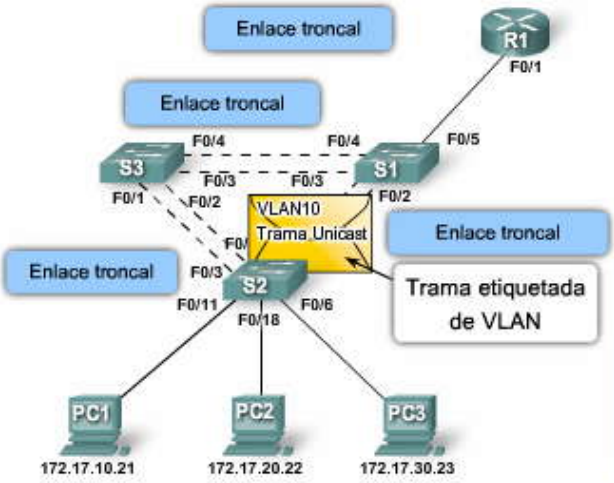
Como la subinterfaz F0/0.10 ha sido configurada para la VLAN10, y ha sido configurada con la dirección IP especificada en la petición de ARP, el router responds a la PC1 con la dirección MAC de la interfaz física.

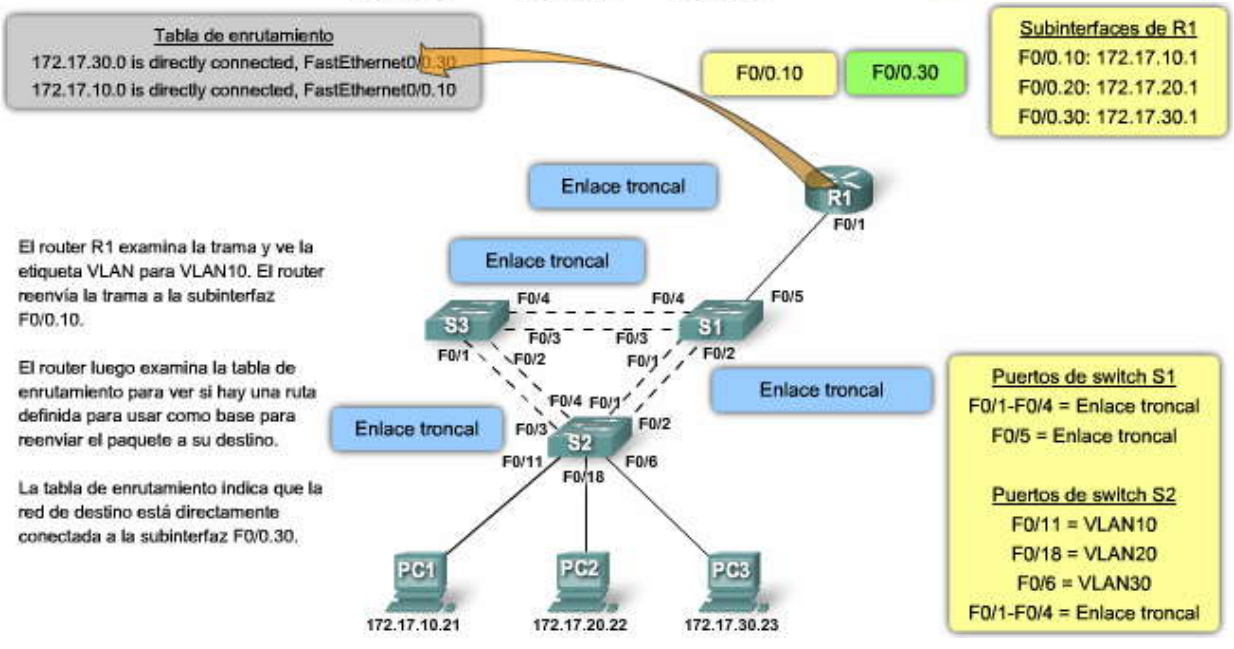


La PC1 usa la dirección MAC recibida del router R1 para entramar el paquete unicast antes de que se envíe por la red.

El switch S2 etiqueta la trama en la VLAN10 mientras atraviesa el enlace troncal al switch S1.

El switch S1 mantiene la etiqueta VLAN mientras continúa enviando la trama al router R1.





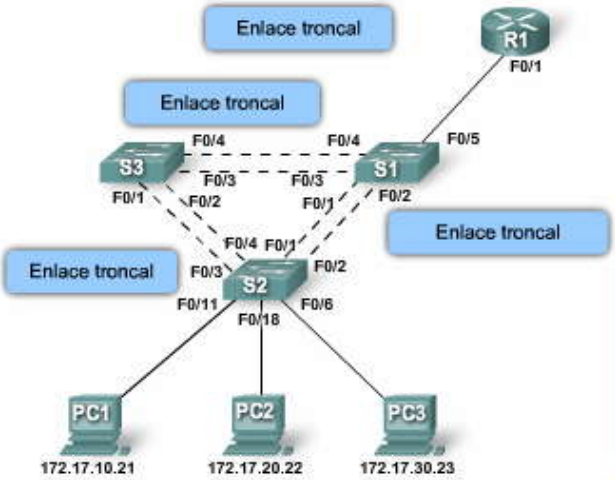
El router R1 examina la trama y ve la etiqueta VLAN para VLAN10. El router reenvía la trama a la subinterfaz F0/0.10.

El router luego examina la tabla de enrutamiento para ver si hay una ruta definida para usar como base para reenviar el paquete a su destino.

La tabla de enrutamiento indica que la red de destino está directamente conectada a la subinterfaz F0/0.30.

Subinterfaces de R1
F0/0.10: 172.17.10.1
F0/0.20: 172.17.20.1
F0/0.30: 172.17.30.1

El router luego reenvía el paquete a la subinterfaz F0/0.30.



Puertos de switch S1
F0/1-F0/4 = Enlace troncal
F0/5 = Enlace troncal

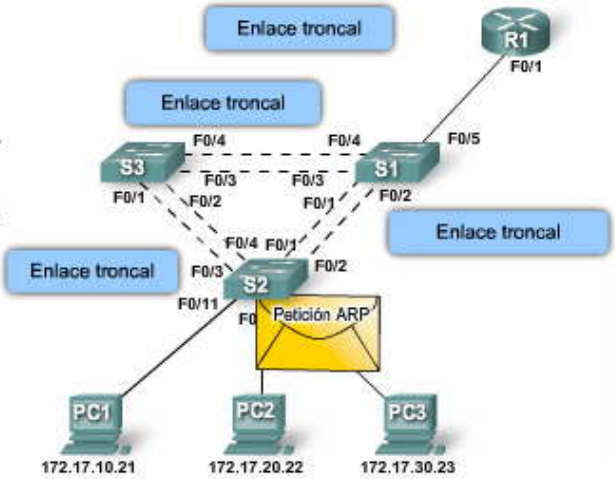
Puertos de switch S2
F0/11 = VLAN10
F0/18 = VLAN20
F0/6 = VLAN30
F0/1-F0/4 = Enlace troncal

Subinterfaces de R1
F0/0.10: 172.17.10.1
F0/0.20: 172.17.20.1
F0/0.30: 172.17.30.1

R1 envía una nueva petición de ARP por la dirección MAC de PC3.

La petición de ARP se envía de la interfaz física del router etiquetada con VLAN30.

La PC3 recibe la petición de ARP.

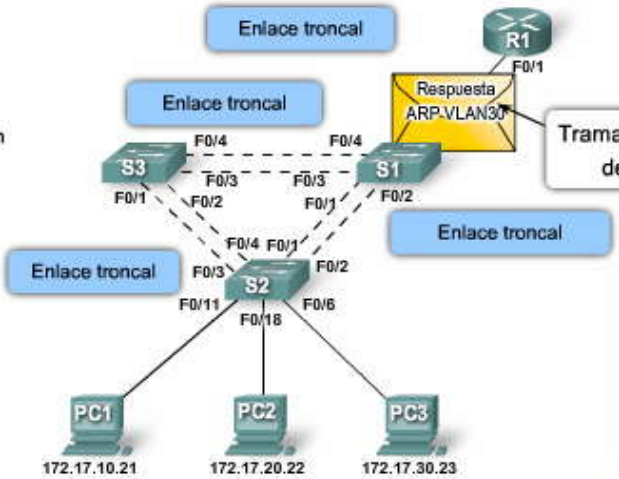


Puertos de switch S1
F0/1-F0/4 = Enlace troncal
F0/5 = Enlace troncal

Puertos de switch S2
F0/11 = VLAN10
F0/18 = VLAN20
F0/6 = VLAN30
F0/1-F0/4 = Enlace troncal

Subinterfaces de R1
F0/0.10: 172.17.10.1
F0/0.20: 172.17.20.1
F0/0.30: 172.17.30.1

La PC3 le envía de regreso una respuesta de ARP con su dirección MAC.

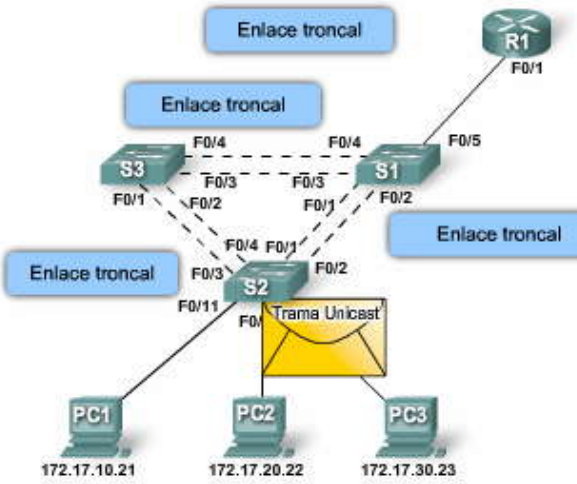


Puertos de switch S1
F0/1-F0/4 = Enlace troncal
F0/5 = Enlace troncal

Puertos de switch S2
F0/11 = VLAN10
F0/18 = VLAN20
F0/6 = VLAN30
F0/1-F0/4 = Enlace troncal

El router R1 recibe la respuesta ARP y termina el entramado del paquete antes de enviarlo por la red.

El switch S1 reenvía la trama al switch S2, que luego finalmente entrega la trama a la PC3.



La PC3 envía una trama unicast de regreso a la PC1.

Sin embargo, esta vez, los broadcasts de ARP no son necesarios ya que las direcciones MAC de los dispositivos adyacentes ya se conocen.

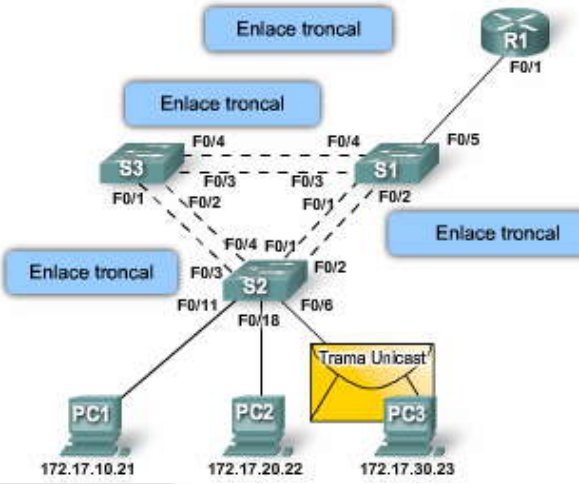
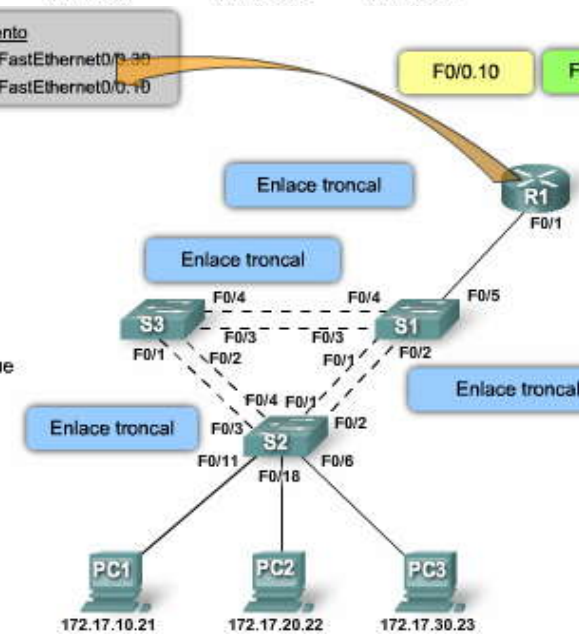
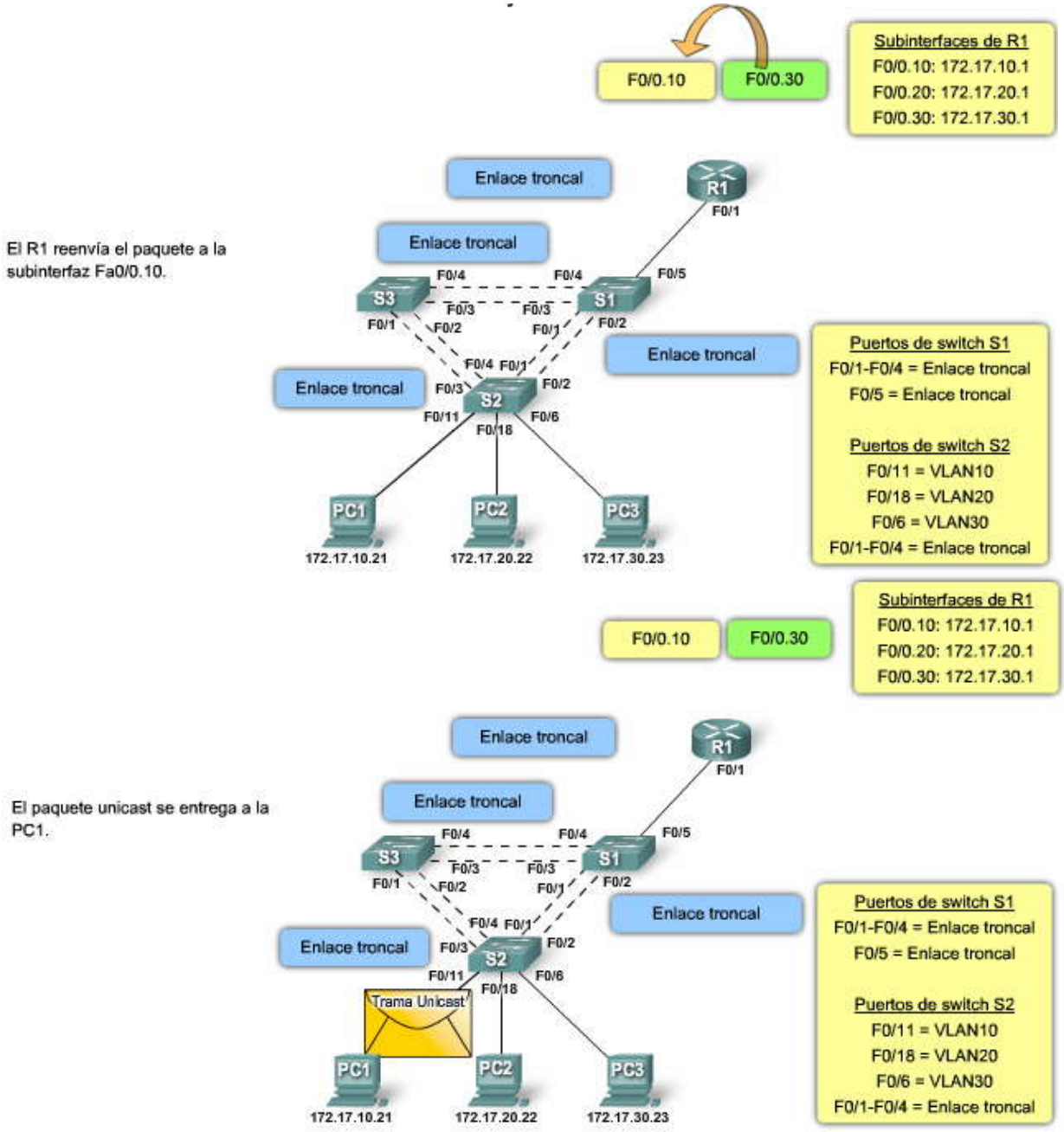


Tabla de enrutamiento
172.17.30.0 is directly connected, FastEthernet0/0.30
172.17.10.0 is directly connected, FastEthernet0/0.10

El R1 usa su tabla de enrutamiento para determinar que la dirección de la red de destino del paquete unicast de la PC3 está directamente conectado a Fa0/0.10.





Configuración de la subinterfaz

La configuración de las subinterfaces del router es similar a la configuración de las interfaces físicas, excepto que es necesario crear la subinterfaz y asignarla a una VLAN.

En el ejemplo, ingrese el comando interface f0/0.10 en el modo de configuración global para crear la subinterfaz del router. La sintaxis para la subinterfaz es siempre la interfaz física, en este caso f0/0, seguida de un punto y un número de subinterfaz. El número de la subinterfaz es configurable, pero generalmente está asociado para reflejar el número de VLAN. En el ejemplo, las subinterfaces utilizan 10 y 30 como números de subinterfaz para recordar con más facilidad las VLAN a las que se encuentran asociadas. La interfaz física está especificada porque puede haber múltiples interfaces en el router, cada una configurada para admitir muchas subinterfaces.

Antes de asignar una dirección IP a una subinterfaz, es necesario configurar la subinterfaz para que funcione en una VLAN específica mediante el comando encapsulation dot1q vlan id. En el ejemplo, la subinterfaz Fa0/0.10 está asignada a la VLAN10. Una vez asignada la VLAN, el comando ip address 172.17.10.1 255.255.255.0 asigna la subinterfaz a la dirección IP apropiada para esa VLAN.

A diferencia de una interfaz física típica, las subinterfaces no están habilitadas con el comando no shutdown en el nivel de modo de configuración de la subinterfaz del software IOS de Cisco. Sin embargo, cuando la interfaz física está habilitada con el comando no shutdown, todas las subinterfaces configuradas están habilitadas. De manera similar, si la interfaz física está deshabilitada, todas las subinterfaces están deshabilitadas.

Haga clic en el botón Tabla de enrutamiento que se muestra en la figura para ver un ejemplo de una tabla de enrutamiento cuando las subinterfaces están configuradas.

Resultado de la tabla del router
Como muestra la figura, las rutas definidas en la tabla de enrutamiento indican que están asociadas con las subinterfaces específicas, en lugar de las interfaces físicas separadas.

Una ventaja de utilizar un enlace troncal es que se reduce el número de puertos del switch y del router. Esto no sólo permite un ahorro de dinero sino también reduœ la complejidad de la configuración. Como consecuencia, el enfoque de la subinterfaz del router puede ampliarse hasta un número mucho más alto de VLAN que una configuración con una interfaz física por diseño de VLAN.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface f0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#interface f0/0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
R1(config-if)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 2 subnets
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.30.0 is directly connected, FastEthernet0/0.30
```

Como hemos analizado, tanto las interfaces físicas como las subinterfaces se utilizan para realizar el enrutamiento inter VLAN. Éstas son las ventajas y desventajas de cada método.

Límites del puerto
Las interfaces físicas están configuradas para tener una interfaz por VLAN en la red. Enlas redes con muchas VLAN, no es posible utilizar un único router para realizar el enrutamiento inter VLAN. Los routers tienen limitaciones físicas para evitar que contengan una gran cantidad de interfaces físicas. Sin embargo, si es una prioridad evitarel uso de subinterfaces, puede utilizar múltiples routers para realizar el enrutamiento inter VLAN para todas las VLAN.

Las subinterfaces permiten ampliar el router para acomodar más VLAN que las permitidas por las interfaces físicas. El enrutamiento inter VLAN en grandes ambientes con muchas VLAN puede acomodarse mejor si se utiliza una interfaz física única con muchas subinterfaces.

Rendimiento

Debido a que no existe contención para ancho de banda en interfaces físicas separadas, las interfaces físicastienen un mejor rendimiento cuando se las compara con el uso de subinterfaces. El tráfico de cada VLAN conectada tiene acceso al ancho de banda completo de la interfaz física del router conectado a dicha VLAN para el enrutamiento inter VLAN.

Cuando se utilizan subinterfaces para el enrutamiento inter VLAN, el tráfico que se está enrutando compite por ancho de banda en la interfaz física única. En una red ocupada, esto puede causar un cuello de botella en la comunicación. Para balancear la carga de tráfico en una interfaz física, las subinterfaces se configuran en múltiples interfaces físicas, lo que da como resultado una menor contención entre el tráfico de la VLAN.

Puertos de acceso y puertos de enlace troncal

La conexión de las interfaces físicas para el enrutamiento inter VLAN requiere que los puertos del switch estén configurados como puertos de acceso. Las subinterfaces requieren que el puerto del switch esté configurado como un puerto de enlace troncal, para que pueda aceptar el tráfico etiquetado de la VLAN en el enlace troncal. Al utilizar subinterfaces, muchas VLAN pueden enrutarse sobre un enlace troncal único, en lugar de utilizar una interfaz física única para cada VLAN.

Costo

Con respecto a la parte financiera, resulta más económico utilizar subinterfaces, en lugar de interfaces físicas separadas. Los routers que tienen muchas interfaces físicas son más caros que los routers con una interfaz única. Además, si tiene un router con muchas interfaces físicas, cada interfaz está conectada a un puerto del switch separado, lo que consume puertos del switch adicionales en la red. Los puertos del switch son un recurso costoso en switches de alto rendimiento. Al consumir puertos adicionales para las funciones de enrutamiento inter VLAN, el switch y el router elevan el costo total de la solución de enrutamiento inter VLAN.

Complejidad

El uso de subinterfaces para el enrutamiento inter VLAN tiene como resultado una configuración física menos compleja que el uso de interfaces físicas separadas, debido a que la cantidad de cables de red física que interconectan el router con el switch es menor. Con menos cables, hay menos confusión acerca de dónde está conectado el cable en el switch. Dado que las VLAN son entroncadas en un enlace único, resulta más fácil resolver el problema de las conexiones físicas.

Por otro lado, el uso de subinterfaces con un puerto de enlace troncal tiene como resultado una configuración de software más compleja, que puede ser difícil de solucionar en caso de presentarse problemas. En el modelo router-on-a-stick se utiliza sólo una interfaz única para acomodar todas las VLAN. Si una VLAN tiene problemas al enrutarse con otras VLAN, no puede simplemente rastrear el cable para ver si éste está conectado en el puerto correcto. Es necesario verificar si el puerto del switch está configurado para ser un enlace troncal y también que la VLAN no esté siendo filtrada en ninguno de los enlaces troncales antes de que llegue a la interfaz del router. Además, es necesario verificar si la subinterfaz del router está configurada para utilizar el ID de la VLAN y la dirección IP correctos, para la subred asociada con dicha VLAN.

Comparación de la interfaz del router y las subinterfaz

Interfaz física	Subinterfaz
Una interfaz física por VLAN	Una interfaz física para muchas VLAN
No existe contención de ancho de banda	Contención de ancho de banda
Conectado para acceder al modo puerto de switch	Conectado para establecer el enlace troncal en el modo puerto de switch
Más costoso	Menos costoso
Configuración de la conexión más compleja	Configuración de la conexión menos compleja

6.2 CONFIGURACION DEL ENRUTAMIENTO INTER VLAN

6.2.1 CONFIGURAR EL ENRUTAMIENTO INTER VLAN.-

En este tema aprenderá a configurar un router IOS Cisco para el enrutamiento inter VLAN, así como también a revisar los comandos necesarios para configurar un switch para admitir el enrutamiento inter VLAN.

Antes de configurar el router, configure el switch al cual se conectará el router. Como muestra la figura, el router R1 está conectado a los puertos del switch F0/4 y F0/5, que se configuraron para las VLAN 10 y 30 respectivamente.

Haga clic en el botón Configuración del switch que se muestra en la figura para ver un ejemplo de configuración del switch.

Para revisar, las VLAN se crean en el modo de configuración global mediante el comando **vlan** vlan id. En este ejemplo las VLAN 10 y 30 se crearon en el switch S1.

Una vez creadas las VLAN, se asignan a los puertos del switch a los que se conectará el router. Para realizar esta tarea, se ejecuta el comando **switchport access vlan** vlan id desde el modo de configuración de la interfaz en el switch para cada interfaz a la cual se conectará el router.

En este ejemplo, las interfaces F0/4 y F0/11 se configuraron en la VLAN 10 con el comando **switchport access vlan 10**. El mismo proceso se utilizó para asignar la VLAN30 a la interfaz F0/5 y F0/6 en el switch S1.

Finalmente, para proteger la configuración y no perderla después de una recarga del switch, se ejecuta el comando **copy running-config startup-config** en el modo EXEC privilegiado para guardar una copia de seguridad de la configuración en ejecución en la configuración de inicio.

Haga clic en el botón Configuración de las interfaces del router que se muestra en la figura para ver un ejemplo de configuración del router.

Luego, se puede configurar el router para realizar el enrutamiento inter VLAN.

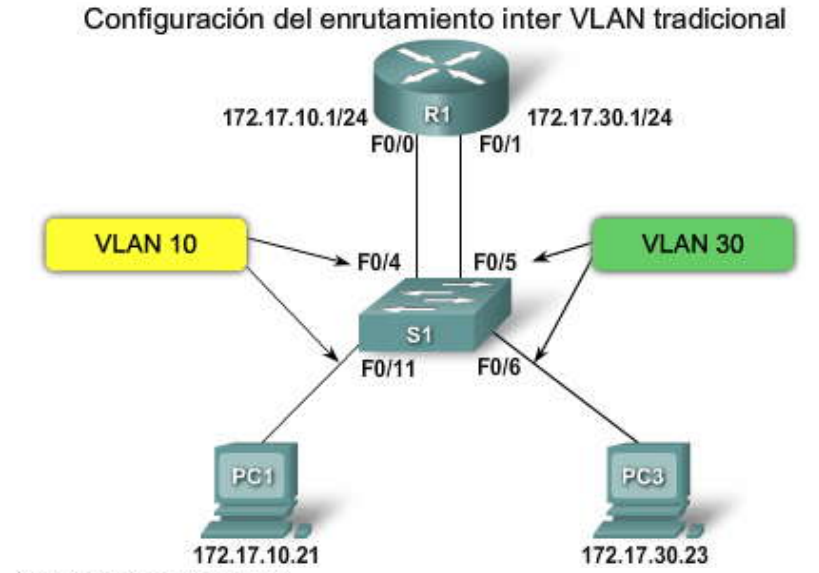
Como muestra la figura, cada interfaz está configurada con una dirección IP mediante el comando ip address ip_address subnet_mask en el modo configuración de la interfaz.

Las interfaces del router están deshabilitadas de manera predeterminada y es necesario habilitarlas con el comando no shutdown antes de utilizarlas.

En este ejemplo, la interfaz F0/0 se asignó a la dirección IP de 172.17.10.1 mediante el comando **ip address 172.17.10.1 255.255.255.0.** También observe que se ejecutó el comando **no shutdown** en el modo de configuración de la interfaz. Se muestra una notificación que indica el cambio de estado de la interfaz; la interfaz ahora se encuentra habilitada.

El proceso se repite para todas las interfaces del router. Es necesario asignar cada interfaz del router a una subred única para que se produzca el enrutamiento. En este ejemplo, la otra interfaz del router, F0/1, se configuró para utilizar la dirección IP 172.17.30.1, que está en una subred diferente a la interfaz F0/0.

Los routers Cisco están configurados de manera predeterminada para enrutar el tráfico entre las interfaces locales. Por lo tanto, no es necesario que esté habilitado el enrutamiento. Sin embargo, si se configuran múltiples routers para realizar el enrutamiento inter VLAN, tal vez desee habilitar un protocolo de enrutamiento dinámico para simplificar la administración de la tabla de enrutamiento. Si no realizó el curso CCNA Exploration: Conceptos y protocolos de enrutamiento, puede aprender más en el sitio de Cisco: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca760.html.




```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#vlan 30
S1(config-vlan)#exit
S1(config)#interface f0/11
S1(config-if)#switchport access vlan 10
S1(config-if)#interface f0/4
S1(config-if)#switchport access vlan 10
S1(config-if)#interface f0/6
S1(config-if)#switchport access vlan 30
S1(config-if)#interface f0/5
S1(config-if)#switchport access vlan 30
S1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
```

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f0/0
R1(config-if)#ip address 172.17.10.1 255.255.255.0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R1(config-if)#interface f0/1
R1(config-if)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
R1(config-if)#end
R1#copy running-config startup-config
```

Tabla de enrutamiento

Ahora examine la tabla de enrutamiento mediante el comando show ip route en el modo EXEC privilegiado.

En el ejemplo, hay dos rutas en la tabla de enrutamiento. Una ruta es a la subred 172.17.10.0, que está conectada a la interfaz local F0/0. La otra ruta es a la subred 172.17.30.0, que está conectada a la interfaz local F0/1. El router utiliza esta tabla de enrutamiento para determinar dónde enviar el tráfico que recibe. Por ejemplo: si el router recibe un paquete en la interfaz F0/0 destinado a la subred 172.17.30.0, el router identificará que debe enviar el paquete fuera de la interfaz F0/1 para alcanzar los hosts en la subred 172.17.30.0.

Haga clic en el botón Verificar la configuración del router que se muestra en la figura para ver un ejemplo de configuración del router.

Verificar configuración del router

Para verificar la configuración del router, utilice el comando **show running-config** en el modo EXEC privilegiado. Este comando muestra la configuración operativa actual del router. Puede ver las direcciones IP que se configuraron para cada una de las interfaces del router, así como también el estado operativo de la interfaz.

En este ejemplo, observe que la interfaz F0/0 está configurada correctamente con la dirección IP 172.17.10.1. Además, observe la ausencia del comando **shutdown** debajo de la interfaz F0/0. La ausencia del comando **shutdown** confirma que se ejecutó el comando **no shutdown** y se habilitó la interfaz.

Puede obtener información más detallada sobre las interfaces del router, como información de diagnóstico, estado, dirección MAC y errores de transmisión y recepción, mediante el comando **show interface** en el modo EXEC privilegiado.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

        172.17.0.0/24 is subnetted, 2 subnets
C       172.17.10.0 is directly connected, FastEthernet0/0
C       172.17.30.0 is directly connected, FastEthernet0/1
```

```
R1#show run
Building configuration...
Current configuration : 358 bytes
version 12.3
no service password-encryption
!
hostname R1
!
interface FastEthernet0/0
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.17.30.1 255.255.255.0
!
ip classless
!
line con 0
line vty 0 4
 login
!
end
```

6.2.2 CONFIGURAR EL ENRUTAMIENTO INTER VLAN DEL ROUTER-ON-A-STICK.-

Antes de configurar el router, configure el switch al cual éste se conectará.

Como muestra la figura, el router R1 está conectado al switch S1 en el puerto de enlace troncal F0/5. También se agregaron las VLAN 10 y 30 al switch S1.

Haga clic en el botón Configuración del switch que se muestra en la figura para ver un ejemplo de configuración del switch.

Para revisar, las VLAN se crean en el modo de configuración global mediante el comando **vlan** vlan id. En este ejemplo, las VLAN 10 y 30 se crearon en el switch S1 con los comandos **vlan 10** y **vlan 30**.

Dado que el puerto del switch F0/5 se configura como un puerto de enlace troncal, el usuario no tiene que asignar ninguna VLAN al puerto. Para configurar el puerto del switch F0/5 como un puerto de enlace troncal, ejecute el comando **switchport mode trunk** en el modo de configuración de la interfaz, en la interfaz F0/5. No puede utilizar los comandos **switchport mode dynamic auto** o **switchport mode dynamic desirable** porque el router no admite el protocolo de enlace troncal dinámico.

Finalmente, para proteger la configuración y no perderla después de una recarga del switch, se ejecuta el comando **copy running-config startup-config** en el modo EXEC privilegiado para guardar una copia de seguridad de la configuración en ejecución en la configuración de inicio.

Haga clic en el botón Configuración del router que se muestra en la figura para ver un ejemplo de configuración del router.

Configuración del router

A continuación, se puede configurar el router para realizar el enrutamiento inter VLAN.

Como muestra la figura, la configuración de múltiples subinterfaces es diferente a cuando se utilizan interfaces físicas.

Cada subinterfaz se crea con el comando interface interface_id.Subinterface_id en el modo de configuración global.En este ejemplo, la subinterfaz Fa0/0.10 se crea mediante el comando interface fa0/0.10 en el modo de configuración global. Una vez creada la subinterfaz, se asigna el ID de la VLAN mediante el comando encapsulation dot1q vlan_id en el modo de configuración de la subinterfaz.

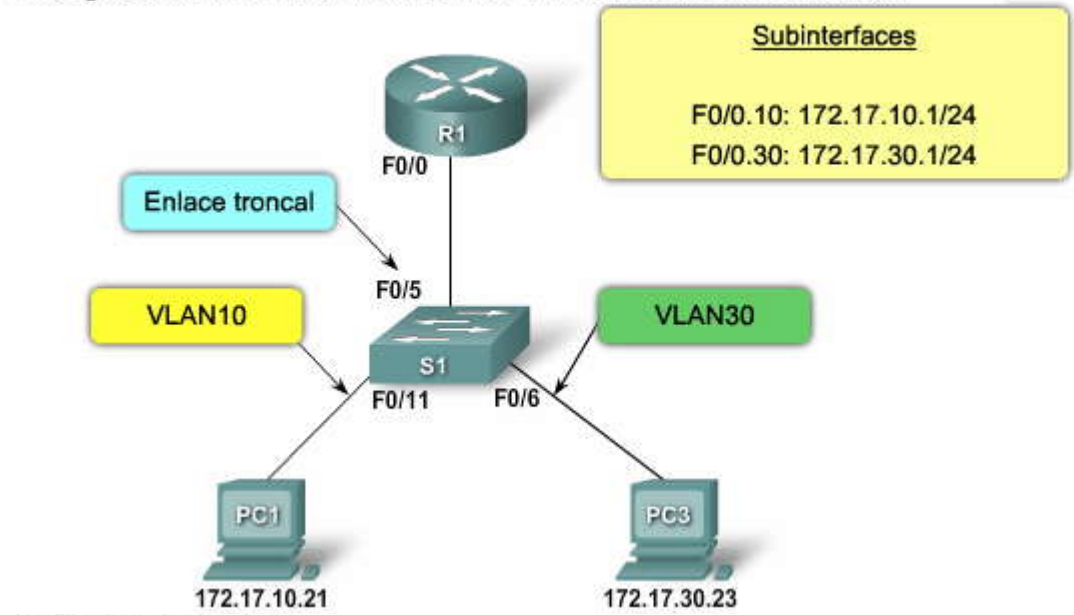
A continuación, asigne la dirección IP para la subinterfaz mediante el comando ip address ip_address subnet_mask en el modo de configuración de la subinterfaz. En este ejemplo, la subinterfaz F0/0.10 es asignada a la dirección IP 172.17.10.1 mediante el comando ip address 172.17.10.1 255.255.255.0. No es necesario que ejecute un comando no shutdown en el nivel de la subinterfaz porque éste no habilita la interfaz física.

Este proceso se repite para todas las subinterfaces del router necesarias para enrutar entre las VLAN configuradas en la red. Es necesario asignar una dirección IP a cada subinterfaz del router en una subred única para que tenga lugar el enrutamiento. En este ejemplo, se configuró la otra subinterfaz del router, F0/030, para utilizar la dirección IP 172.17.30.1, que está en una subred diferente a la subinterfaz F0/0.10.

Una vez configuradas todas las subinterfaces en la interfaz física del router, se habilita la interfaz física. En el ejemplo, la interfaz F0/0 tiene ejecutado el comando no shutdown para habilitar la interfaz, la cual habilita todas las subinterfaces configuradas.

Los routers Cisco están configurados de manera predeterminada para enrutar el tráfico entre las subinterfaces locales. Por lo tanto, no es necesario que esté habilitado el enrutamiento.

Configuración del enrutamiento inter VLAN del Router-on-a- Stick




```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#vlan 30
S1(config-vlan)#exit
S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#end

R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface f0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#interface f0/0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10,
changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30,
changed state to up
R1(config-if)#end
```

Tabla de enrutamiento

Luego, examine la tabla de enrutamiento mediante el comando show ip route en el modo EXEC privilegiado. En el ejemplo, hay dos rutas en la tabla de enrutamiento. Una ruta es la subred 172.17.10.0, que está conectada a la subinterfaz local F0/0.10. La otra ruta es la subred 172.17.30.0, que está conectada a la subinterfaz local F0/0.30. El router utiliza la tabla de enrutamiento para determinar dónde enviar el tráfico que recibe. Por ejemplo: si el router recibe un paquete en la

subinterfaz F0/0.10 destinado a la subred 172.17.30.0, el router identificará que debe enviar el paquete fuera de la subinterfaz F0/0.30 para alcanzar los hosts en la subred 172.17.30.0.

Haga clic en el botón Verificar configuración del router que se muestra en la figura para ver un ejemplo de configuración del router.

Verificar configuración del router

Para verificar la configuración del router, utilice el comando show running-config en el modo EXEC privilegiado. El comando show running-config muestra la configuración operativa actual del router. Observe cuáles son las direcciones IP configuradas para cada subinterfaz del router, así como también si la interfaz física quedó deshabilitada o habilitada, mediante el comando no shutdown.

En este ejemplo, observe que la interfaz F0/0.10 se configuró correctamente con la dirección IP 172.17.10.1. Además, observe la ausencia del comando shutdown debajo de la interfaz F0/0. La ausencia del comando shutdown confirma que se ejecutó el comando no shutdown y se habilitó la interfaz.

Puede obtener información más detallada sobre las interfaces del router, como información de diagnóstico, estado, dirección MAC y errores de transmisión y recepción, mediante el comando show interface en el modo EXEC privilegiado.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

        172.17.0.0/24 is subnetted, 2 subnets
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.30.0 is directly connected, FastEthernet0/0.30
Router#show running-config
<output omitted>
!
hostname R1
!
interface FastEthernet0/0
 no ip address
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.17.30.1 255.255.255.0
!
<output omitted>
!
end
```

Una vez configurados el router y el switch para realizar el enrutamiento inter VLAN, el siguiente paso es verificar que el router funcione correctamente. Puede probar el acceso a los dispositivos en las VLAN remotas utilizando el comando ping.

Para el ejemplo que se muestra en la figura, debe iniciar un ping y un tracert desde PC1 hacia la dirección de destino de PC3.

Prueba de ping

El comando ping envía una solicitud de eco del ICMP a la dirección de destino. Cuando un host recibe una solicitud de eco del ICMP, éste responde con una respuesta de eco del ICMP para confirmar que recibió dicha solicitud. El comando ping calcula el tiempo transcurrido, para lo cual utiliza la diferencia de tiempo entre el momento en que se envió el ping y el momento en que se recibió la respuesta de eco. El tiempo transcurrido se utiliza para determinar la latencia de la conexión. Al recibir una respuesta con éxito, confirma que existe una ruta entre el dispositivo emisor y el dispositivo receptor.

Prueba del tracert

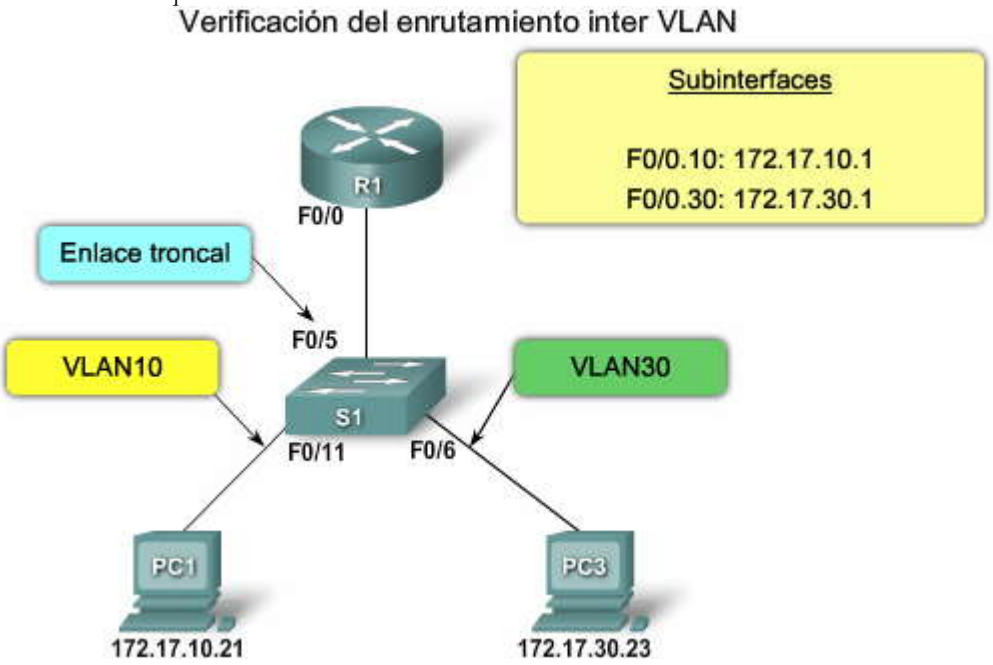
Tracert es una utilidad práctica utilizada para confirmar la ruta enrutada tomada entre dos dispositivos. En los sistemas UNIX, la utilidad está especificada por traceroute. Tracert también utiliza el ICMP para determinar la ruta tomada, pero utiliza las solicitudes de eco del ICMP con valores de tiempo de vida específicos definidos en la trama.

El valor de tiempo de vida determina con exactitud la cantidad de saltos del router que el eco del ICMP puede alcanzar. La primera solicitud de eco del ICMP se envía con un valor de tiempo de vida configurado para expirar en el primer router en la ruta hacia el dispositivo de destino.

Cuando la solicitud de eco del ICMP expira en la primera ruta, se reenvía una confirmación desde el router al dispositivo de origen. El dispositivo registra la respuesta desde el router y procede a enviar otra solicitud de eco del ICMP, pero esta vez con un valor de tiempo de vida mayor. Esto permite a la solicitud de eco del ICMP atravesar el primer router y llegar al segundo dispositivo en la ruta hacia el destino final. El proceso se repite hasta que finalmente se envía la solicitud de eco del ICMP hacia el dispositivo de destino final. Una vez que la utilidad tracert deja de funcionar, se le presenta al usuario una lista de todas las interfaces del router que la solicitud de eco del ICMP alcanzó hasta llegar al destino.

Haga clic en el botón Resultados del dispositivo que se muestra en la figura para ver una muestra del resultado de los comandos ping y tracert.

En el ejemplo, la utilidad ping pudo enviar una solicitud de eco del ICMP a la dirección IP del PC3. Además, la utilidad tracert confirma que la ruta a PC3 es a través de la dirección IP de la subinterfaz 172.17.10.1 del router R1.



```
PC>ping 172.17.30.23

Pinging 172.17.30.23 with 32 bytes of data:

Reply from 172.17.30.23: bytes=32 time=17ms TTL=127
Reply from 172.17.30.23: bytes=32 time=15ms TTL=127
Reply from 172.17.30.23: bytes=32 time=18ms TTL=127
Reply from 172.17.30.23: bytes=32 time=19ms TTL=127

Ping statistics for 172.17.30.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 19ms, Average = 17ms

PC>tracert 172.17.30.23

Tracing route to 172.17.30.23 over a maximum of 30 hops:

  1    9 ms      7 ms      9 ms      172.17.10.1
  2    16 ms     15 ms     16 ms     172.17.30.23

Trace complete.
```

6.3 RESOLUCION DE PROBLEMAS DE ENRUTAMIENTO ENTRE VLAN.-

6.3.1 TEMAS DE CONFIGURACION DEL SWITCH.-

En este tema analizamos los retos asociados con la configuración de múltiples VLAN en una red. Este tema explora los problemas comunes y describe los métodos de resolución de problemas para identificarlos y corregirlos.

Al utilizar el modelo de enrutamiento tradicional para el enrutamiento inter VLAN, asegúrese de que los puertos del switch que conectan a las interfaces del router estén configurados en las VLAN correctas. Si los puertos del switch no están configurados en la VLAN correcta, los dispositivos configurados en dicha VLAN no pueden conectarse a la interfaz del router y en consecuencia no pueden enrutarse a las demás VLAN.

Haga clic en el botón Topología 1 que se muestra en la figura.

Como puede ver en Topología 1, PC1 y la interfaz F0/0 del router R1 están configurados para estar en la misma subred lógica, como lo indica la asignación de la dirección IP. Sin embargo, el puerto del switch F0/4 que conecta a la interfaz F0/0 del router R1 no se configuró y permanece en la VLAN predeterminada. Dado que el router R1 está en una VLAN diferente que PC1, no pueden comunicarse.

Para corregir este problema, ejecute el comando switchport access vlan 10 en la configuración de la interfaz en el puerto del switch F0/4 en el switch S1. Cuando el puerto del switch está configurado para la VLAN correcta, PC1 puede comunicarse con la interfaz F0/0 del router R1, que le permite acceder a las otras VLAN conectadas al router R1.

Haga clic en el botón Topología 2 que se muestra en la figura para ver otro problema en la configuración del switch.

En Topología 2, se eligió el modelo de enrutamiento del router-on-a-stick. Sin embargo, la interfaz F0/5 en el switch S1 no está configurada como un enlace troncal y posteriormente se le dejó en la VLAN predeterminada para el puerto. Como consecuencia, el router no puede funcionar correctamente porque cada una de las subinterfaces configuradas no puede enviar o recibir el tráfico etiquetado de la VLAN. Esto evita que todas las VLAN configuradas desde el enrutamiento a través del router R1 lleguen a las demás VLAN.

Para corregir este problema, ejecute el comando switchport mode trunk en la configuración de la interfaz en el puertodel switch F0/5 en el switch S1. Esto convierte a la interfaz en enlace troncal, lo que le permite a éste establecer con éxito una conexión con el router R1. Una vez establecido el enlace troncal en forma exitosa, los dispositivos conectados a cada una de las VLAN pueden comunicarse con la subinterfaz asignada a su VLAN, permitiendo, de esta manera, que tenga lugar el enrutamiento inter VLAN.

Haga clic en el botón Topología 3 que se muestra en la figura para ver otro problema en la configuración del switch

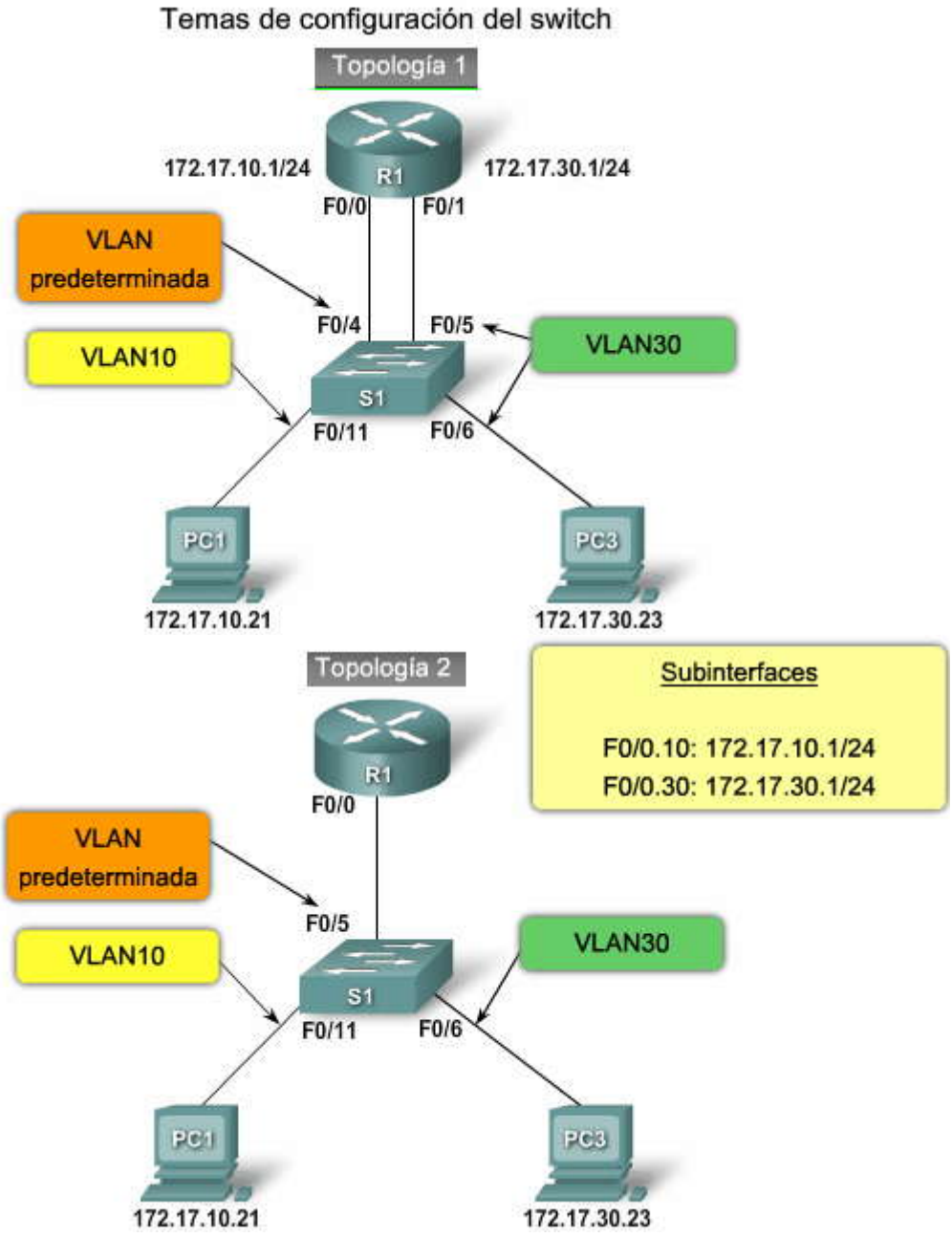
En Topología 3, el enlace troncal entre el switch S1 y el switch S2 está caído. Dado que no hay una conexión o ruta redundante entre los dispositivos, todos los dispositivos conectados al switch S2 no pueden llegar al router R1. Por lo tanto, todos los dispositivos conectados al switch S2 no pueden enrutar con otras VLAN a través del router R1.

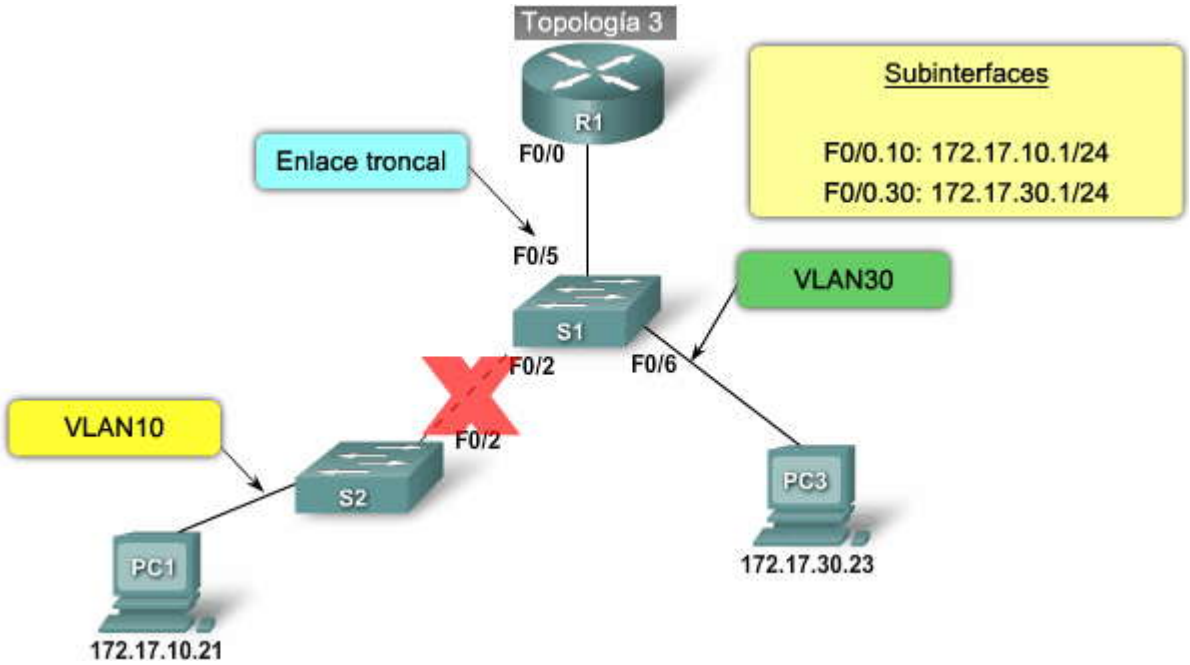
Para reducir el riesgo de que acontezca un enlace inter switch fallado, y de esta manera interrumpa el enrutamiento inter VLAN, deben configurarse los enlaces redundantes y las rutas alternativas entre el switch S1 y el switch S2. Los enlaces redundantes se configuran en forma de un EtherChannel que protege contra una falla de enlace único. La tecnología EtherChannel de Cisco le permite agregar múltiples enlaces físicos a un enlace lógico. Esto puede proporcionar hasta 80 Gb/s de ancho de banda agregado con 10 Gigabit EtherChannel.

Además, se pueden configurar las rutas alternativas a través de otros switches interconectados. Este enfoque depende del protocolo spanning tree (STP) para evitar la posibilidad de bucles dentro del ambiente del switch. Puede haber una pequeña disrupción en el acceso al router mientras el STP determina si el enlace actual está caído y encuentra una ruta alternativa.

El currículo CCNP dirige la tecnología EtherChannel; además, para obtener más información sobre la tecnología EtherChannel de Cisco, visite:
http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml.

Para obtener más información sobre la configuración de EtherChannel en un switch Catalyst 2960 de Cisco, visite:
http://www.cisco.com/en/US/products/ps6406/products_configuration_guide_chapter09186a00808752d9.html.





Comandos IOS del switch Cisco

Cuando sospeche que hay un problema con una configuración del switch, utilice los distintos comandos de verificación para examinar la configuración e identificar el problema.

Haga clic en el botón Asignación incorrecta de una VLAN que se muestra en la figura.

La pantalla muestra los resultados del comando show interface interface-id switchport. Supongamos que ejecutó estos comandos porque sospecha que la VLAN 10 no se asignó al puerto F0/4 en el switch S1. El área superior resaltada muestra que el puerto F0/4 en el switch S1 está en el modo de acceso, pero no muestra que se asignó directamente a la VLAN 10. El área inferior resaltada confirma que el puerto F0/4 aún está configurado en la VLAN predeterminada. Los comandos show running-config y show interface interface-id switchport son útiles para identificar las asignaciones de la VLAN y los problemas de configuración del puerto.

Haga clic en el botón Modo de acceso incorrecto que se muestra en la figura.

Después de un esfuerzo de reconfiguración, se detuvo la comunicación entre el router R1 y el switch S1. Se supone que el enlace entre el router y el switch es un enlace troncal. La pantalla muestra los resultados de los comandos show interface interface-id switchport y show running-config. El área superior resaltada confirma que el puerto F0/4 en el switch S1 está en el modo de acceso, no en el modo de enlace troncal. El área inferior resaltada también confirma que el puerto F0/4 se configuró para el modo de acceso.

```
S1#show interfaces fastEthernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: up
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<Output omitted>
```

```
S1#show interface f0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
<output truncated>
S1#
s1#show run
Building configuration...

<output truncated>
!
interface FastEthernet0/4
 switchport mode access
!
<output truncated>
```

6.3.2 TEMAS DE CONFIGURACION DE ROUTER.-

Uno de los errores de configuración del router inter VLAN más comunes es conectar la interfaz física del router al puerto del switch incorrecto, ya que la coloca en la VLAN incorrecta y evita que llegue a las demás VLAN.

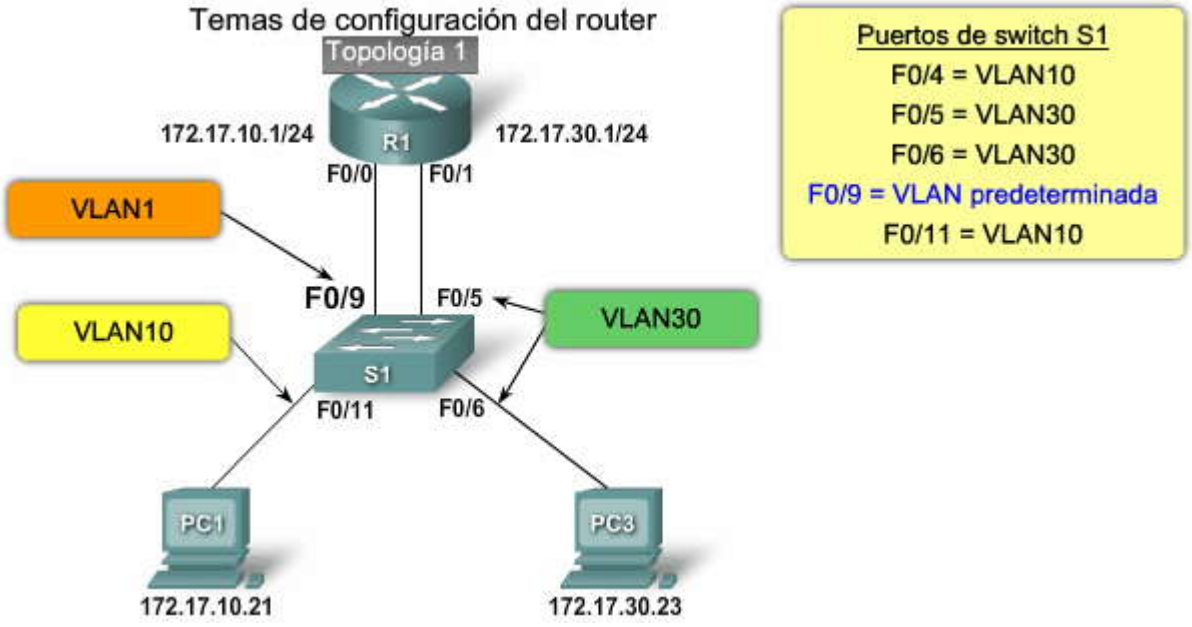
Como puede ver en Topología 1, la interfaz F0/0 del router R1 está conectada al puerto F0/9 del switch S1. El puerto del switch F0/9 está configurado para la VLAN predeterminada, no para la VLAN10. Esto evita que PC1 pueda comunicarse con la interfaz del router y, en consecuencia, enrutarse con la VLAN30.

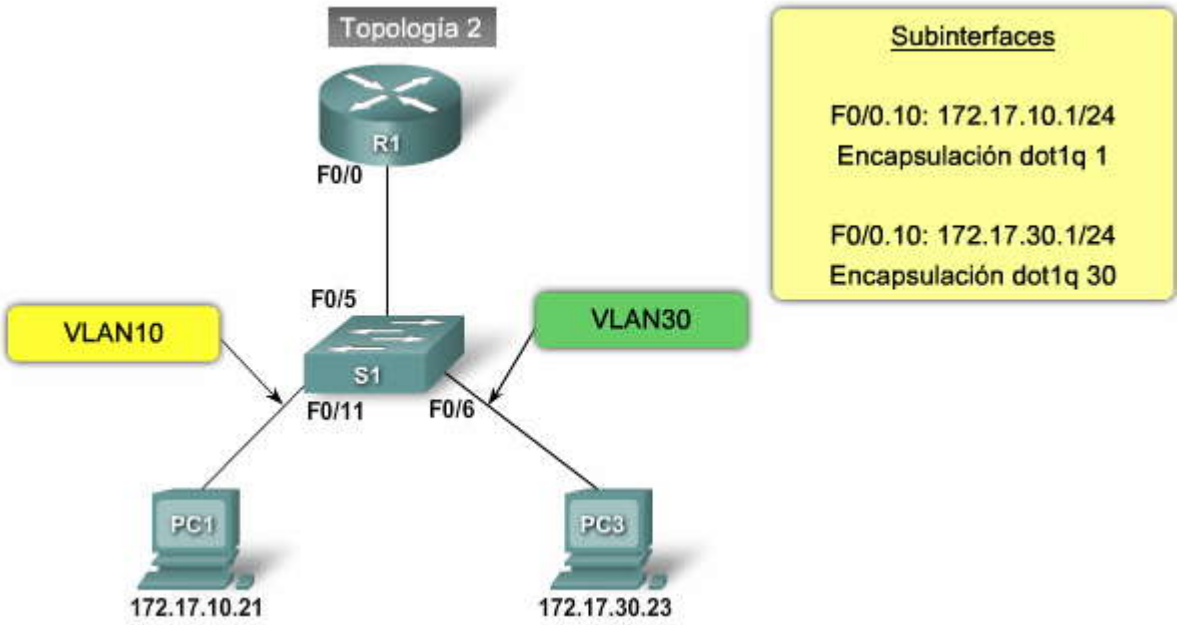
Para corregir este problema, conecte físicamente la interfaz F0/0 del router R1 al puerto F0/4 del switch S1. Esto coloca la interfaz del router en la VLAN correcta y permite que funcione el enrutamiento inter VLAN. Otra alternativa es cambiar la asignación de la VLAN del puerto del switch F0/9 para que esté en la VLAN10. Esto también permite a PC1 comunicarse con la interfaz F0/0 del router R1.

Haga clic en el botón Topología 2 que se muestra en la figura para ver otro problema en la configuración del router.

En Topología 2, el router R1 se configuró para utilizar la VLAN incorrecta en la subinterfaz F0/0.10, evitando que los dispositivos configurados en la VLAN10 se comuniquen con la subinterfaz F0/0.10. Luego, evita que dichos dispositivos puedan enrutarse con otras VLAN en la red.

Para corregir este problema, configure la subinterfaz F0/0.10 en la VLAN correcta mediante el comando encapsulation dot1q 10 en el modo de configuración de la subinterfaz. Una vez asignada la subinterfaz a la VLAN correcta, se puede acceder por medio de los dispositivos a esa VLAN y realizar el enrutamiento inter VLAN.





Verificar la configuración del router

En este escenario de resolución de problemas, el usuario sospecha que hay un problema con el router R1. La subinterfaz F0/0.10 debe permitir el acceso al tráfico de la VLAN 10 y la subinterfaz F0/0.30 debe permitir el tráfico de la VLAN 30. La captura de pantalla muestra los resultados de la ejecución de los comandos show interface y show runningconfig.

La sección superior resaltada muestra que la subinterfaz F0/0.10 en el router R1 utiliza la VLAN 100. El comando show interface produce muchos resultados, y esto dificulta la visión del problema.

El comando show running-config confirma que la subinterfaz F0/0.10 en el router R1 se configuró para permitir el acceso al tráfico de la VLAN 100 y no de la VLAN 10. Quizás esto fue un error de mecanografía.

Con la correcta verificación, los problemas de configuración del router se resuelven rápidamente, lo que permite que el enrutamiento inter VLAN funcione bien nuevamente. Recuerde que las VLAN están conectadas directamente, siendo ésta la manera en que ingresan a la tabla de enrutamiento.

```
R1#show interface
<output truncated>
FastEthernet0/0.10 is up, line protocol is down (disabled)
  Encapsulation 802.1Q Virtual LAN, Vlan ID 100
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last clearing of "show interface" counters never
<output truncated>
R1#
R1#show run
Building configuration...
Current configuration : 505 bytes
<output truncated>
!
interface FastEthernet0/0.10
 encapsulation dot1Q 100
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.17.30.1 255.255.255.0
!
<output truncated>
```

6.3.3 TEMAS DE DIRECCIONAMIENTO IP.-

Como analizamos, las subredes son la clave para implementar el enrutamiento inter VLAN. Las VLAN corresponden a subredes únicas en la red. Para que el enrutamiento inter VLAN funcione, es necesario conectar un router a todas las VLAN, ya sea por medio de interfaces físicas separadas o subinterfaces de enlace troncal. Toda interfazo subinterfaz necesita que se le asigne una dirección IP que corresponda a la subred para la cual está conectada. Esto permite que los dispositivos en la VLAN se comuniquen con la interfaz del router y habiliten el enrutamiento del tráfico a otras VLAN conectadas al router.

Examinemos algunos errores comunes.

Como puede ver en Topología 1, el router R1 se configuró con una dirección IP incorrecta en la interfaz F0/0. Esto evita que PC1 pueda comunicarse con el router R1 en la VLAN10.

Para corregir este problema, asigne la dirección IP correcta a la interfaz F0/0 del router R1 mediante el comando ip address 172.17.10.1 255.255.255.0 en el modo de configuración de la interfaz. Una vez asignada la interfaz del router a la dirección IP correcta, PC1 puede utilizar la interfaz como un gateway predeterminado para acceder a las otras VLAN.

Haga clic en el botón Topología 2 que se muestra en la figura para ver otro problema en la configuración de la dirección IP.

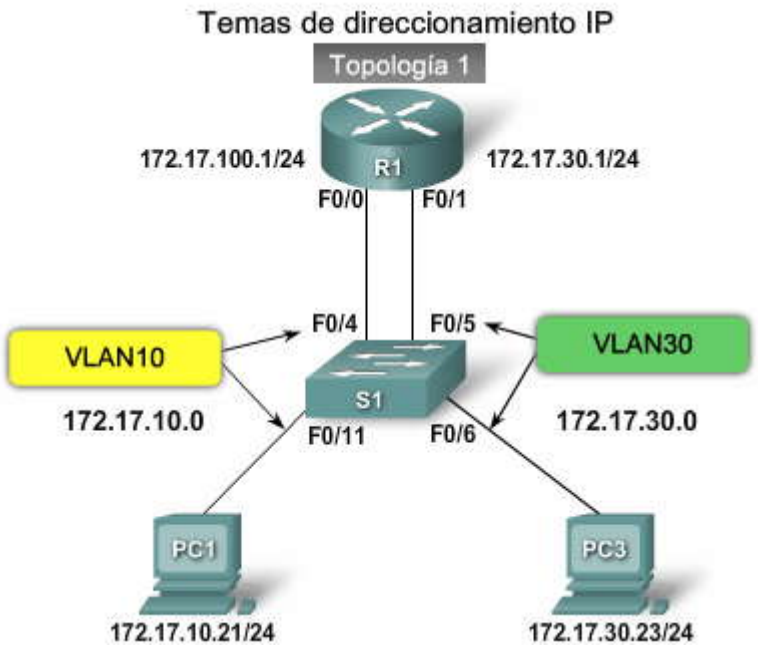
En Topología 2, PC1 se configuró con la dirección IP incorrecta para la subred asociada con la VLAN10. Esto evita que PC1 pueda comunicarse con el router R1 en la VLAN10.

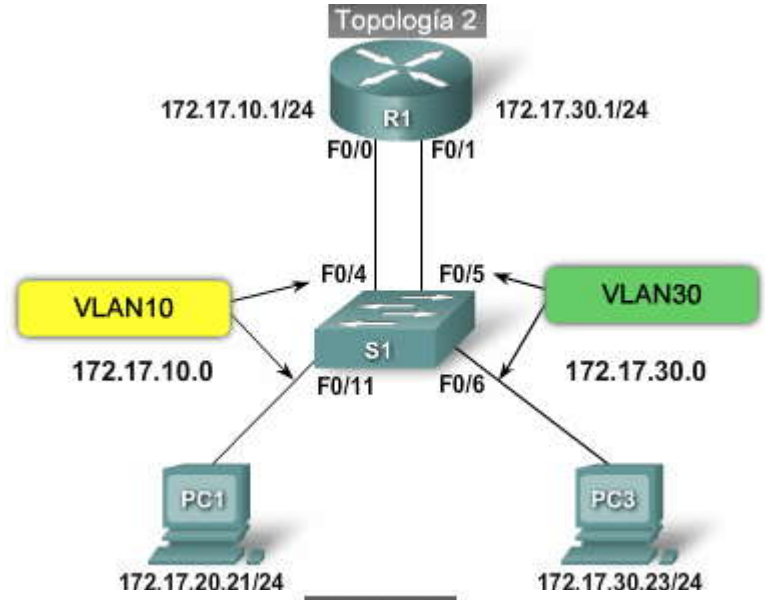
Para corregir este problema, asigne la dirección IP correcta a PC1. Según el tipo de computadora que utilice, los detalles de configuración pueden ser diferentes.

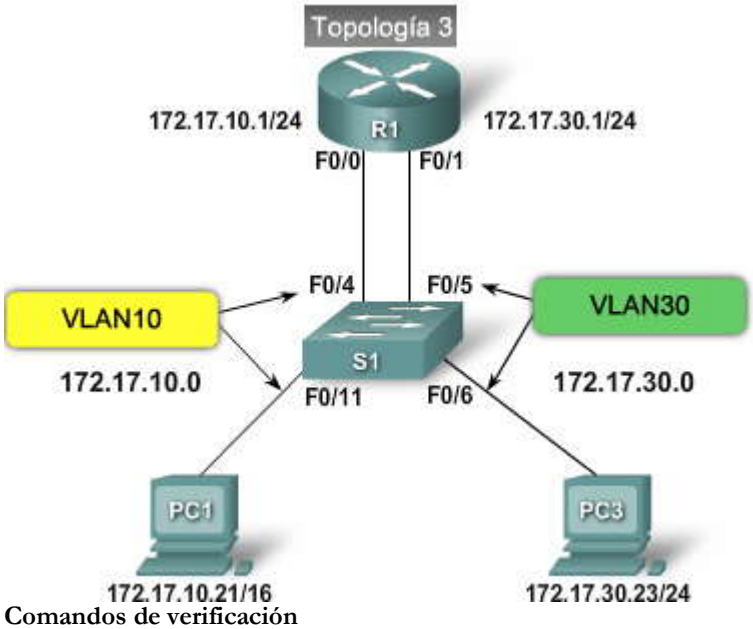
Haga clic en el botón Topología 3 que se muestra en la figura para ver otro problema en la configuración de la dirección IP.

En Topología 3, PC1 se configuró con la máscara de subred incorrecta. Según la máscara de subred configurada para PC1, PC1 está en la red 172.17.0.0. Esto da como resultado que PC1 determine que PC3, con la dirección IP 172.17.30.23, está en la subred local. Por lo tanto, PC1 no reenvía el tráfico destinado a PC3 a la interfaz F0/0 del router R1. Entonces, el tráfico nunca llega a PC3.

Para corregir este problema, cambie la máscara de subred en PC1 a 255.255.255.0. Según el tipo de computadora que utilice, los detalles de configuración pueden ser diferentes.







Comandos de verificación

Antes aprendió que toda interfaz, o subinterfaz, necesita que se le asigne una dirección IP que corresponda a la subred para la cual está conectada. Un error común es configurar incorrectamente una dirección IP para una subinterfaz. La captura de pantalla muestra los resultados del comando show running-config. El área resaltada muestra que la subinterfaz F0/0.10 en el router R1 tiene una dirección IP de 172.17.20.1. La VLAN para esta subinterfaz debe permitir el tráfico de la VLAN 10. Hay una dirección IP que se configuró incorrectamente. El comando show ip interface es otro comando útil. La segunda área resaltada muestra la dirección IP incorrecta.

Haga clic en el botón Problema en el direccionamiento IP de la computadora.

Algunas veces es el dispositivo de usuario final, como por ejemplo una computadora personal, el que ocasiona el problema. En la configuración de pantalla de la computadora PC1, la dirección IP es 172.17.20.21, con una máscara de subred de 255.255.255.0. Pero en este escenario, PC1 debe estar en la VLAN10, con una dirección de 172.17.10.21 y una máscara de subred de 255.255.255.0.

```
R1#show run
Building configuration...
<output truncated>
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/0.30
<output truncated>
R1#
R1#show ip interface
<output truncated>
Packet Tracer PC Command Line 1.0
PC1>ip config
Invalid Command.

PC1>ipconfig

IP Address.....................: 172.17.20.21
Subnet Mask....................: 255.255.255.0
Default Gateway................: 172.17.10.1

PC1>
```

Esta PC1 debe estar en la subred VLAN 10
Por lo tanto, debe ser: 172.17.10.21 con una máscara de subred de 255.255.255.0

CAPITULO VII – "CONCEPTOS Y CONFIGURACION BÁSICOS DE LA CONEXIÓN INALÁMBRICA"

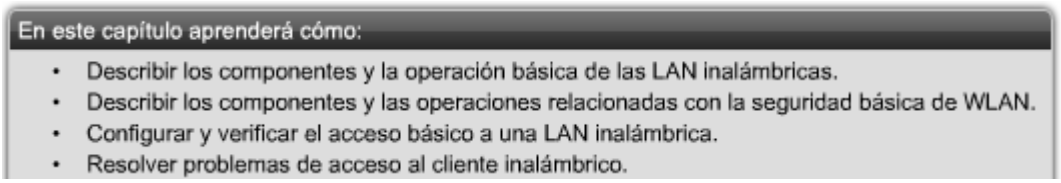
7.0 INTRODUCCIÓN DEL CAPITULO.-

7.0.1 INTRODUCCIÓN DEL CAPITULO.-

En los capítulos anteriores, aprendió cómo las funciones del switch pueden facilitar la interconexión de dispositivos enuna red conectada por cable. Las redes comerciales típicas hacen uso extensivo de las redes conectadas por cable. Las conexiones físicas se realizan entre sistemas de computación, sistemas de teléfono y otros dispositivos periféricos a switches ubicados en los armarios de cableado.

Administrar una infraestructura de cableado puede ser desafiante. Considere qué sucede cuando un trabajador decide que prefiere ubicar su sistema de computación en otro lugar de su oficina, o cuando un administrador quiere llevar su computadora portátil a la sala de conferencias y conectarse a la red desde allí. En una red conectada por cable, necesitará mover el cable de conexión de la red a una nueva ubicación en la oficina del trabajador y asegurarse de que exista una conexión de red disponible en la sala de conferencias. Cada vez son más comunes las redes inalámbricas para evitar estos cambios físicos.

En este capítulo, aprenderá cómo las redes inalámbricas de área local (WLAN) ofrecen un entorno de red flexible a las empresas. Aprenderá los distintos estándares inalámbricos que están disponibles hoy y las características que cada estándar ofrece. Aprenderá qué componentes de hardware son usualmente necesarios en una infraestructura inalámbrica, cómo operan las WLAN y cómo asegurarlas. Finalmente, aprenderá a configurar un punto de acceso inalámbrico y un cliente inalámbrico.



7.1 LAN INALÁMBRICA.-

7.1.1 ¿POR QUÉ UTIULIZAR INALÁMBRICA?.-

¿Por qué las LAN inalámbricas se han vuelto tan populares?

Las redes comerciales actuales evolucionan para dar soporte a la gente que está en continuo movimiento. Empleados y empleadores, estudiantes y docentes, agentes del gobierno y aquellos a quienes sirven, aficionados a los deportes y compradores están todos en continuo movimiento y muchos de elbs están "conectados". Tal vez usted tiene un teléfono celular al que envía mensajes instantáneos cuando se encuentra lejos de su computadora. Esta es la visión de ambiente móvil donde las personas pueden llevar su conexión a la red consigo cuando se trasladan.

Hay muchas infraestructuras diferentes (LAN conectada por cable, redes del proveedor de servicios) que permiten que exista este tipo de movilidad, pero en un ambiente de negocios, lo más importante es la WLAN.

La productividad ya no está restringida a una ubicación de trabajo fija o a un período de tiempo definido. Las personas esperan ahora estar conectadas en cualquier momento y en cualquier lugar, desde la oficina hasta el aeropuerto o incluso en el hogar. Los empleados que viajan solían estar restringidos a utilizar teléfonos públicos para verificar sus mensajes y para devolver algunas llamadas telefónicas entre vuelos. Ahora pueden verificar su correo electrónico, correo de voz y estado de los productos en asistentes personales digitales (PDA) mientras están en ubicaciones temporales diferentes.

Muchas personas cambiaron su forma de vivir y aprender en el hogar. Internet es un servicio estándar en muchos hogares, junto con el servicio de TV y teléfono. Incluso el método para acceder a Internetcambió de servicio temporal de discado vía módem a DSL dedicado o servicio por cable. Los usuarios domésticos buscan muchas de las mismas soluciones flexibles inalámbricas que buscan los trabajadores de oficina. Por primera vez, en 2005, se compraron más computadoras portátiles con Wi-Fi habilitado que computadoras personales fijas.

Además de la flexibilidad que ofrecen las WLAN, el costo reducido es un beneficio importante. Por ejemplo: con una infraestructura inalámbrica ya ubicada, se ahorra al moverse una persona dentro del edificio, al reorganizar un laboratorio, o al moverse a ubicaciones temporarias o sitios de proyectos. En promedio, el costo de IT de mover a un empleado a una nueva ubicación dentro del sitio es de $375 (USD).

Otro ejemplo es cuando la compañía se muda a un nuevo edificio que no tiene ninguna infraestructura de cableado. En este caso, el ahorro resultante de utilizar las WLAN puede ser incluso más notorio, dado que se evita el gran costo de pasar cables a través de paredes, techos y suelos.

Aunque es difícil de medir, las WLAN pueden dar como resultado una mejor productividad y empleados más relajados, y así obtener mejores resultados para los clientes y mayores ingresos.

LAN inalámbricas

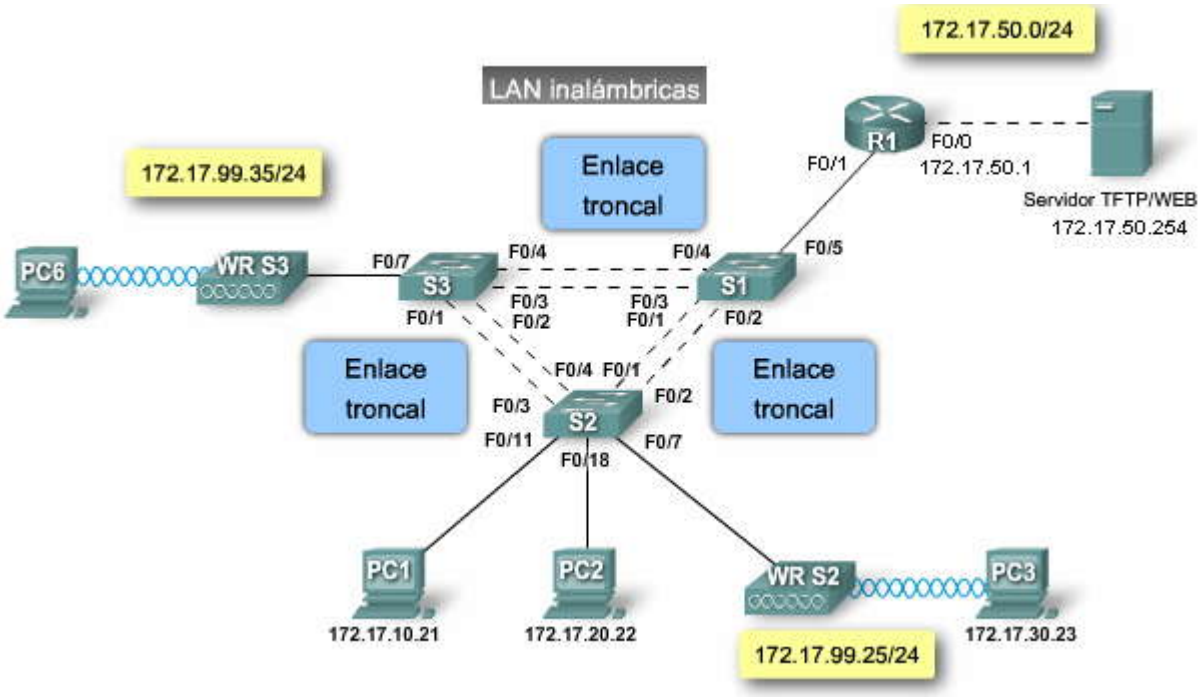
En los capítulos anteriores, aprendió sobre funciones y tecnologías de switch. Muchas redes de negocios actuales dependen de las LAN basadas en switch para las operaciones diarias dentro de las oficinas. Sin embargo, los trabajadores son cada vez más móviles y desean mantener el acceso a los recursos de LAN de sus negocios desde otras ubicaciones además de sus escritorios. Los trabajadores en la oficina desean llevar sus computadoras portátiles a reuniones o a la oficina de sus colegas. Cuando se utiliza una computadora portátil en otra ubicación, no es conveniente depender de una conexión conectada por cable. En este tema, aprenderá acerca de las LAN inalámbricas y cómo benefician a su negocio. También explorará las consideraciones de seguridad asociadas con las WLAN.

Las comunicaciones portátiles se convirtieron en una expectativa en muchos países alrededor del mundo. Puede ver movilidad y portabilidad en todo, desde teclados inalámbricos y audífonos, hasta teléfonos satelitales y sistemas de posicionamiento global (GPS). La mezcla de tecnologías inalámbricas en diferentes tipos de redes permite que los trabajadores tengan movilidad.

Haga clic en el botón de LAN inalámbricas en la figura.

Puede ver que la WLAN es una extensión de la LAN Ethernet. La función de la LAN se ha vuelto móvil. Aprenderá acerca de la tecnología WLAN y los estándares detrás de la movilidad que permiten a las personas continuar con una conferencia mientras caminan, en el taxi o en el aeropuerto.

	PAN	LAN	MAN	WAN
Estándares	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satélite
Velocidad	< 1 Mbps	de 11 a 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Intervalo	Cortocircuito	Medio	Medio-Largo	Largo
Aplicaciones	Par-a-par Dispositivo-a-Dispositivo	Redes de empresas	Acceso de última milla	Datos móviles Dispositivos



Comparación entre una WLAN y una LAN

Las LAN inalámbricas comparten un origen similar con las LAN Ethernet. El IEEE adoptó la cartera 802 LAN/MAN de estándares de arquitectura de red de computadoras. Los dos grupos de trabajo 802 dominantes son 802.3 Ethernet y IEEE 802.11 LAN inalámbrica. Sin embargo, hay diferencias importantes entre ellos.

Las WLAN utilizan frecuencias de radio (RF), en lugar de cables en la Capa física y la sub-capa MAC de la Capa de enlace de datos. Comparada con el cable, la RF tiene las siguientes características:

La RF no tiene límites, como los límites de un cable envuelto. La falta de dicho límite permite a las tramas de datos viajar sobre el medio RF para estar disponibles para cualquiera que pueda recibir la señal RF.
La señal RF no está protegida de señales exteriores, como sí lo está el cable en su envoltura aislante. Las radios que funcionan independientemente en la misma área geográfica, pero que utilizan la misma RF o similar, pueden interferirse mutuamente.
La transmisión RF está sujeta a los mismos desafíos inherentes a cualquier tecnología basada en ondas, como la radio comercial. Por ejemplo: a medida que usted se aleja del origen, puede oír estaciones superpuestas una sobre otra o escuchar estática en la transmisión. Con el tiempo, puede perder la señal por completo. Las LAN conectadas tienen cables que son del largo apropiado para mantener la fuerza de la señal.
Las bandas RF se regulan en forma diferente en cada país. La utilización de las WLAN está sujeta a regulaciones adicionales y a conjuntos de estándares que no se aplican a las LAN conectadas por cable.

Las WLAN conectan a los clientes a la red a través de un punto de acceso inalámbrico (AP) en lugar de un switch Ethernet.

Las WLAN conectan los dispositivos móviles que, en general, están alimentados por batería, en lugar de los dispositivos enchufados de la LAN. Las tarjetas de interfaz de la red inalámbrica (NIC) tienden a reducir la vida de la batería de un dispositivo móvil.

Las WLAN admiten hosts que se disputan el acceso a los medios RF (bandas de frecuencia). 802.11 recomienda la prevención de colisiones, en lugar de la detección de colisiones para el acceso a medios, para evitar -en forma proactiva- colisiones dentro del medio.

Las WLAN utilizan un formato de trama diferente al de las LAN Ethernet conectadas por cable. Las WLAN requieren información adicional en el encabezado de la Capa 2 de la trama.

Las WLAN tienen mayores inconvenientes de privacidad debido a que las frecuencias de radio pueden salir fuera de las instalaciones.

Comparación entre una WLAN y una LAN

Característica	802.11 LAN inalámbrica	802.3 Redes LAN Ethernet
Capa física	Frecuencia de radio (RF)	Cable
Acceso de medios	Prevención de colisión	Detección de colisiones
Disponibilidad	Cualquiera con una radio NIC en el rango de un punto de acceso	Se requiere conexión por cable
Interferencia en la señal	Sí	Irrelevante
Regulación	Regulación adicional a cargo de las autoridades locales	El estándar IEEE dictamina

Introducción de las LAN inalámbricas

Las LAN inalámbricas 802.11 extienden las infraestructuras LAN Ethernet 802.3 para proveer opciones adicionales de conectividad. Sin embargo, se utilizan componentes y protocolos adicionales para completar las conexiones inalámbricas.

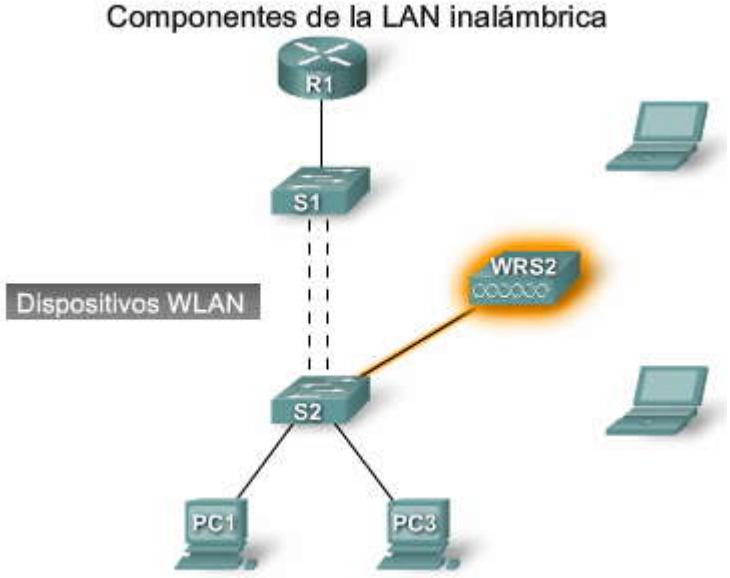
En una LAN Ethernet 802.3 cada cliente tiene un cable que conecta el NIC del cliente a un switch. El switch es el punto en el que el cliente obtiene acceso a la red.

Haga clic en el botón de Dispositivos WLAN en la figura.

En una LAN inalámbrica, cada cliente utiliza un adaptador inalámbrico para obtener acceso a la red a través de un dispositivo inalámbrico como un router inalámbrico o punto de acceso.

Haga clic en el botón Clientes en la figura.

El adaptador inalámbrico en el cliente se comunica con el router inalámbrico o punto de acceso mediante señales RF. Una vez conectados a la red, los clientes inalámbricos pueden acceder a los recursos de la red como si estuvieran conectados a la red mediante cable.



7.1.2 ESTÁNDARES DE LAN INALÁMBRICAS.-

Estándares de LAN inalámbricas

LAN inalámbrica 802.11 es un estándar IEEE que define cómo se utiliza la radiofrecuencia (RF) en las bandas sin licencia de frecuencia médica, científica e industrial (ISM) para la Capa física y la sub-capa MAC de enlaces inalámbricos.

Cuando el 802.11 se emitió por primera vez, prescribía tasas de datos de 1 - 2 Mb/s en la banda de 2,4 GHz. En ese momento, las LAN conectadas por cable operaban a 10 Mb/s, de modo que la nueva tecnología inalámbrica no se adoptó con entusiasmo. A partir de entonces, los estándares de LAN inalámbricas mejoraron continuamente con la edición de IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, y el borrador 802.11n.

La elección típica sobre qué estándar WLAN utilizar se basa en las tasas de datos. Por ejemplo: 802.11a y g puedenadmitir hasta 54 Mb/s, mientras que 802.11b admite hasta un máximo de 11 Mb/s, lo que implica que 802.11b es un estándar "lento" y que 802.11 a y g son los preferidos. Un cuarto borrador WLAN, 802.11n, excede las tasas de datos disponibles en la actualidad. El IEEE 802.11n debe ser ratificado para septiembre de 2008. La figura compara los estándares IEEE 802.11a, b y g.

Haga clic en el botón Tabla en la figura para ver detalles sobre cada estándar.

Las tasas de datos de los diferentes estándares de LAN inalámbrica están afectadas por algo llamado técnica de modulación. Las dos técnicas de modulación comprendidas en este curso son: Espectro de dispersión de secuencia directa (DSSS) y Multiplexación por división de frecuencias octagonales (OFDM). No necesita saber cómo trabajan estas técnicas para este curso, pero debe saber que cuando un estándar utilice OFDM, tendrá tasas de datos más veloces. Además, el DSSS es más simple que el OFDM, de modo que su implementación es más económica.

802.11a

El IEEE 802.11a adoptó la técnica de modulación OFDM y utiliza la banda de 5 GHz.

Los dispositivos 802.11a que operan en la banda de 5 GHz tienen menos probabilidades de sufrir interferencia que los dispositivos que operan en la banda de 2,4 GHz porque existen menos dispositivos comerciales que utilizan la banda de 5 GHz. Además, las frecuencias más altas permiten la utilización de antenas más pequeñas.

Existen algunas desventajas importantes al utilizar la banda de 5 GHz. La primera es que, a frecuencia de radio más alta, mayor es el índice de absorción por parte de obstáculos tales como paredes, y esto puede ocasionar un rendimiento pobre del 802.11a debido a las obstrucciones. El segundo es que esta banda de frecuencia alta tiene un rango más acotado que el 802.11b o el g. Además, algunos países, incluida Rusia, no permiten la utilización de la banda de 5 GHz, lo que puede restringir más su implementación.

802.11b y 802.11g

802.11b especificó las tasas de datos de 1; 2; 5,5 y 11 Mb/s en la banda de 2,4 GHz ISM que utiliza DSSS. 802.11g logra tasas de datos superiores en esa banda mediante la técnica de modulación OFDM. IEEE 802.11g también especifica la utilización de DSSS para la compatibilidad retrospectiva de los sistemas IEEE 802.11b. El DSSS admite tasas de datos de 1; 2; 5,5 y 11 Mb/s, como también las tasas de datos OFDM de 6; 9; 12; 18; 24; 48 y 54 Mb/s.

Existen ventajas en la utilización de la banda de 2,4 GHz. Los dispositivos en la banda de 2,4 GHz tendrán mejor alcance que aquellos en la banda de 5 GHz. Además, las transmisiones en esta banda no se obstruyen fácilmente como en 802.11a.

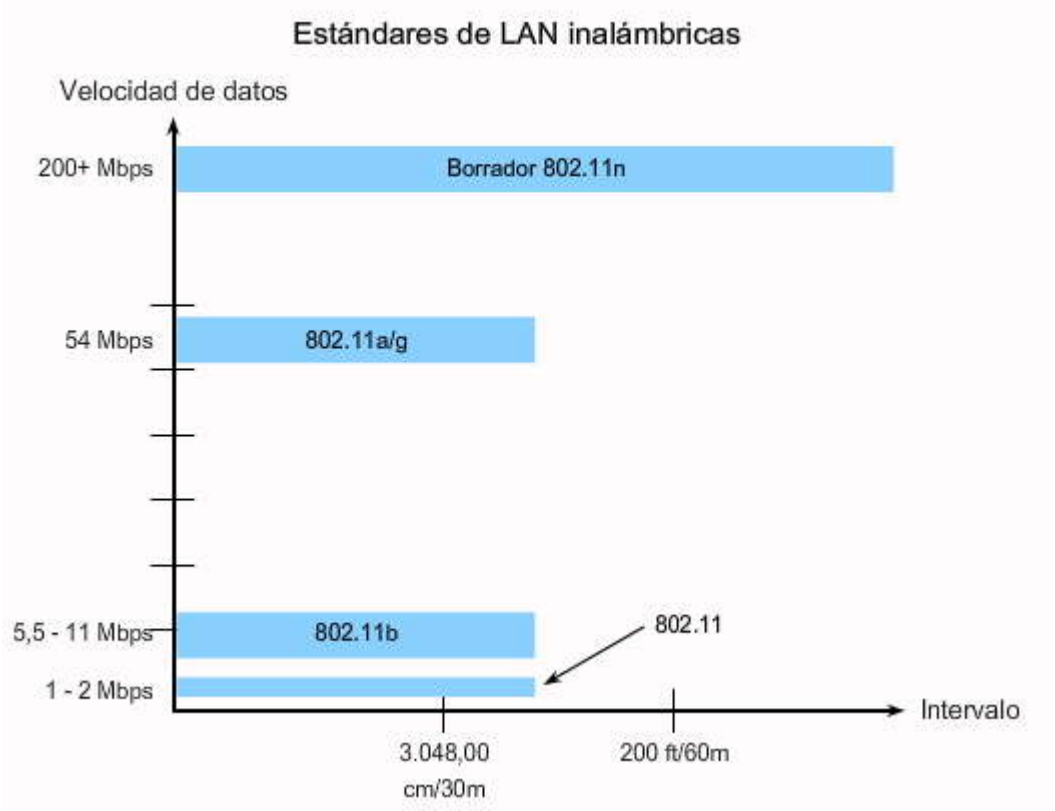
Hay una desventaja importante al utilizar la banda de 2,4 GHz. Muchos dispositivos de clientes también utilizan la banda de 2,4 GHz y provocan que los dispositivos 802.11b y g tiendan a tener interferencia.

802.11n

El borrador del estándar IEEE 802.11n fue pensado para mejorar las tasas de datos y el alcance de la WLAN sin requerir energía adicional o asignación de la banda RF. 802.11n utiliza radios y antenas múltiples en los puntos finales, y cada uno transmite en la misma frecuencia para establecer streams múltiples. La tecnología de entrada múltiple/salida múltiple (MIMO) divide un stream rápido de tasa de datos en múltiples streams de menor tasa y los transmite simultáneamente por las radios y antenas disponibles. Esto permite una tasa de datos teórica máxima de 248 Mb/s por medio de dos streams.

Se espera que el estándar se ratifique para septiembre de 2008.

Importante: El sector de comunicaciones de la Unión internacional de telecomunicaciones (ITU-R) asigna las bandas RF. La ITU-R designa las frecuencias de banda de 900 MHz, 2,4 GHz, y 5 GHz como sin licencia para las comunidades ISM. A pesar de que las bandas ISM no tienen licencia a nivel global, sí están sujetas a regulaciones locales. La FCC administra la utilización de estas bandas en los EE. UU., y la ETSI hace lo propio en Europa. Estos temas tendrán un impacto en su decisión a la hora de seleccionar los componentes inalámbricos en una implementación inalámbrica.



	802.11a	802.11b	802.11g		802.11n
Banda	5,7 GHz	2,4 GHz	2,4 GHz		No confirmado Posiblemente bandas 2,4 y 5 GHz
Canales*	Hasta 23	3	3		
Modulación	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Velocidad de los datos	Hasta 54 Mbps	Hasta 11 Mbps	Hasta 11 Mbps	Hasta 54 Mbps	Se especula que será 248 Mbps para dos streams MIMO
Pros	~150 pies o 35 metros	~150 pies o 35 metros	~150 pies o 35 metros		~230 pies o 70 metros
Contras	Octubre de 1999	Octubre de 1999	Junio de 2003		Esperado para el 2008
Pros	Rápido, menos susceptible a interferencias	Bajo costo, buen alcance	Rápido, buen alcance, difícil de obstruir		Buenas velocidades de transferencia de datos, alcance mejorado
Contras	Costo superior, menor alcance	Lenta, susceptible a interferencias	Susceptible a interferencias desde aplicaciones que operan en la banda de 2,4 GHz		Tabla

*Canales no superpuestos.

Certificación Wi-Fi

La certificación Wi-Fi la provee la Wi-Fi Alliance (http://www.wi-fi.org), una asociación de comercio industrial global sin fines de lucro, dedicada a promover el crecimiento y aceptación de las WLAN. Apreciará mejor laimportancia de la certificación Wi-Fi si considera el rol de la Wi-Fi Alliance en el contexto de los estándares WLAN.

Los estándares aseguran interoperabilidad entre dispositivos hechos por diferentes fabricantes. Las tres organizaciones clave que influencian los estándares WLAN en todo el mundo son:

ITU-R
IEEE
Wi-Fi Alliance

El ITU-R regula la asignación del espectro RF y órbitas satelitales. Éstos se describen como recursos naturales finitos que se encuentran en demanda por parte de clientes, como redes inalámbricas fijas, redes inalámbricas móviles y sistemas de posicionamiento global.

El IEEE desarrolló y mantiene los estándares para redes de área local y metropolitanas con la familia de estándares IEEE 802 LAN/MAN. El IEEE 802 es administrado por el comité de estándares IEEE 802 LAN/MAN (LMSC), que supervisa múltiples grupos de trabajo. Los estándares dominantes en la familia IEEE 802 son 802.3 Ethernet, 802.5 Token Ring, y 802.11 LAN inalámbrica.

A pesar de que el IEEE especificó estándares para los dispositivos de modulación RF, no especificó estándares de fabricación, de modo que las interpretaciones de los estándares 802.11 por parte de los diferentes proveedores pueden causar problemas de interoperabilidad entre sus dispositivos.

La Wi-Fi Alliance es una asociación de proveedores cuyo objetivo es mejorar la interoperabilidad de productos que están basados en el estándar 802.11, y certifica proveedores en conformidad con las normas de la industria y adhesión a los estándares. La certificación incluye las tres tecnologías RF IEEE 802.11, así como la adopción temprana de los borradores pendientes de la IEEE, como el estándar 802.11n, y los estándares de seguridad WPA y WPA2 basados en IEEE 802.11i.

Los roles de estas tres organizaciones pueden resumirse de la siguiente manera:

El ITU-R regula la asignación de las bandas RF.
IEEE especifica cómo se modula RF para transportar información.
Wi-Fi asegura que los proveedores fabriquen dispositivos que sean interoperables.

7.1.3 COMPONENTES DE INFRAESTRUCTURA INALÁMBRICA?

NIC inalámbricos

Puede que ya esté utilizando una red inalámbrica en su hogar, en un cyber café local o en la escuela a la que concurre. ¿Alguna vez se preguntó qué componentes de hardware están involucrados en su acceso inalámbrico a la red local o a Internet? En este tema, aprenderá qué componentes están disponibles para implementar las WLAN y cómo se utiliza cada uno de ellos en la infraestructura inalámbrica.

Para revisar, los componentes constitutivos de una WLAN son estaciones cliente que conectan a los puntos de acceso, que se conectan, a su vez, a la infraestructura de la red. El dispositivo que hace que una estación cliente pueda enviar y recibir señales RF es el NIC inalámbrico.

Como un NIC Ethernet, el NIC inalámbrico, utiliza la técnica de modulación para la que está configurado y codifica un stream de datos dentro de la señal RF. Los NIC inalámbricos se asocian más frecuentemente a dispositivos móviles, como computadoras portátiles. En la década de los noventa, los NIC inalámbricos para computadoras portátiles eran tarjetas que se deslizaban dentro de la ranura PCMCIA. Los NIC inalámbricos PCMCIA son todavía comunes, pero muchos fabricantes comenzaron a incorporar el NIC inalámbrico dentro de la computadora portátil. A diferencia de las interfaces Ethernet 802.3 incorporadas en las PC, el NIC inalámbrico no es visible, ya que no es necesario conectar un cable a éste.

También surgieron otras opciones a través de los años. Las computadoras personales ubicadas en una instalaciónexistente no conectada por cable pueden tener instalado un NIC PCI inalámbrico. Existen, además, muchas opciones USB disponibles para configurar rápidamente una computadora, ya sea portátil o de escritorio, con o sin NIC inalámbrico.

Puntos de acceso inalámbricos

Un punto de acceso conecta a los clientes (o estaciones) inalámbricas a la LAN cableada. Los dispositivos de los clientes, por lo general, no se comunican directamente entre ellos; se comunican con el AP. En esencia, un punto de acceso convierte los paquetes de datos TCP/IP desde su formato de encapsulación en el aire 802.11 al formato de trama de Ethernet 802.3 en la red Ethernet conectada por cable.

En una infraestructura de red, los clientes deben asociarse con un punto de acceso para obtener servicios de red. La asociación es el proceso por el cual un cliente se une a una red 802.11. Es similar a conectarse a una red LAN conectada por cable. La asociación se discute en temas posteriores.

Un punto de acceso es un dispositivo de Capa 2 que funciona como un hub Ethernet 802.3. La RF es un medio compartido y los puntos de acceso escuchan todo el tráfico de radio (frecuencia). Al igual que con el Ethernet 802.3, los dispositivos que intentan utilizar el medio compiten por él. A diferencia de los NIC Ethernet, sin embargo, es costoso realizar NIC inalámbricos que puedan transmitir y recibir información al mismo tiempo, de modo que los dispositivos de radio no detectan colisiones. En cambio, los dispositivos WLAN están diseñados para evitarlos.

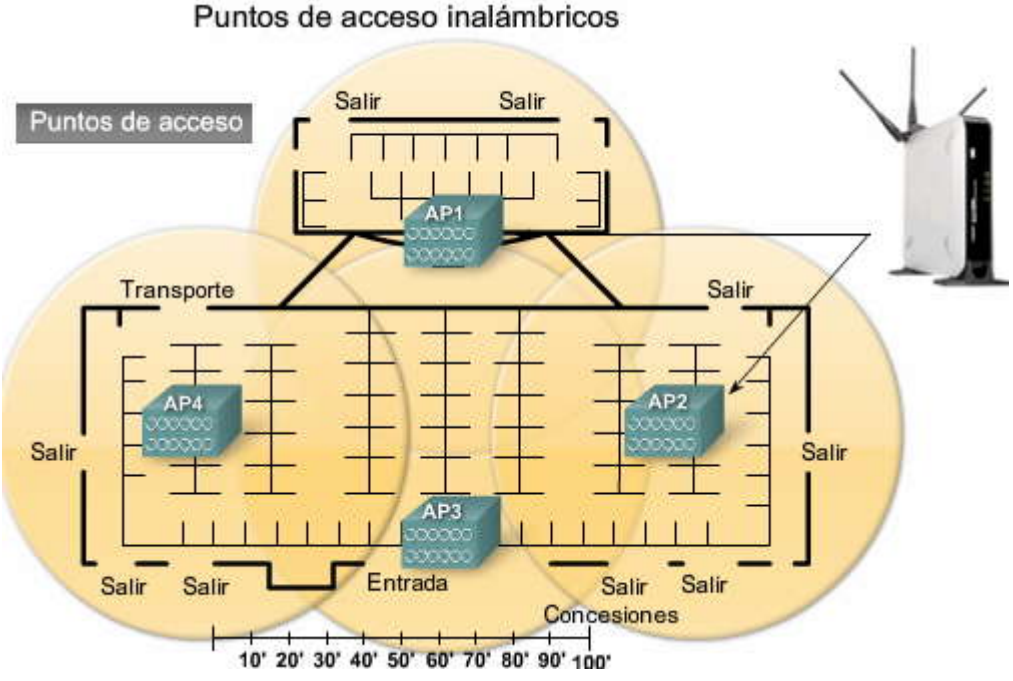
CSMA/CA

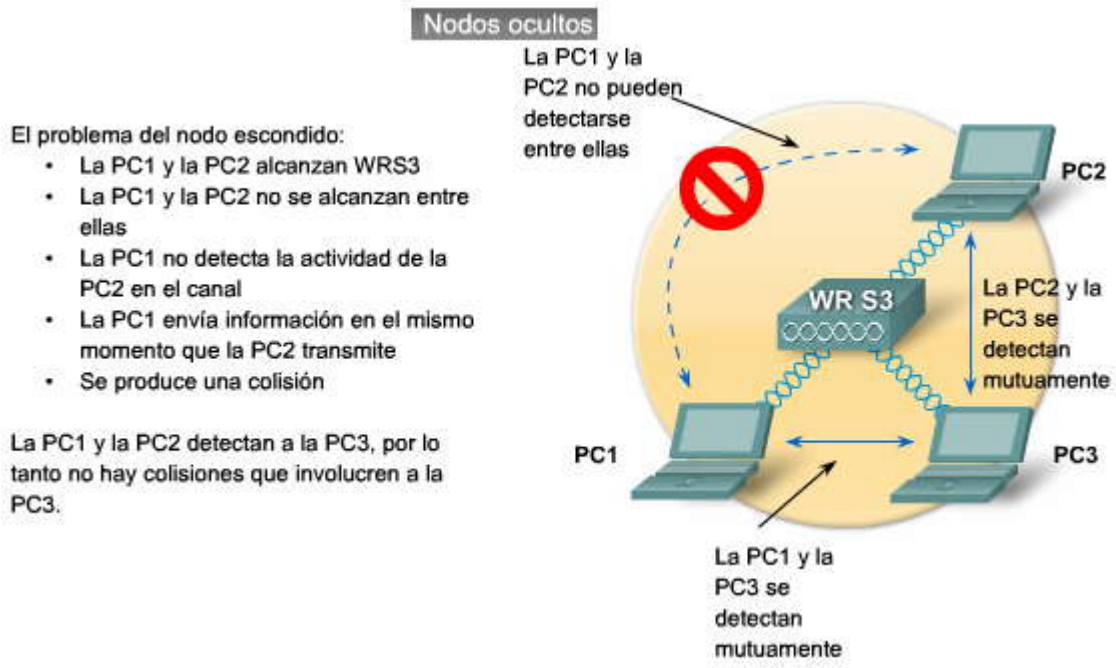
Los puntos de acceso supervisan una función de coordinación distribuida (DCF) llamada Acceso múltiple por detección de portadora con prevención de colisiones (CSMA/CA). Esto simplemente significa que los dispositivos en una WLAN deben detectar la energía del medio (estimulación de la RF sobre cierto umbral) y esperar hasta que éste se libere antes de enviar. Dado que se requiere que todos los dispositivos lo realicen, se distribuye la función de coordinar el acceso al medio. Si un punto de acceso recibe información desde la estación de un cliente, le envía un acuse de recibo para confirmar que se recibió la información. Este acuse de recibo evita que el cliente suponga que se produjo una colisión e impide la retransmisión de información por parte del cliente.

Haga clic en el botón de Nodos ocultos en la figura.
Atenuación de las señales RF. Eso significa que pueden perder energía a medida que se alejan de su punto de origen. Piense en alejarse del alcance de una estación de radio. Esta atenuación de la señal puede ser un problema en una WLAN donde las estaciones se disputan el medio.

Imagine dos estaciones cliente que conectan al punto de acceso, pero están en lugares opuestos de su alcance. Si están del alcance máximo del punto de acceso, no podrán conectarse entre sí. De esta manera, ninguna de esas estaciones detecta a la otra en el medio, y pueden terminar por transmitir en simultáneo. A esto se lo llama problema de nodo (o estación) escondido.

Una manera de resolver este problema de nodo escondido es una característica de CSMA/CA llamada petición para enviar/listo para enviar (RTS/CTS). El RTS/CTS se desarrolló para permitir una negociación entre un cliente y un punto de acceso. Cuando está activado el RTS/CTS en una red, los puntos de acceso asignan un medio para la estación que lo solicite por el tiempo que sea necesario para completar la transmisión. Cuando se completa la transmisión, otras estaciones pueden solicitar el canal de modo similar. De otra forma, se retoma la función de prevención de colisiones normal.

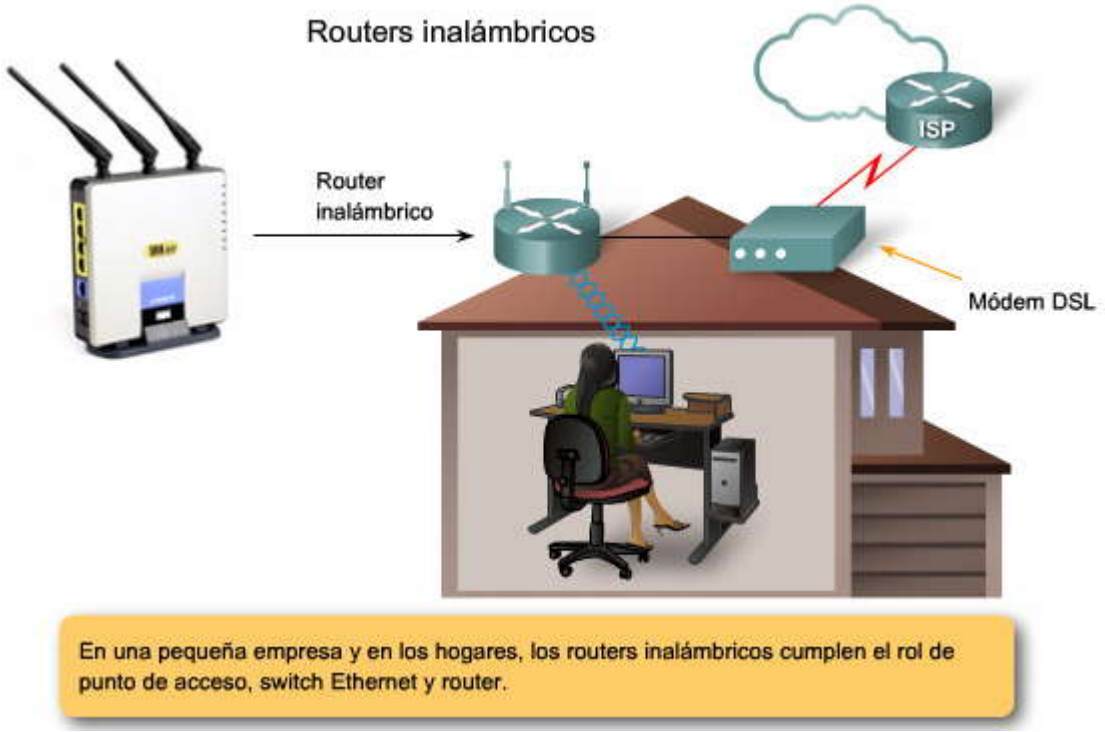




Routers inalámbricos

Los routers inalámbricos cumplen el rol de punto de acceso, switch Ethernet y router. Por ejemplo: los Linksys WRT300N utilizados son en realidad tres dispositivos en una caja. Primero está el punto de acceso inalámbrico, que cumple las funciones típicas de un punto de acceso. Un switch integrado de cuatro puertos full-duplex, 10/100 proporciona la conectividad a los dispositivos conectados por cable. Finalmente, la función de router provee un gateway para conectar a otras infraestructuras de red.

El WRT300N se utiliza más frecuentemente como dispositivo de acceso inalámbrico en residencias o negocios pequeños. La carga esperada en el dispositivo es lo suficientemente pequeña como para administrar la provisión de WLAN, 802.3 Ethernet, y conectar a un ISP.



7.1.4 OPERACIÓN INALÁMBRICA.-

Parámetros configurables para los puntos finales inalámbricos

La figura muestra la pantalla inicial para la configuración inalámbrica en un router Linksys inalámbrico. Varios procesos deben tener lugar para crear una conexión entre cliente y punto de acceso. Debe configurar los parámetros en el punto de acceso y, posteriormente, en el dispositivo de su cliente, para permitir la negociación de estos procesos.

Haga clic en el botón Modos en la figura para ver el parámetro de Modo de red inalámbrica.

El modo de red inalámbrica se remite a los protocolos WLAN: 802.11a, b, g, o n. Dado que 802.11g es compatible con versiones anteriores de 802.11b, los puntos de acceso admiten ambos estándares. Recuerde que si todos los clientes se conectan a un punto de acceso con 802.11g, se beneficiarán con las mejores velocidades de transmisión de datos. Cuando los clientes 802.11b se asocian con el punto de acceso, todos los clientes más veloces que se disputan el canal deben esperar que los clientes en 802.11b lo despejen antes de poder transmitir. Cuando un punto de acceso Linksys se configura para permitir clientes de 802.11b y 802.11g, opera en modo mixto.

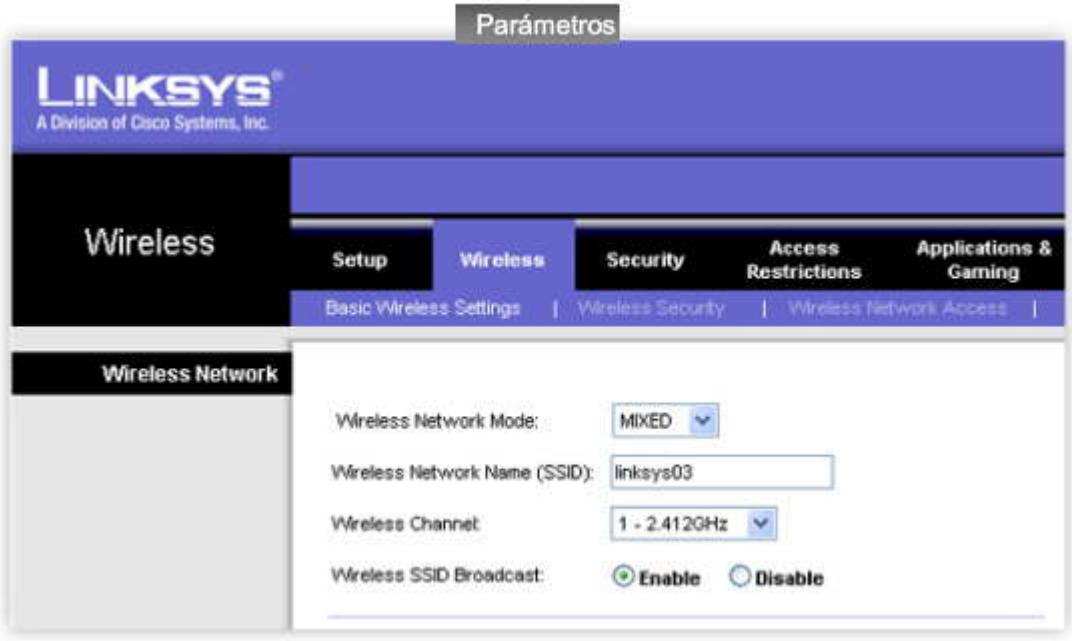
Para que un punto de acceso admita tanto el 802.11a como los 802.11b y g, deberá tener una segunda radio para operar en la banda RF diferente.

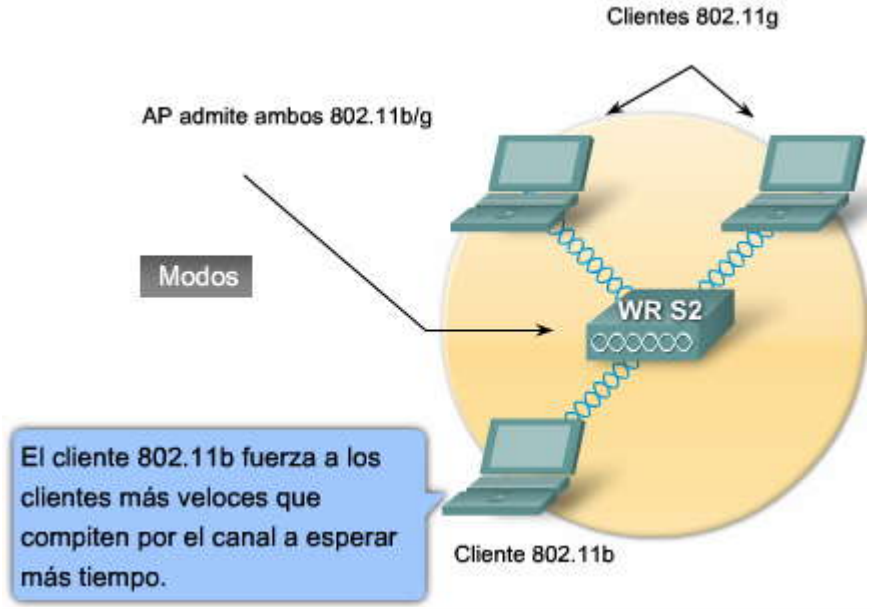
Haga clic en el botón SSID en la figura para ver una lista de SSID para un cliente de Windows.

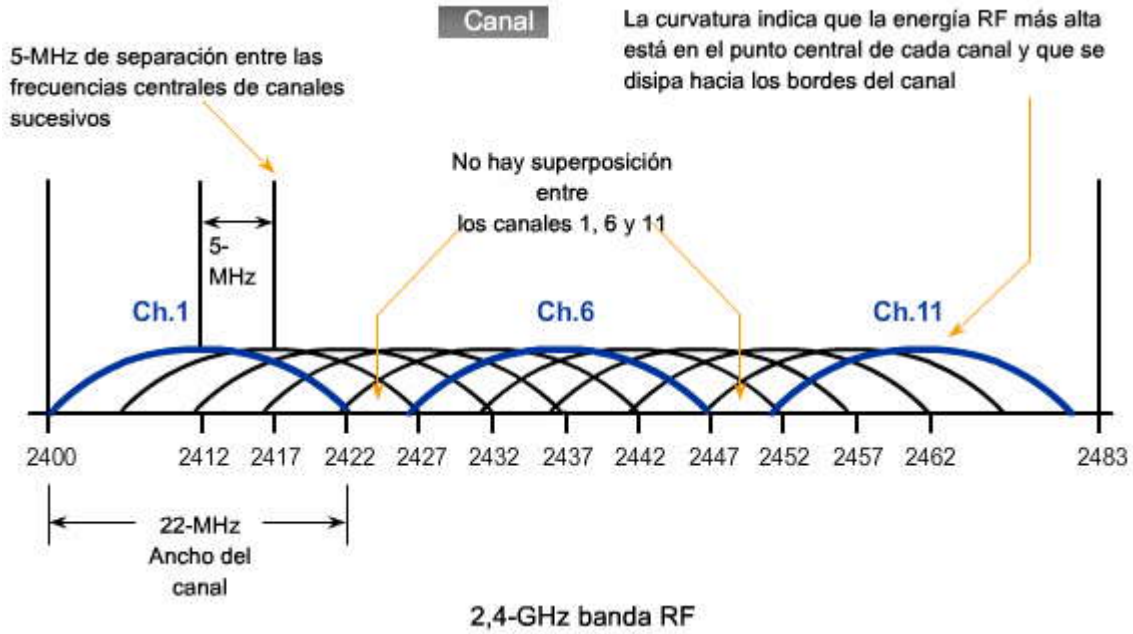
Un identificador de servicio compartido (SSID) es un identificador único que utiliza los dispositivos cliente para distinguir entre múltiples redes inalámbricas cercanas. Varios puntos de acceso en la red pueden compartir un SSID. La figura muestra un ejemplo de los SSID que se distinguen entre las WLAN, cada uno de los cuales puede ser alfanumérico, con entrada de 2 a 32 caracteres de longitud, con distinción entre mayúsculas y minúsculas.

Haga clic en el botón Canal en la figura para ver una gráfica de canales no superpuestos.

El estándar IEEE 802.11 establece el esquema de canalización para el uso de las bandas ISM RF no licenciadas en las WLAN. La banda de 2,4 GHz se divide en 11 canales para Norteamérica y 13 canales para Europa. Estos canales tienen una separación de frecuencia central de sólo 5 MHz y un ancho de banda total (u ocupación de frecuencia) de 22 MHz. El ancho de banda del canal de 22 MHz combinado con la separación de 5 MHz entre las frecuencias centrales significa que existe una superposición entre los canales sucesivos. Las optimizaciones para las WLAN que requieren puntos de acceso múltiple se configuran para utilizar canales no superpuestos. Si existen tres puntos de acceso adyacentes, utilice los canales 1, 6 y 11. Si sólo hay dos, seleccione dos canales cualesquiera con al menos 5 canales de separación entre ellos, como el canal 5 y el canal 10. Muchos puntos de acceso pueden seleccionar automáticamente un canal basado en el uso de canales adyacentes. Algunos productos monitorean continuamente el espacio de radio para ajustar la configuración de canal de modo dinámico en respuesta a los cambios del ambiente.







2,4-GHz banda RF

Topologías 802.11

Las LAN inalámbricas pueden utilizar diferentes topologías de red. Al describir estas topologías, la pieza fundamental de la arquitectura de la WLAN IEEE 802.11 es el conjunto de servicio básico (BSS). El estándar define al BSS como un grupo de estaciones que se comunican entre ellas.
Haga clic en el botón Ad Hoc en la figura.
Redes Ad hoc

Las redes inalámbricas pueden operar sin puntos de acceso; se llama topología ad hoc. Las estaciones cliente que están configuradas para operar en modo ad hoc configuran los parámetros inalámbricos entre ellas. El estándar IEEE 802.11 se refiere a una red ad hoc como un BSS (IBSS) independiente.

Haga clic en el botón de BSS en la figura.
Conjunto de servicios básicos

Los puntos de acceso proveen una infraestructura que agrega servicios y mejora el alcance para los clientes. Un punto de acceso simple en modo infraestructura administra los parámetros inalámbricos y la topología es simplemente un BSS. El área de cobertura para un IBSS y un BSS es el área de servicio básica (BSA).

Haga clic en el botón de ESS en la figura.
Conjuntos de servicios extendidos

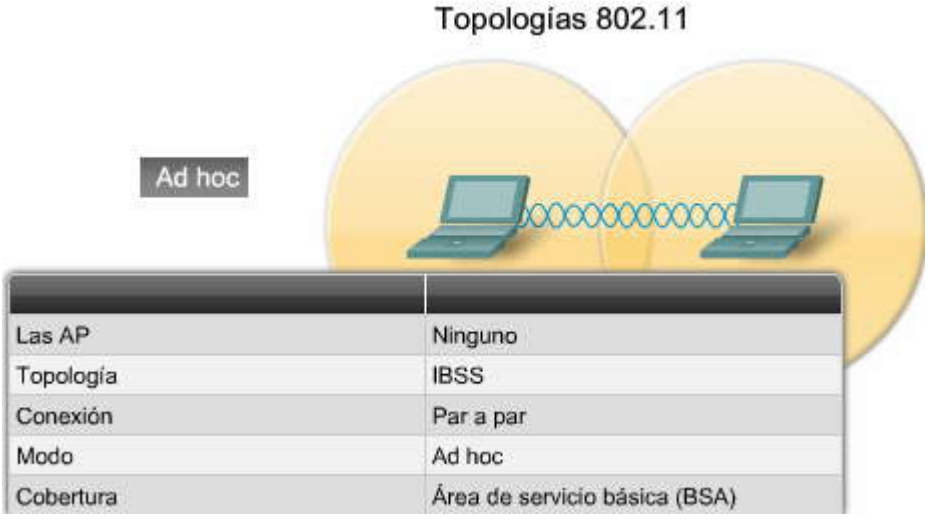
Cuando un BSS simple no provee la suficiente cobertura RF, uno o más se pueden unir a través de un sistema de distribución simple hacia un conjunto de servicios extendidos (ESS). En un ESS, un BSS se diferencia de otro mediante el identificador BSS (BSSID), que es la dirección MAC del punto de acceso que sirve al BSS. El área de cobertura es el área de servicio extendida (ESA).

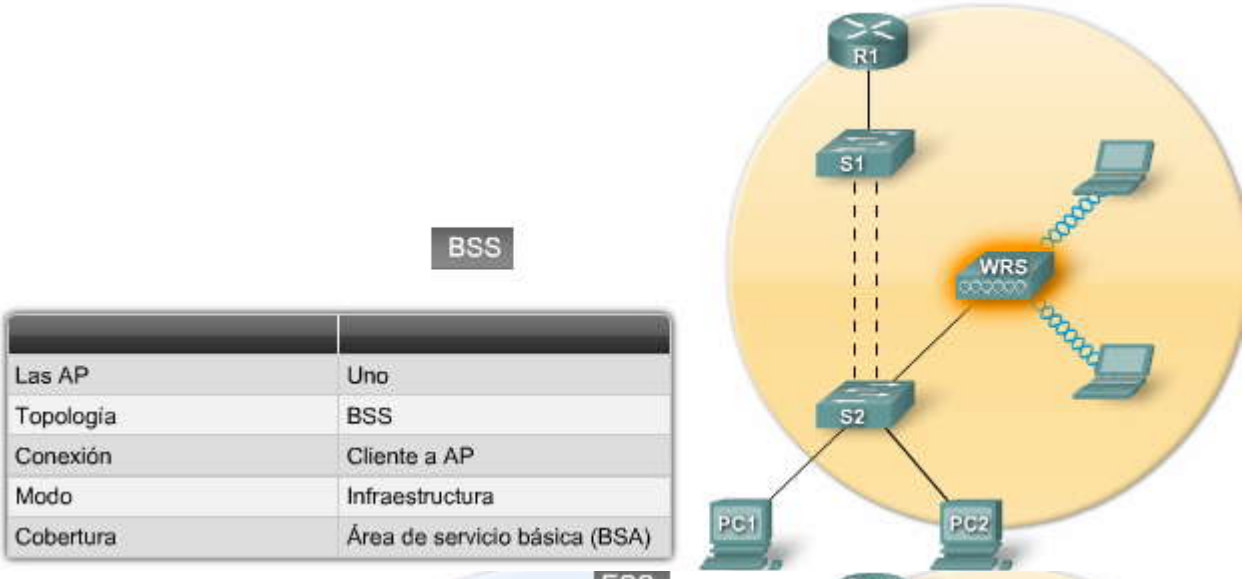
Sistema de distribución común

El sistema de distribución común permite a los puntos de acceso múltiple en un ESS aparentar ser un BSS simple. Un ESS incluye generalmente un SSID común para permitir al usuario moverse de un punto de acceso a otro.

Las celdas representan el área de cobertura proporcionada por un único canal. Un ESS debe tener de 10 a 15 por ciento de superposición entre celdas en un área de servicio extendida. Con un 15 por ciento de superposición entre celdas, un SSID y canales no superpuestos (una celda en canal 1 y la otra en canal 6), se puede crear la capacidad de roaming.

Haga clic en el botón Resumen en la figura para ver las comparaciones de las topologías WLAN.





Las AP	Uno
Topología	BSS
Conexión	Cliente a AP
Modo	Infraestructura
Cobertura	Área de servicio básica (BSA)

Las AP	Más de una
Topología	ESS
Conexión	Cliente a AP
Modo	Infraestructura
Cobertura	Área de servicio extendida (ESA)

Resumen de las topologías WLAN Resumen

Dispositivos inalámbricos	Modo de topología	Topología del bloque del edificio	Área de cobertura
No hay puntos de acceso	Ad hoc	Conjunto de servicios básicos independientes (IBSS)	Área de servicio básica (BSA)
Un punto de acceso	Infraestructura	Conjunto de servicio básico (BSS)	Área de servicio básica (BSA)
Más de un punto de acceso	Infraestructura	Conjunto de servicio extendido (ESS)	Área de servicio extendida (ESA)

Asociación punto de acceso y cliente

Una parte clave del proceso de 802.11 es descubrir una WLAN y, luego, conectarse a ella. Los componentes principales de este proceso son los siguientes:

Beacons - Tramas que utiliza la red WLAN para comunicar su presencia.
Sondas - Tramas que utilizan los clientes de la WLAN para encontrar sus redes.
Autenticación - Proceso que funciona como instrumento del estándar original 802.11, que el estándar todavía exige.
Asociación - Proceso para establecer la conexión de datos entre un punto de acceso y un cliente WLAN.

El propósito principal de la beacon es permitir a los clientes de la WLAN conocer qué redes y puntos de acceso están disponibles en un área dada, permitiéndoles, por lo tanto, elegir qué red y punto de acœso utilizar. Los puntos de acceso pueden transmitir beacons periódicamente.

Aunque las beacons pueden transmitirse regularmente por un punto de acceso, las tramas para sondeo, autenticación y asociación se utilizan sólo durante el proceso de asociación (o reasociación).

Proceso conjunto 802.11 (Asociación)

Antes de que un cliente 802.11 pueda enviar información a través de una red WLAN, debe atravesar el siguiente proceso de tres etapas:

Haga clic en el botón Sondear en la figura.
Etapa 1 - Sondeo de 802.11

Los clientes buscan una red específica mediante un pedido de sondeo a múltiples canales. El pedido de sondeo especifica el nombre de la red (SSID) y las tasas de bit. Un cliente típico de WLAN se configura con el SSID deseado, de modo que los pedidos de sondeo del cliente WLAN contienen el SSID de la red WLAN deseada.

Si el cliente WLAN sólo quiere conocer las redes WLAN disponibles, puede enviar un pedido de sondeo sin SSID, y todos los puntos de acceso que estén configurados para responder este tipo de consulta, responderán. Las WLAN con la característica de broadcast SSID deshabilitada no responderán.

Haga clic en el botón Autenticar en la figura.

Etapa 2 - Autenticación 802.11

802.11 se desarrolló originalmente con dos mecanismos de autenticación. El primero, llamado autenticación abierta, es fundamentalmente una autenticación NULL donde el cliente dice "autentícame", y el punto de acceso responde con "sí". Éste es el mecanismo utilizado en casi todas las implementaciones de 802.11.

Un segundo mecanismo de autenticación se basa en una clave que es compartida por la estación del cliente y el punto de acceso llamado Protección de equivalencia por cable (cable WEP). La idea de la clave WEP compartida es que le permita a una conexión inalámbrica la privacidad equivalente a una conexión por cable, pero cuando originalmente se implementó este método de autenticación resultó deficiente. A pesar de que la clave de autenticación compartida necesita estar incluida en las implementaciones de cliente y de punto de acceso para el cumplimiento general de los estándares, no se utiliza ni se recomienda.

Haga clic en el botón Asociar en la figura.

Etapa 3 - asociación 802.11

Esta etapa finaliza la seguridad y las opciones de tasa de bit, y establece el enlace de datos entre el cliente WLAN y el punto de acceso. Como parte de esta etapa, el cliente aprende el BSSID, que es la dirección MAC del punto de acceso, y el punto de acceso traza un camino a un puerto lógico conocido como el identificador de asociación (AID) al cliente WLAN. El AID es equivalente a un puerto en un switch. El proceso de asociación permite al switch de infraestructura seguir la pista de las tramas destinadas para el cliente WLAN, de modo que puedan ser reenviadas.

Una vez que un cliente WLAN se asoció con un punto de acceso, el tráfico puede viajar de un dispositivo a otro.

Asociación del cliente y el punto de acceso

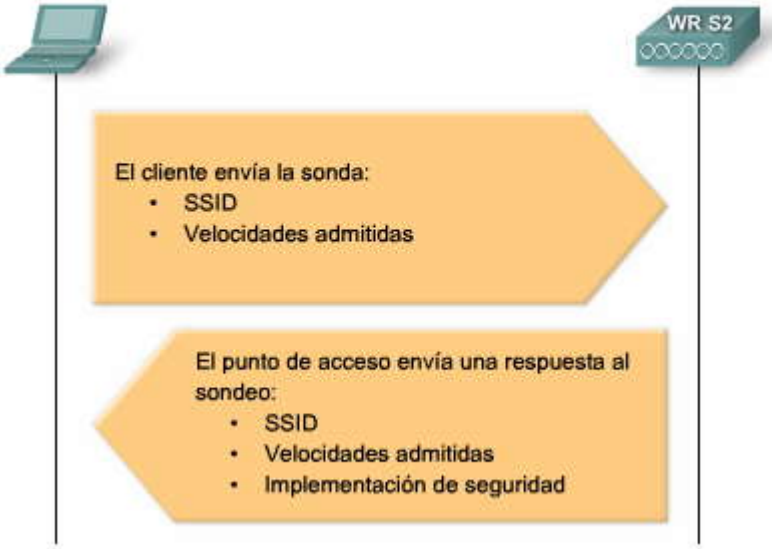
El punto de acceso emite beacon periódicos:

- SSID
- Velocidades admitidas
- Implementación de la seguridad (por ejemplo: WPA2)

Los clientes con NIC de radio "escuchan" el beacon:

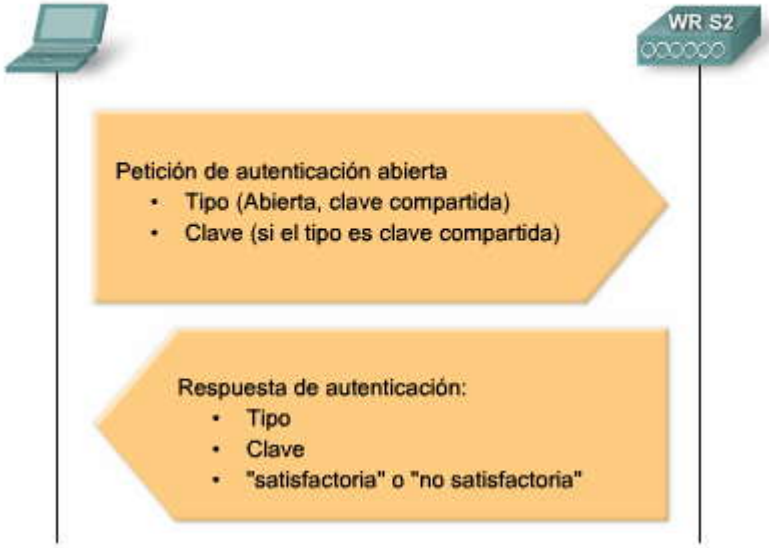
Sondear

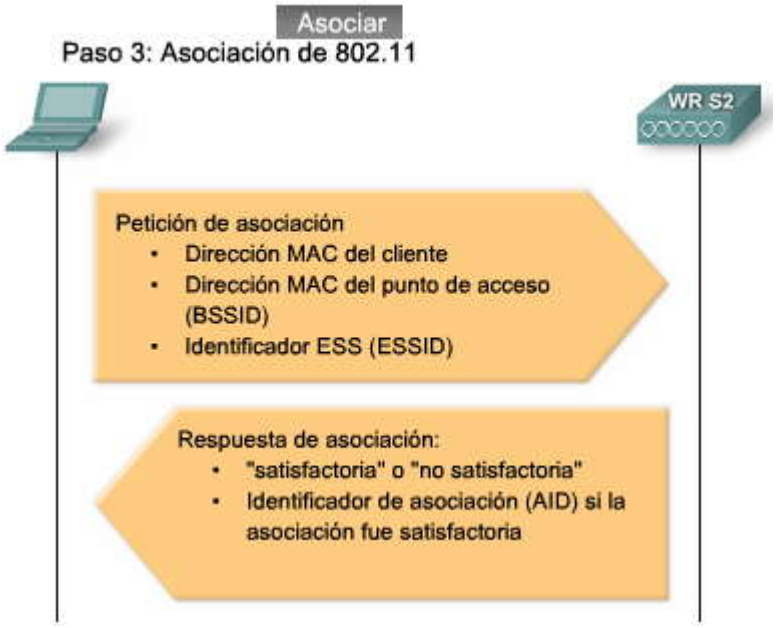
Paso 1: Sondeo de 802.11



Autenticar

Paso 2: autenticación de 802.11





7.1.5 PLANIFICACIÓN DE LA LAN INALÁMBRICA.-

Planificación de la LAN inalámbrica

Implementar una WLAN que saque el mejor provecho de los recursos y entregue el mejor servicio puede requerir de una planificación cuidadosa. Las WLAN pueden abarcar desde instalaciones relativamente simples a diseños intrincados y muy complejos. Se necesita un plan bien diseñado antes de poder implementar una red inalámbrica. En este tema, presentamos las consideraciones que deben tenerse en cuenta para el diseño y la planificación de una LAN inalámbrica.

El número de usuarios que una WLAN puede admitir no es un cálculo simple. El número de usuarios depende de la distribución geográfica de sus instalaciones (cuántos cuerpos y dispositivos entran en un espacio), las velocidades de transmisión de datos que los usuarios esperan (porque la RF es un medio compartido y, a mayor cantidad de usuarios, hay una mayor cantidad de disputa por la RF), el uso de canales no superpuestos mediante puntos de acceso múltiples en un ESS y la configuración de la energía de transmisión (que están limitadas por regulación local).Tendrá suficiente soporte inalámbrico para sus clientes si planifica su red para una cobertura RF adecuada en un ESS. Las consideraciones detalladas acerca de cómo planificar números específicos de usuarios están más allá del alcance de este curso.

Haga clic en el botón Asignar en la figura.

Al planificar la ubicación de los puntos de acceso, puede que no sea capaz de simplemente dibujar los círculos del área de cobertura y volcarlos en un plano. El área de cobertura circular aproximada es muy importante, pero existen algunas recomendaciones adicionales.

Si los puntos de acceso utilizarán cableado existente o si existen ubicaciones donde los puntos de acceso no pueden ubicarse, anote estas ubicaciones en el mapa.

Posicione los puntos de acceso sobre las obstrucciones.
Posicione los puntos de acceso en forma vertical, cerca del techo en el centro de cada área de cobertura, de ser posible.
Posicione los puntos de acceso en las ubicaciones donde se espera que estén los usuarios. Por ejemplo: las salas de conferencia son una mejor ubicación para los puntos de acceso que un vestíbulo.

Cuando estas indicaciones se hayan tenido en cuenta, estime el área de cobertura esperada de un punto de acceso. Este valor varía dependiendo del estándar WLAN o el conjunto de estándares que esté distribuyendo, la naturaleza de las instalaciones, la energía de transmisión para la cual el punto de acceso está configurado, etc. Siempre consulte las especificaciones para el punto de acceso cuando planifica las áreas de cobertura.

Basándose en su plano, ubique los puntos de acceso en el plano del piso, de modo que los círculos de cobertura se superpongan, como se ilustra en el siguiente ejemplo.

Cálculo de ejemplo

El auditorio abierto (un edificio del tipo Depósito/Fabrica) que se muestra en la figura es de aproximadamente 20 000 pies cuadrados.

Los requerimientos de la red especifican que debe haber un mínimo de 6 Mb/s 802.11b de rendimiento en cada BSA, porque hay una voz inalámbrica sobre la implementación de la WLAN superpuesta en esta red. Con los puntos de acceso se pueden lograr 6 Mbps en áreas abiertas como las del mapa, con un área de cobertura de 5000 pies cuadrados en muchos ambientes.

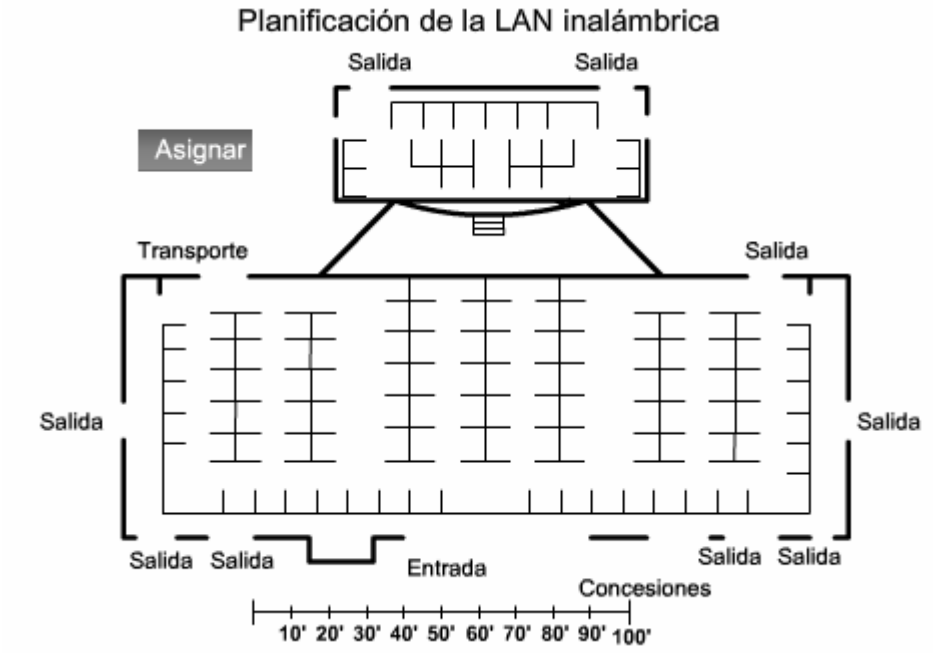
Nota: El área de cobertura de 5000 pies cuadrados es para un cuadrado. El BSA toma su radio diagonalmente desde el centro de este cuadrado.

Determinemos dónde ubicar los puntos de acceso.

Haga clic en el botón Área de cobertura en la figura.

Las instalaciones tienen 20 000 pies cuadrados, por lo tanto, dividir 20 000 pies cuadrados por un área de cobertura de 5000 pies cuadrados por punto de acceso resulta en, al menos, cuatro puntos de acceso requeridos para el auditorio. A continuación, determine la dimensión de las áreas de cobertura y acomódelas en el plano de la planta.

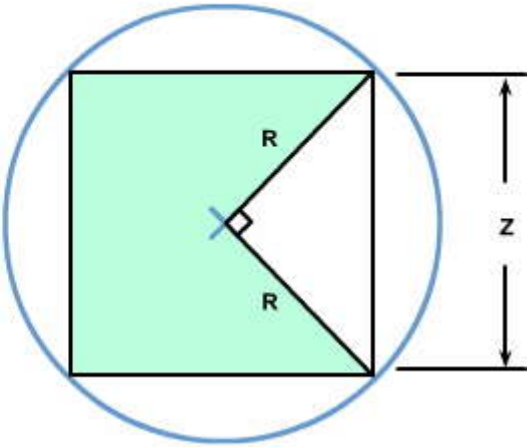
Dado que el área de cobertura es un cuadrado con un lado "Z", el círculo tangente a sus cuatro esquinas tiene un radio de 50 pies, como se muestra en los cálculos.
Cuando las dimensiones del área de cobertura se determinen, debe acomodarlas de manera similar a las que se muestran para las Áreas de cobertura alineadas en la figura. Haga clic en el botón Alineación de áreas de cobertura en la figura.
En su mapa de plano de planta, dibuje cuatro círculos de cobertura de 50 pies de radio de modo que se superpongan, como se muestra en el Plano. Haga clic en el botón Plano en la figura.



Área de cobertura

Los requerimientos especifican un Área de cobertura, A = 5000 metros cuadrados

Donde $A = Z^2$, Encuentre R



A partir de Pitágoras:

$2R^2 = Z^2$

Salida

$R = \sqrt{Z^2/2}$

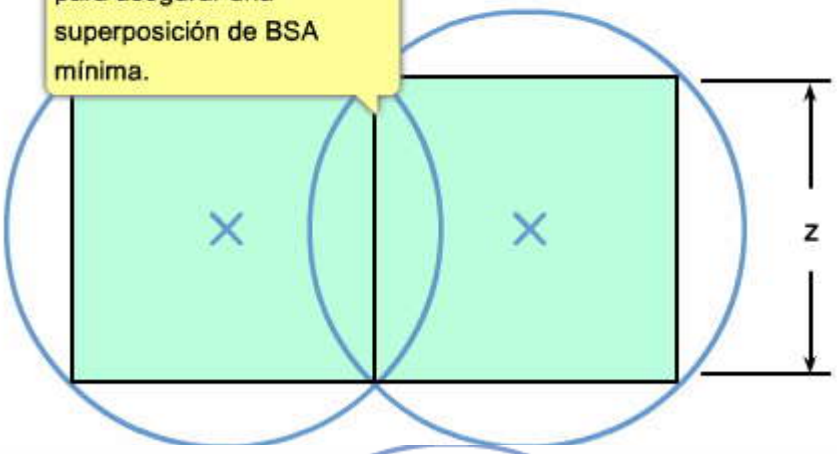
$R = \sqrt{5000 \text{ pie cuadrado}/2}$

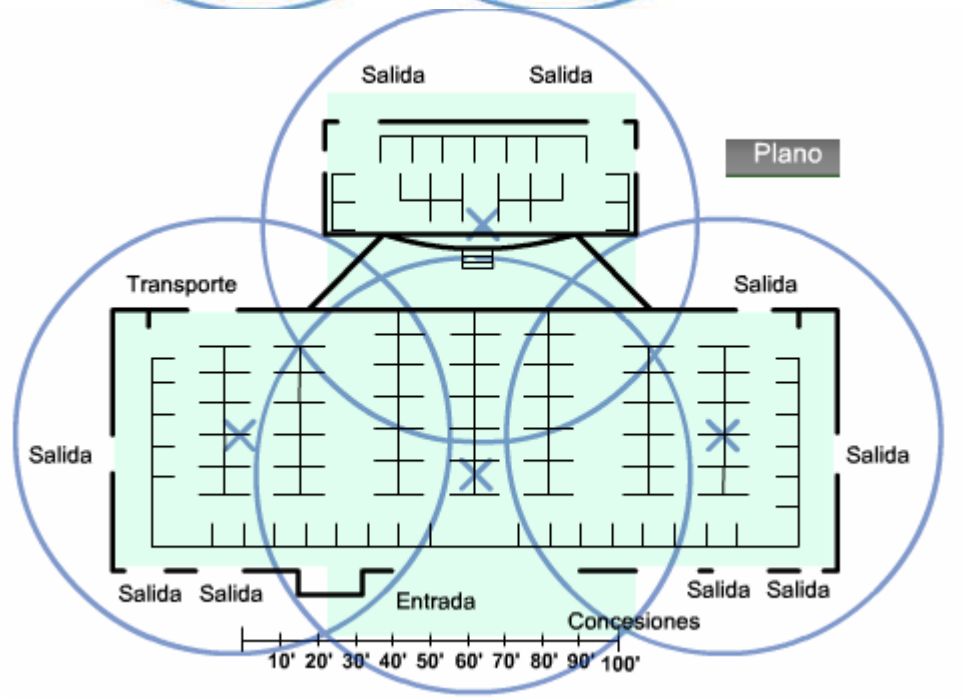
$R = \sqrt{2500 \text{ pie cuadrado}}$

R = 50 pie; Z = 70.71 pie

Alineación de áreas de cobertura

Alineación de las áreas de cobertura a lo largo de "Z" para asegurar una superposición de BSA mínima.





Estándar	Año ratificado	Banda RF	Modulación	Velocidad de datos	Intervalo
802.11b	1999	2,4-GHz	DSSS	Hasta 11 Mbps	150 pies o 46 m
802.11a	1999	5-GHz	OFDM	Hasta 54 Mbps	150 pies o 46 m
802.11g	2003	2,4-GHz	OFDM y DSSS	Hasta 54 Mbps	150 pies o 46 m
802.11n	2008	No confirmado	MIMO	248 Mbps	230 pies o 70 m

Frase	Respuesta
La _____ habilita una estación cliente que pueda enviar y recibir señales RF.	NIC inalámbrico
Un _____ conecta clientes inalámbricos a la LAN conectada por cable.	puntos de acceso
Los clientes inalámbricos que están en el alcance máximo y en lados opuestos de un punto de acceso no podrán conectarse entre sí o detectar las transmisiones del otro. A esto se lo conoce como el problema de _____ .	nodo oculto
Se desarrolló _____ para resolver el problema del nodo oculto. Cuando esté habilitado, el punto de acceso asignará el medio a la estación peticionante por el tiempo que sea necesario para completar la transmisión.	RTS/CTS
Las computadoras personales ubicadas en una instalación existente no conectada por cable, puede tener instalado un _____ inalámbrico.	PCI NIC
Un _____ como el WRT300N cumple el rol de punto de acceso, switch Ethernet y router.	router inalámbrico
En la década de los noventa, los NIC inalámbricos para computadoras portátiles eran tarjetas que se deslizaban dentro de la ranura _____.	PCMCIA

Frase	Respuesta					
Cuando un punto de acceso Linksys se configura para permitir clientes de 802.11b y 802.11g, opera en modo _____.	mixto					
La banda de 2,4 GHz se divide en ____ canales para Norteamérica y ____ canales para Europa.	11		13			
La optimización para las WLAN que requieren puntos de acceso múltiples debe utilizar canales no superpuestos. Si hay tres puntos de acceso adyacentes, utilice los canales ___, ___ y ___.	1		6		5	
La piedra fundamental de la arquitectura IEEE 802.11 LAN inalámbrica es la ____.	Conjunto de servicios básicos					
Cuando un único BSS provee una cobertura RF insuficiente, se pueden unir uno o más a través de un sistema de distribución común, a un _____.	área de servicio extendida					
El _____ permite puntos de acceso múltiples en un ESS para aparentar ser un BSS único.	sistema de distribución común					
La red WLAN utiliza _____ para reconocer su presencia, mientras que los clientes WLAN utilizan _____ para encontrar una red WLAN.	beacons		sondas			

7.2 SEGURIDAD LAN INALÁMBRICA.-

7.2.1 AMENAZAS A LA SEGURIDAD INALÁMBRICA.-

Acceso no autorizado

La seguridad debe ser una prioridad para cualquiera que utilice o administre redes. Las dificultades para mantener segura una red conectada por cable se multiplican con una red inalámbrica. Una WLAN está abierta a cualquiera dentro del alcance de un punto de acceso y de las credenciales apropiadas para asociarse a él. Con un NIC inalámbrico y conocimiento de técnicas de decodificación, un atacante no tendrá que entrar físicamente al espacio de trabajo para obtener acceso a una WLAN.

En este primer tema de esta sección, describimos cómo evolucionaron las amenazas de seguridad. Estas preocupaciones de seguridad son incluso más significativas cuando se trata con redes de empresas, porque el sustento de vida de la empresa depende de la protección de su información. En estos casos, las violaciones a la seguridad pueden tener graves repercusiones, sobre todo si la empresa guarda información financiera relacionada con sus clientes.

Hay tres categorías importantes de amenaza que llevan a acceso no autorizado:

Buscadores de redes inalámbricas abiertas
Piratas informáticos (Crackers)
Empleados

"Búsqueda de redes inalámbricas abiertas" se refería originalmente a la utilización de un dispositivo de rastreo para buscar números de teléfonos celulares para explotar. Búsqueda de redes inalámbricas abiertas, ahora también significa conducir alrededor de un vecindario con una computadora portátil y una tarjeta de cliente 802.11b/g en búsqueda de un sistema 802.11b/g no seguro para explotar.

El término pirata informático originalmente significaba una persona que explora a fondo los sistemas de computación para entender y tal vez explotar por razones creativas, la estructura y complejidad de un sistema. Hoy en día, los términos pirata informático y cracker describen a intrusos maliciosos que ingresan en sistemas como delincuentes y roban información o dañan los sistemas deliberadamente. Los piratas informáticos con la intención de dañar son capaces de explotar las medidas de seguridad débiles.

La mayoría de los dispositivos vendidos hoy en día están preparados para funcionar en una WLAN. En otras palabras, los dispositivos tienen configuraciones predeterminadas y pueden instalarse y utilizarse con poca o ninguna configuración por parte de los usuarios. Generalmente, los usuarios finales no cambian la configuración predeterminada, y dejan la autenticación de cliente abierta, o pueden implementar solamente una seguridad WEP estándar. Desafortunadamente, como mencionamos antes, las claves WEP compartidas son defectuosas y por consiguiente, fáciles de atacar.

Herramientas con propósito legítimo, como los husmeadores inalámbricos, permiten a los ingenieros de red capturar paquetes de información para depurar el sistema. Los intrusos pueden utilizar estas mismas herramientas para explotar las debilidades de seguridad.

Puntos de acceso no autorizados

Un punto de acceso no autorizado es un punto de acceso ubicado en una WLAN que se utiliza para interferir con la operación normal de la red. Si un punto de acceso no autorizado se configura correctamente, se puede capturar información del cliente. Un punto de acceso no autorizado también puede configurarse para proveer acceso no autorizado a usuarios con información como las direcciones MAC de los clientes (tanto inalámbricas como conectadas por cable), o capturar y camuflar paquetes de datos o, en el peor de lo casos, obtener acceso a servidores y archivos.

Una versión simple y común de un punto de acceso no autorizado es uno instalado por empleados sin autorización. Los empleados instalan puntos de acceso con la intención de utilizar la red de la empresa en su hogar. Estos puntos de acceso no tienen la configuración de seguridad típica necesaria, por lo tanto la red termina con una brecha en su seguridad.

Acceso no autorizado

"Buscadores de redes inalámbricas abiertas"	Piratas informáticos	Empleados
Encuentran "Redes" abiertas; las utilizan para conseguir acceso gratis a Internet	Explotan medidas de privacidad débiles para ver información de WLAN sensible e incluso ingresar sin autorización a las WLAN.	Enchufan las APL/gateways de calidad comercial a los puntos Ethernet de la compañía para crear sus propias WLAN

Ataques de Hombre-en-el-medio

Uno de los ataques más sofisticados que un usuario no autorizado puede realizar se llama ataque de hombre-en-el-medio (MITM). El atacante selecciona un host como objetivo y se posiciona logísticamente entre el objetivo y el router o gateway del objetivo. En un ambiente de LAN conectada por cable, el atacante necesita poder acceder físicamente a la LAN para insertar un dispositivo lógico dentro de la topología. Con una WLAN, las ondas de radio emitidas por los puntos de acceso pueden proveer la conexión.

Las señales de radio desde las estaciones y puntos de acceso son "audibles" para cualquiera en un BSS con el equipo apropiado, como una computadora portátil y un NIC. Dado que los puntos de acceso actúan como hubs Ethernet, cada NIC en el BSS escucha todo el tráfico. El dispositivo descarta cualquier tráfico no dirigido al mismo. Los atacantes pueden modificar el NIC de su computadora portátil con un software especial para que acepte todo el tráfico. Con esta modificación, el atacante puede llevar a cabo ataques MITM inalámbricos, usando el NIC de la computadora portátil como punto de acceso.

Para llevar a cabo este ataque, un pirata informático selecciona una estación como objetivo y utiliza software husmeador de paquetes, como Wireshark, para observar la estación cliente que se conecta al punto de acceso. El pirata informático puede ser capaz de leer y copiar el nombre de usuario objetivo, nombre del servidor y dirección IP del servidor y cliente, el ID

utilizado para computar la respuesta y el desafío y su respuesta asociada, que se pasa no cifrada entre la estación y el punto de acceso.

Si un atacante puede comprometer un punto de acceso, puede comprometer potencialmente a todos los usuarios en el BSS. El atacante puede monitorear un segmento de red inalámbrica completo y causar estragos en cualquier usuario conectado al mismo.

Prevenir un ataque MITM depende de la sofisticación de la infraestructura de su WLAN y su actividad de monitoreo y vigilancia en la red. El proceso comienza identificando los dispositivos legítimos en su WLAN. Para hacer esto, debe autenticar a los usuarios de su WLAN.

Cuando se conocen todos los usuarios legítimos, debe monitorear la red en busca de dispositivos y tráfico que no deberían estar allí. Las WLAN de empresas que utilizan dispositivos WLAN de tecnología avanzada proveen herramientas a los administradores que trabajan juntas como un sistema de prevención de intrusión inalámbrica (IPS). Estas herramientas incluyen escáners que identifican puntos de acceso no autorizados y redes ad hoc y también administración de recursos de radio (RRM) que monitorean la banda RF en busca de actividad y carga de puntos de acceso. Un punto de acceso que está más ocupado que de costumbre alerta al administrador sobre un posible tráfico no autorizado.

La explicación detallada de estas técnicas de mitigación escapa del alcance de este curso. Para mayor información, consulte al documento de CISCO "Addressing Wireless Threats with Integrated Wireless IDS and IPS" disponible en http://www.cisco.com/en/US/products/ps6521/products_white_paper0900aecd804f155b.shtml.

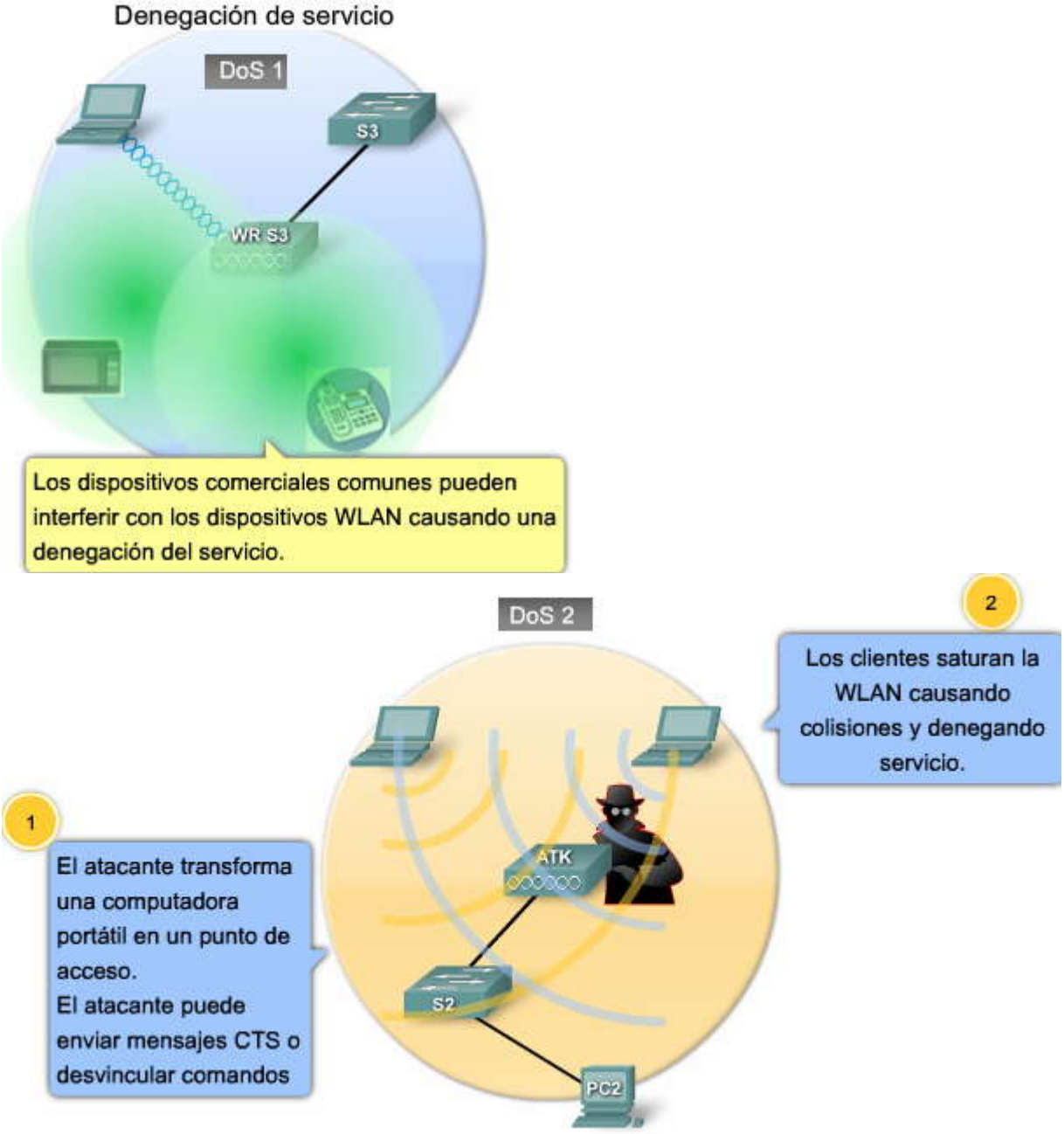
Denegación de servicio

Las WLAN 802.11b y g utilizan la banda 2,4 GHz ISM sin licencia. Ésta es la misma banda utilizada por la mayoría de los productos de consumo, incluyendo monitores de bebé, teléfonos inalámbricos y hornos de microondas. Con estos dispositivos que congestionan la banda RF, los atacantes pueden crear ruido en todos los canales de la banda con dispositivos comúnmente disponibles.

Haga clic en el botón DoS 2 en la figura.

Anteriormente discutimos sobre cómo un atacante puede convertir un NIC en un punto de acceso. Ese truco también se puede utilizar para crear un ataque DoS. El atacante, mediante una PC como punto de acceso, puede inundar el BSS con mensajes listos para enviar (CTS), que inhabilitan la función de CSMA/CA utilizada por las estaciones. Los puntos de acceso, a su vez, inundan la BSS con tráfico simultáneo y causan un stream constante de colisiones.

Otro ataque DoS que puede lanzarse en un BSS es cuando un atacante envía una serie de comandos desvinculados que causa que todas las estaciones en el BSS se desconecten. Cuando las estaciones están desconectadas, tratande reasociarse inmediatamente, lo que crea una explosión de tráfico. El atacante envía otro comando desvinculado y el ciclo se repite.



7.2.2 PROTOCOLOS DE SEGURIDAD INALÁMBRICOS.-

Descripción general del protocolo inalámbrico

En este tema, aprenderá acerca de las características de los protocolos inalámbricos comunes y del nivel de seguridad que cada uno provee.

Se introdujeron dos tipos de autenticación con el estándar 802.11 original: clave de autenticación WEP abierta y compartida. Mientras la autenticación abierta en realidad es "no autenticación", (un cliente requiere autenticación y el punto de acceso la permite), la autenticación WEP debía proveer privacidad a un enlace, como si fuera un cable conectado de una PC a una conexión de pared Ethernet. Como se mencionó anteriormente, las claves WEP compartidas demostraron ser defectuosas y se requería algo mejor. Para contrarrestar las debilidades de la clave WEP compartida, el primer enfoque de las compañías fue tratar técnicas como SSID camuflados y filtrado de direcciones MAC. Estas técnicas también son muy débiles. Aprenderá más acerca de las debilidades de estas técnicas más adelante.

Las fallas con la encriptación de la clave WEP compartida están desdobladas. Primero, el algoritmo utilizado para encriptar la información podía ser descifrado por crackers. Segundo, la escalabilidad era un problema. Las claves WEP de 32 bit se

administraban manualmente, de modo que los usuarios ingresaban manualmente, por lo general, de manera incorrecta, lo que creaba llamadas a las mesas de ayuda de soporte técnico.

Luego de las debilidades de una seguridad basada en WEP, hubo un período de medidas de seguridad interinas. Los proveedores como Cisco, al querer cumplir con la demanda de mejor seguridad, desarrollaron sus propios sistemas mientras ayudaban simultáneamente a desarrollar el estándar 802.11i. En el camino hacia el 802.11i, se creó el algoritmo de encriptación TKIP, que estaba enlazado con el método de seguridad de Acceso protegido WiFi (WPA) de la Wi-Fi Alliance.

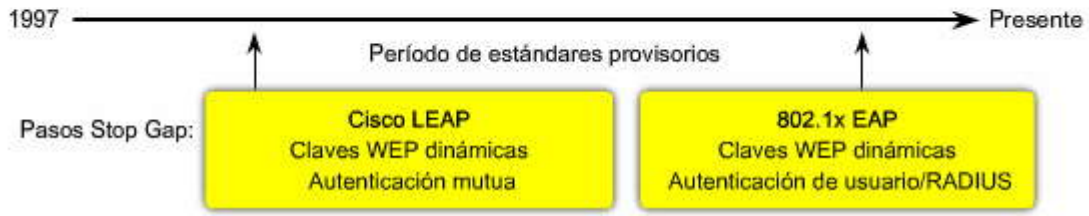
Hoy, el estándar que se debe seguir en la mayoría de las redes de empresas es el estándar 802.11i. Es similar al estándar WPA2 de la Wi-Fi Alliance. Para empresas, el WPA2 incluye una conexión a una base de datos del Servicio de autenticación remota de usuario de acceso telefónico (RADIUS). El RADIUS se describirá más adelante en el capítulo.

Para más información acerca de las debilidades de la seguridad WEP, vea el informe "Security of the WEP algorithm" disponible en http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

Descripción general del protocolo inalámbrico

Pasos principales para proteger una WLAN

Acceso abierto	Encriptación de primera generación	Provisoria	Presente
SSID	WEP	WPA	802.11i/WPA2
• sin encriptación • Autenticación básica • Manejo no seguro	• Sin autenticación fuerte • Claves estáticas, frágiles • No escalable	• Estandarizada • Encriptación mejorada • Autenticación fuerte, basada en el usuario (por ejemplo, LEAP, PEAP, EAP-FAST)	• Encriptación AES • Autenticación: 802.1X • Administración de clave dinámica • WPA2 es la implementación Wi-Fi Alliance de 802.11i



Autenticación de una LAN inalámbrica

En una red abierta, como una red de hogar, la asociación puede ser todo lo que se requiera para garantizar el acceso del cliente a servicios y dispositivos en la WLAN. En redes que tengan requerimientos de seguridad más estrictos, se requiere una autenticación o conexión para garantizar dicho acceso a los clientes. Este proceso de conexión lo administra el Protocolo de autenticación extensible (EAP). El EAP es una estructura para autenticar el acceso a la red. El IEEE desarrolló el estándar 802.11i WLAN para autenticación y autorización, para utilizar IEEE 802.1x.

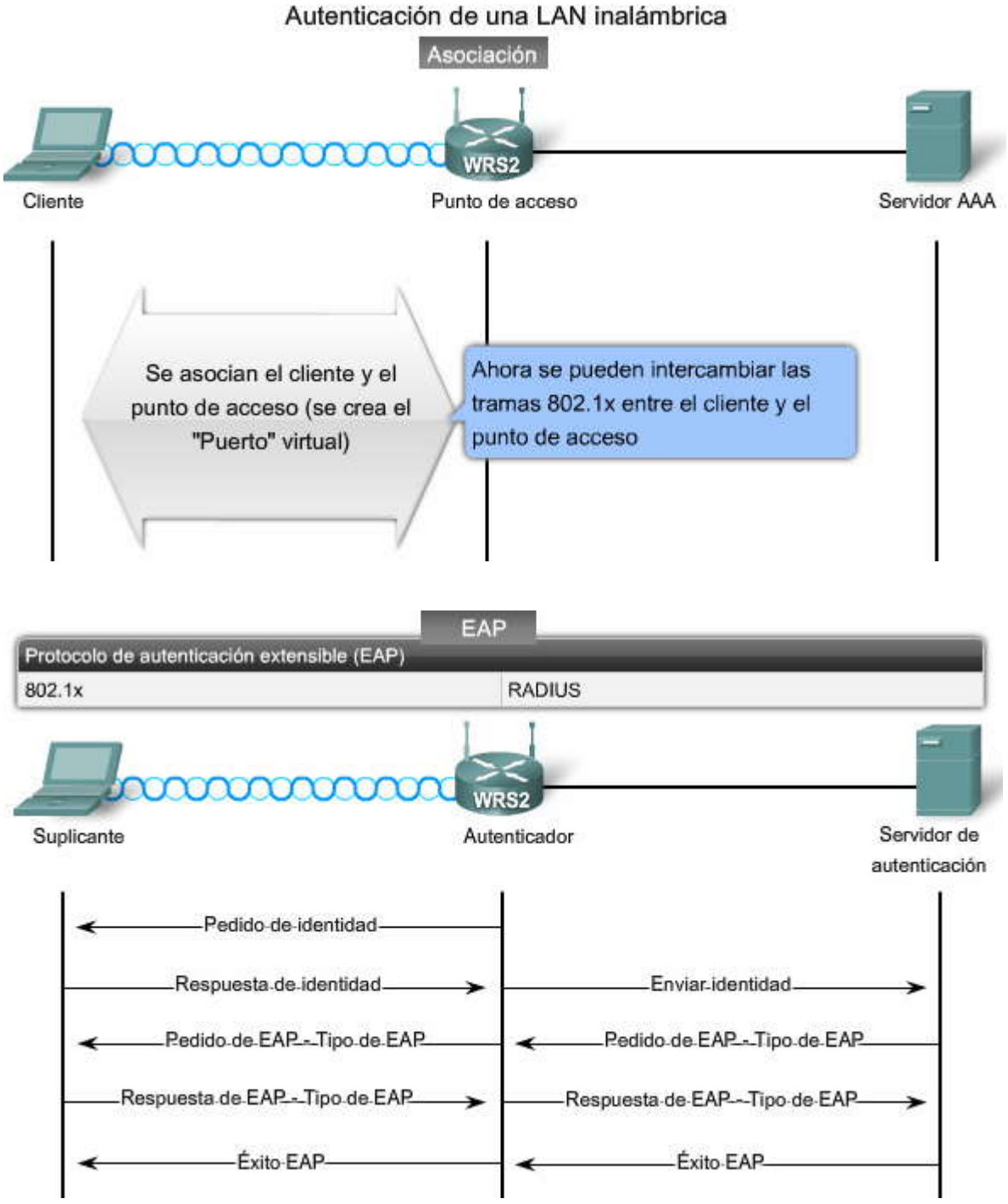
Haga clic en el botón EAP en la figura para ver el proceso de autenticación.
El proceso de autenticación WLAN de la empresa se resume de la siguiente manera:

El proceso de asociación 802.11 crea un puerto virtual para cada cliente WLAN en el punto de acceso.
El punto de acceso bloquea todas las tramas de datos, con excepción del tráfico basado en 802.1x.
Las tramas 802.1x llevan los paquetes de autenticación EAP a través del punto de acceso al servidor que mantiene las credenciales de autenticación. Este servidor tiene en ejecución un protocolo RADIUS y es un servidor de Autenticación, autorización y auditoria (AAA).
Si la autenticación EAP es exitosa, el servidor AAA envía un mensaje EAP de éxito al punto de acceso, que permite entonces que el tráfico de datos atraviese el puerto virtual desde el cliente de la WLAN.
Antes de abrir un puerto virtual se establece un enlace de datos encriptados entre el cliente de la WLAN y el punto de acceso establecido para asegurar que ningún otro cliente de la WLAN pueda acceder al puerto que se haya establecido para un cliente autenticado específico.

Antes de que se utilicen el 802.11i (WPA2) o incluso el WPA, algunas compañías intentaron asegurar sus WLAN al filtrar sus direcciones MAC y evitar transmitir SSID. Hoy, es fácil utilizar software para modificar las direcciones MAC adjuntas a los adaptadores; de esta manera, el filtrado de las direcciones MAC se evita fácilmente. No significa que no debe hacerlo, sino que si utiliza este método, debe respaldarlo con seguridad adicional, como WPA2.

Incluso si un SSID no se trasmite mediante un punto de acceso, el tráfico que viaja de un punto a otro entre el cliente y el punto de acceso revela, eventualmente, el SSID. Si un atacante monitorea pasivamente la banda RF, puede husmear el SSID en una de estas transacciones, porque se envía no cifrado. Esta facilidad para descubrir los SSID llevó a algunas personas a dejar encendido el broadcast SSID. De hacerlo, debe probablemente ser una decisión organizacional registrada en la política de seguridad.

La idea de que puede asegurar su WLAN con nada más que el filtrado MAC y apagando los broadcasts SSID, puedellevar a tener una WLAN totalmente insegura. La mejor manera de asegurar cuáles de los usuarios finales deben estar en la WLAN es utilizar un método de seguridad que incorpore un control de acceso a la red basado en puertos, como el WPA2.



Encriptación

Hay dos mecanismos de encriptación a nivel empresa especificados por el 802.11i certificados como WPA y WPA2 por la Wi-Fi Alliance: Protocolo de integridad de clave temporal (TKIP) y Estándar de encriptación avanzada (AES).

El TKIP es el método de encriptación certificado como WPA. Provee apoyo para el equipo WLAN heredado que atiende las fallas originales asociadas con el método de encriptación WEP 802.11. Utiliza el algoritmo de encriptación original utilizado por WEP.

El TKIP tiene dos funciones primarias:

Encripta el contenido de la Capa 2
Lleva a cabo una comprobación de la integridad del mensaje (MIC) en el paquete encriptado. Esto ayuda a asegurar que no se altere un mensaje.

Aunque el TKIP resuelve todas las debilidades conocidas del WEP, la encriptación AES de WPA2 es el método preferido, porque alinea los estándares de encriptación WLAN con los más amplios estándares IT y las optimizaciones de la industria, más notablemente el IEEE 802.11i.

El AES tiene las mismas funciones que el TKIP, pero utiliza información adicional del encabezado de la MAC que les permite a los hosts de destino reconocer si se alteraron los bits no encriptados. Además, agrega un número de secuencia al encabezado de información encriptada.

Cuando configura los puntos de acceso Linksys o los routers inalámbricos, como el WRT300N, puede que no vea el WPA o el WPA2; en lugar de eso, podrá ver referencias a algo llamado clave precompartida (PSK). A continuación, los distintos tipos de PSK:

PSK o PSK2 con TKIP es el mismo que WPA
PSK o PSK2 con AES es el mismo que WPA2
PSK2, sin un método de encriptación especificado, es el mismo que WPA2.

TKIP y AES

TKIP - Clave de integridad de clave temporal	AES - Estándar de encriptación avanzada
• Encripta mediante el agregado de codificación de bit cada vez más compleja a cada paquete • Basada en la misma cifra (RC4) que el WEP	• Nueva cifra utilizada en 802.11i • Basada en TKIP con características adicionales que mejoran el nivel de seguridad provista

7.2.3 PROTECCION DE UNA LAN INALÁMBRICA.-

Control del acceso a la LAN inalámbrica

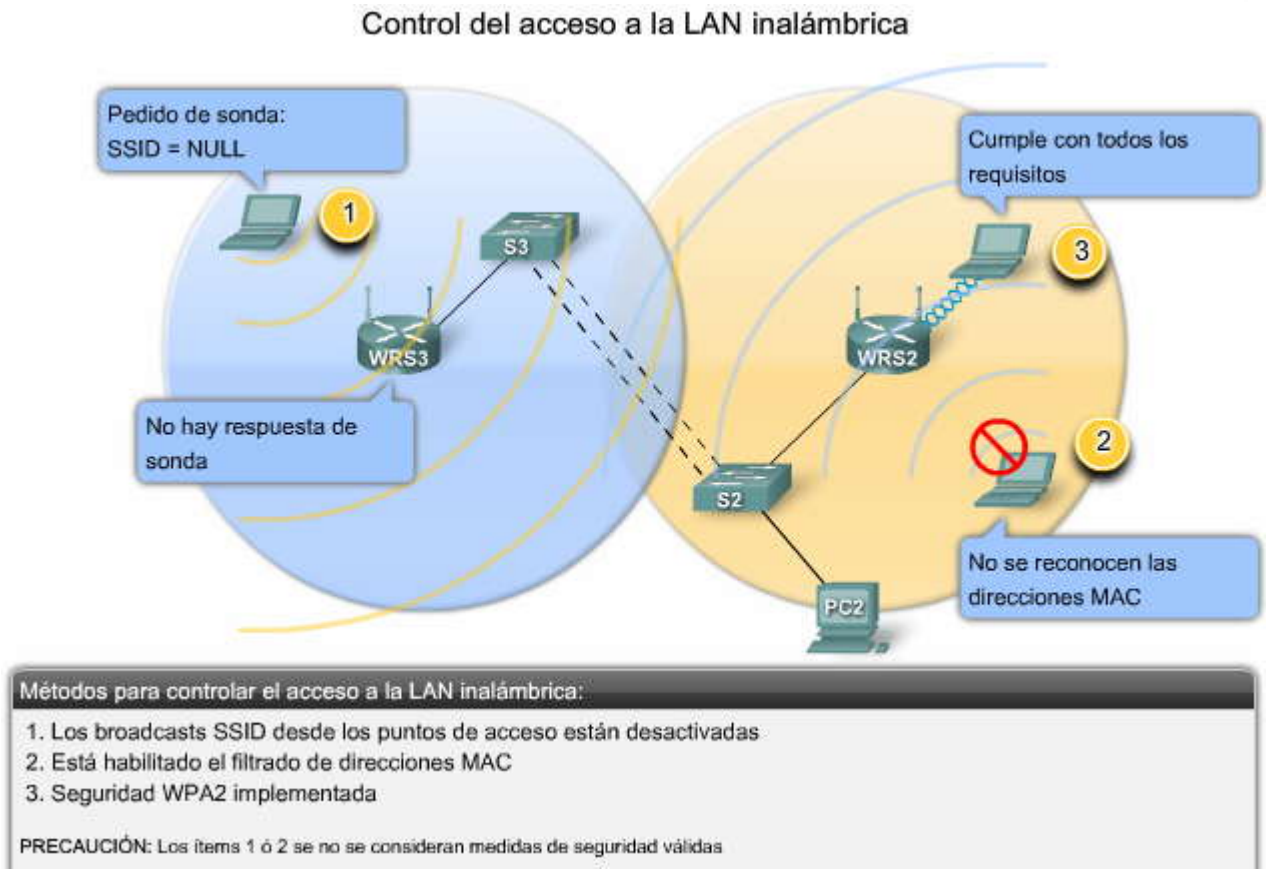
El concepto de profundidad significa que hay múltiples soluciones disponibles. Es como tener un sistema de seguridad en su casa pero, de todas maneras, cerrar las puertas y ventanas y pedirle a los vecinos que la vigilen por usted. Los métodos de seguridad que ha visto, especialmente el WPA2, son como tener un sistema de seguridad. Si quiere realizar algo extra para proteger el acceso a su WLAN, puede agregar profundidad, como se muestra en la figura, y así implementar este enfoque de tres pasos:

Camuflaje SSID - Deshabilite los broadcasts SSID de los puntos de acceso
Filtrado de direcciones MAC - Las Tablas se construyen a mano en el punto de acceso para permitir o impedir el acceso de clientes basado en sus dirección de hardware
Implementación de la seguridad WLAN - WPA o WPA2

Una consideración adicional para un administrador de redes alerta es configurar puntos de acceso cercanos a las paredes exteriores de edificios para transmitir en una configuración de energía menor que los otros puntos de acceso cercanos al centro del edificio. Esto es simplemente para reducir la firma RF en el exterior del edificio donde cualquiera que ejecute una aplicación como Netstumbler (http://www.netstumbler.com), Wireshark, o incluso Windows XP, pueda asignar las WLAN.

Ni el SSID camuflado ni el filtrado de direcciones MAC se consideran medios válidos para proteger a una WLAN, por los siguientes motivos:

Se puede suplantar la identidad de las direcciones MAC fácilmente.
Los SSID se descubren con facilidad, incluso si los puntos de acceso no los transmiten.



7.3 CONFIGURACION DEL ACCESO A LA LAN INALÁMBRICA.-

7.3.1 CONFIGURACION DEL PUNTO DE ACCESO INALAMBRICO.-

Descripción general del punto de acceso inalámbrico

En este tema, aprenderá cómo configurar un punto de acceso inalámbrico. Aprenderá cómo establecer el SSID, activar la seguridad, configurar el canal y ajustar la configuración de energía de un punto de acceso inalámbrico. También aprenderá cómo realizar un respaldo y restauración de la configuración de un punto de acceso inalámbrico típico.

Un enfoque básico a la implementación inalámbrica, como en cualquier trabajo de red básico, es configurar y probar progresivamente. Antes de implementar cualquier dispositivo inalámbrico, verifique la red existente y el acceso a Internet para los hosts conectados por cable. Inicie el proceso de implementación de la WLAN con un único punto de acceso y un único cliente, sin habilitar la seguridad inalámbrica. Verifique que el cliente inalámbrico haya recibido una dirección IP DHCP y pueda hacer ping al router predeterminado conectado por cable y luego explore hacia la Internet externa. Finalmente, configure la seguridad inalámbrica con WPA2. Utilice WEP sólo si el hardware no admite WPA.

La mayoría de los puntos de acceso están diseñados para que sean funcionales ni bien salen de su embalaje con la configuración predeterminada. Es una buena práctica cambiar las configuraciones predeterminadas iniciales. Muchos puntos de acceso se pueden configurar a través de una interfaz web GUI.

Con un plan para la implementación en mente, la conectividad de la red conectada por cable confirmada y el punto de acceso instalado, configurará la red. El siguiente ejemplo utiliza el dispositivo multifunción Linksys WRT300N. Este dispositivo incluye un punto de acceso.

Los pasos para configurar el Linksys WRT300N son los siguientes:

Asegúrese de que su PC esté conectada al punto de acceso mediante una conexión por cable y el acceso a la utilidad web con un explorador Web. Para acceder a la utilidad basada en la web del punto de acceso, inicie Internet Explorer o Netscape Navigator e ingrese la dirección IP predeterminada del WRT300N, 192.168.1.1, en el campo dirección. Presione la tecla Enter.

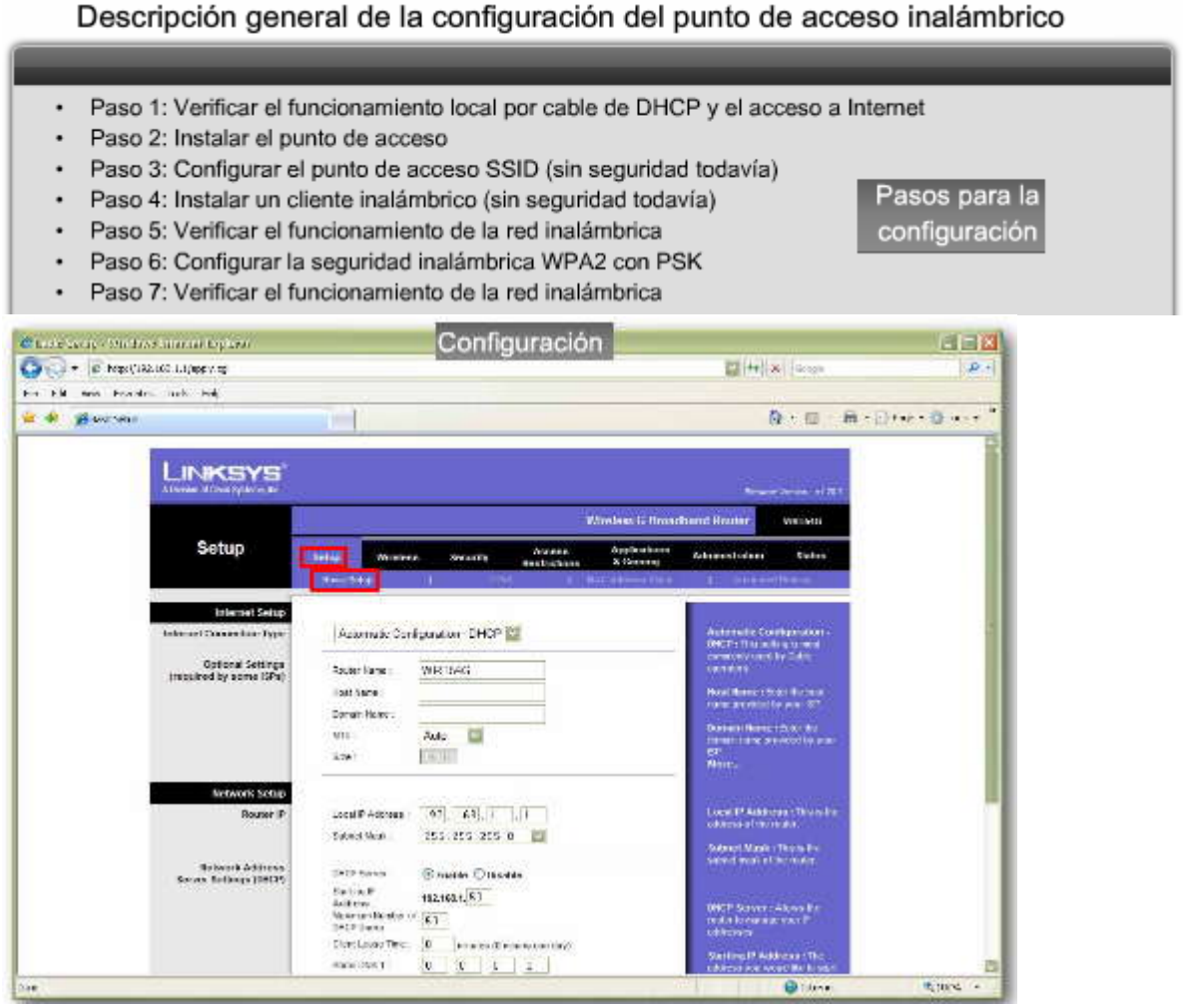
Aparece una pantalla que le pide su nombre de usuario y contraseña. Deje el campo Nombre de usuario en blanco. Ingrese admin en el campo Contraseña. Ésta es la configuración predeterminada para un Linksys WRT300N. Si ya se configuró el dispositivo, el nombre de usuario y la contraseña pueden haber cambiado. Haga clic en Aceptar para continuar.

Para una configuración básica de red, utilice las siguientes pantallas, como se muestra cuando hace clic en los botones Configuración, Administración, e Inalámbrico en la figura:

Configuración - Ingrese la configuración básica de red (dirección IP).
Administración - Haga clic en la etiqueta Administración y luego seleccione la pantalla de Administración La contraseña predeterminada es admin. Para proteger el punto de acceso, cambie la contraseña predeterminada.
Inalámbrico - Cambie el SSID predeterminado en la etiqueta de Configuración inalámbrica básica . Seleccione el nivel de seguridad en la etiqueta de Seguridad inalámbrica y complete las opciones para el modo de seguridad elegido.

Realice los cambios necesarios dentro de la utilidad. Cuando termine de realizar los cambios a la pantalla, haga clic en el botón Guardar cambios , o haga clic en el botón Cancelar cambios para deshacer sus cambios. Para información en una etiqueta, haga clic en Ayuda.

La figura resume los pasos de implementación para un punto de acceso.



Configuración de la configuración inalámbrica básica

La pantalla de Configuración básica es la primera pantalla que ve cuando accede a la utilidad basada en la web. Haga clic en la etiqueta Inalámbrica y luego seleccione la etiqueta Configuración inalámbrica básica.

Configuraciones básicas inalámbricas

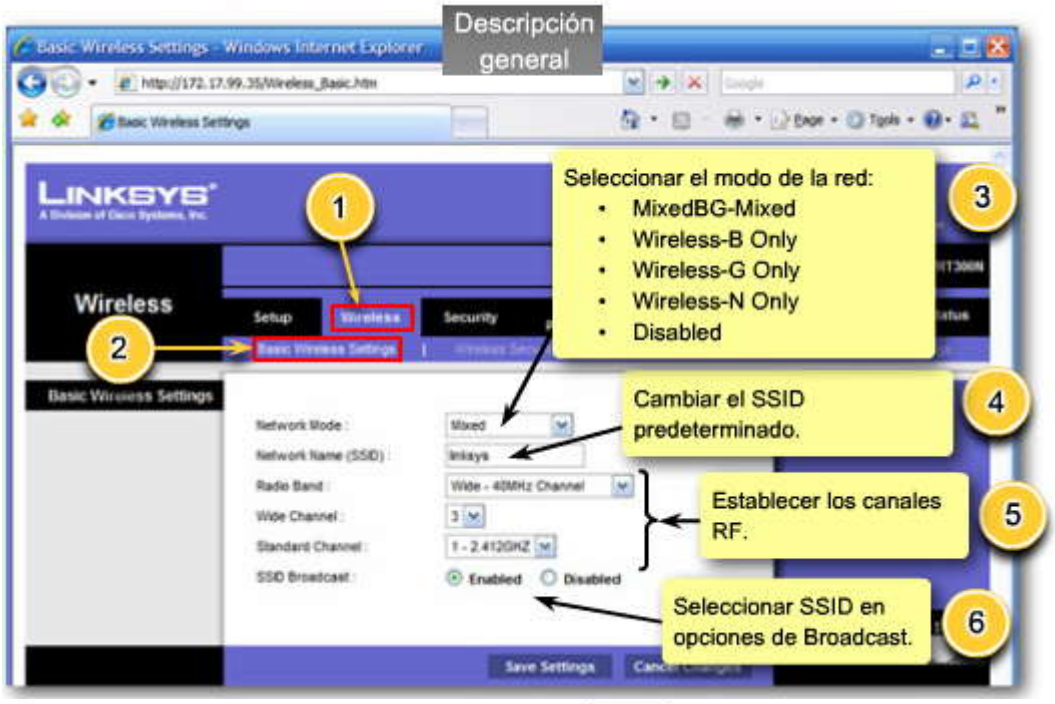
Haga clic en los botones a lo largo de la parte inferior de la figura para ver el GUI para cada configuración.

Modo de red - Si tiene los dispositivos Wireless-N, Wireless-G, y 802.11b en su red, mantenga Mixta, la configuración predeterminada. Si tiene los dispositivos Wireless-G y 802.11b, seleccione BG-Mixto. Si sólo tiene dispositivos Wireless-N, seleccione Wireless-N solamente. Si sólo tiene dispositivos Wireless-G, seleccione Wireless-G solamente. Si sólo tiene dispositivos Wireless-B, seleccione Wireless-B solamente. Si quiere desactivar el networking, seleccione Deshabilitar.
Nombre de la red (SSID) - El SSID es el nombre de red compartido entre todos los puntos en la red inalámbrica. El SSID debe ser idéntico para todos los dispositivos en la red inalámbrica. Distingue entre mayúsculas y minúsculas, y no debe exceder los 32 caracteres (utilice cualquier carácter en el teclado). Para mayor seguridad, debe cambiar el SSID predeterminado (linksys) a un nombre único.

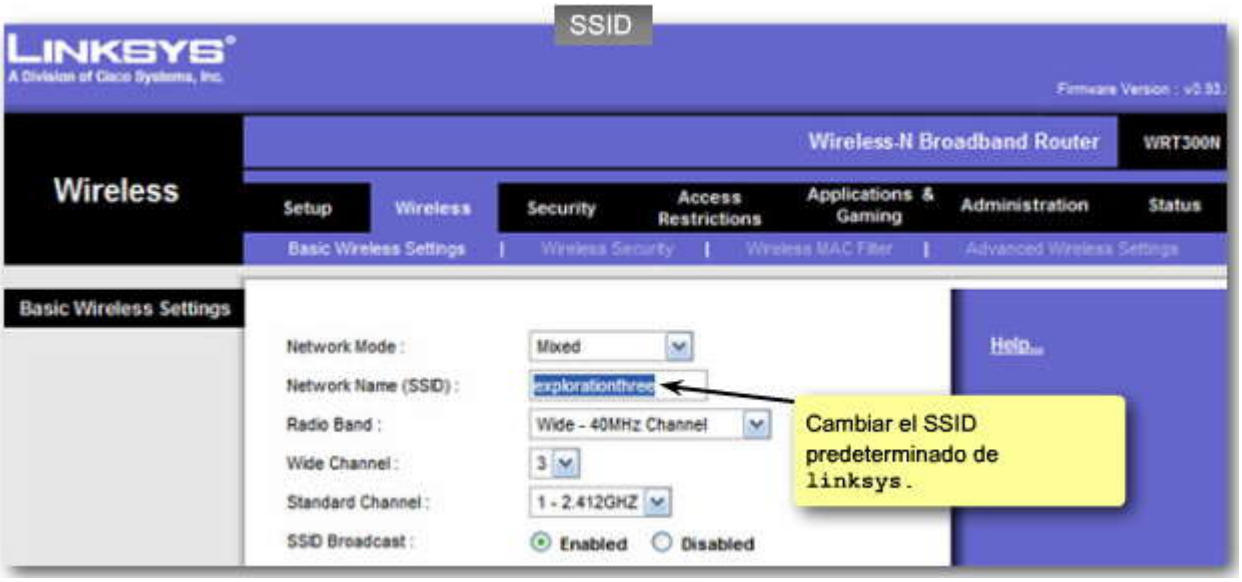
Broadcast SSID - Cuando los clientes inalámbricos inspeccionan el área local para buscar redes inalámbricas para asociarse, detectan el broadcast del SSID mediante el punto de acceso. Para transmitir el SSID, mantenga Habilitado, que esla configuración predeterminada. Si no quiere transmitir el SSID, seleccione Deshabilitado. Cuando termine de realizar los cambios a esta pantalla, haga clic en el botón Guardar cambios , o haga clic en el botón Cancelar cambios para deshacer sus cambios. Para mayor información, haga clic en Ayuda.

Banda de radio - Para un mejor rendimiento en una red que utiliza dispositivos Wireless-N, Wireless-G, y Wireless-B, mantenga el Auto predeterminado. Para dispositivos Wireless-N, únicamente, seleccione Ancho - Canal 40MHz. Para networking, únicamente, Wireless-G y Wireless-B, seleccione Estándar - Canal 20MHz.
Canal ancho. Si seleccionó Ancho - Canal 40MHz para la configuración de la Banda de radio, esta configuración está disponible para su canal Wireless-N principal. Seleccione cualquier canal del menú desplegable.
Canal estándar. Seleccione el canal para networking Wireless-N, Wireless-G y Wireless-B. Si seleccionó Ancho - canal 40MHz para la configuración de la Banda de radio, el canal estándar es un canal secundario para Wireless-N.

Configuración de los parámetros inalámbricos básicos

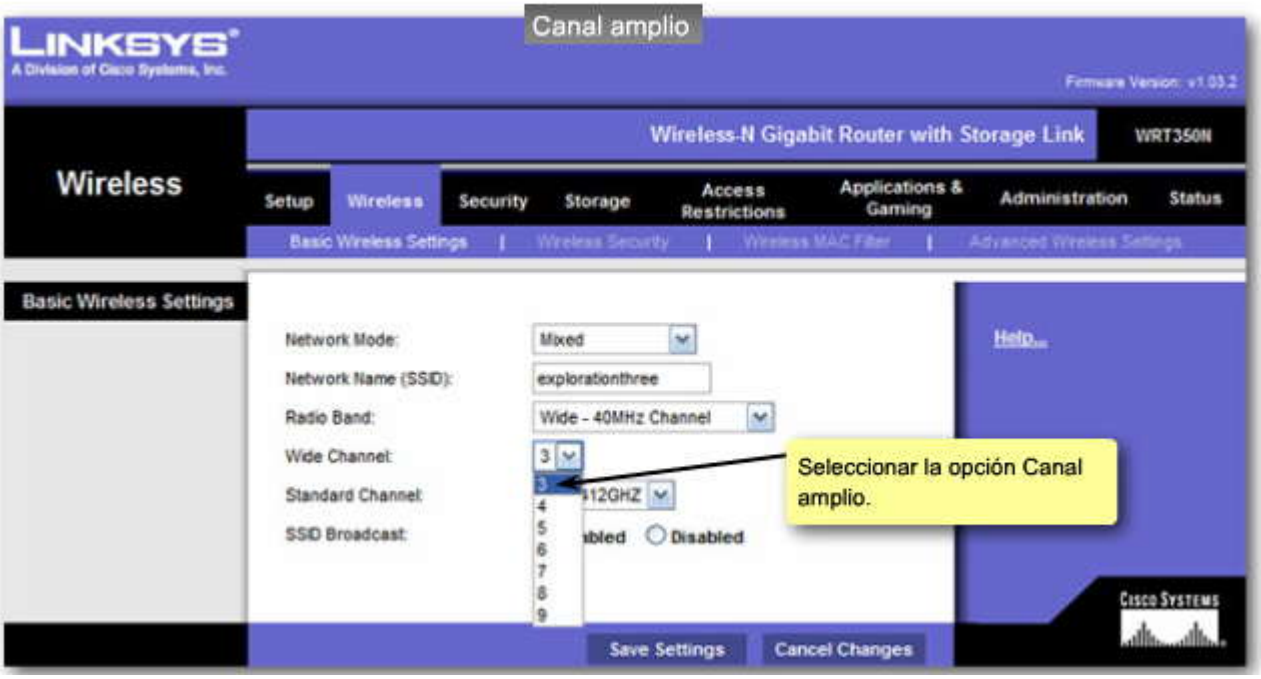


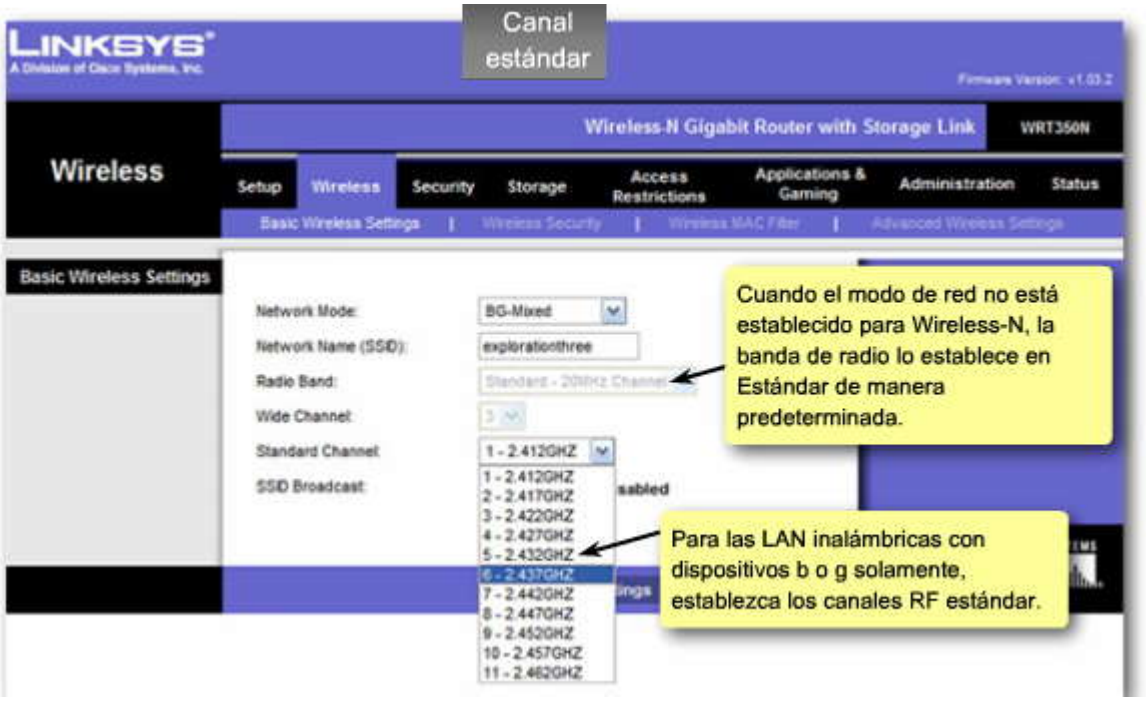
SSID



Banda de radio

Canal amplio





Configuración de seguridad

Haga clic en el botón Descripción general en la figura.

Esta opción configurará la seguridad de su red inalámbrica. Existen siete modos de seguridad inalámbrica que el WTR300N admite. Se listan aquí en el orden en que los ve en el GUI, desde el más débil al más fuerte, con excepción de la última opción, que está deshabilitada:

WEP
PSK-Personal, o WPA-Personal en v0.93.9 firmware o anterior
PSK2-Personal, o WPA2-Personal en v0.93.9 firmware o anterior
PSK-Empresa, o WPA-Empresa en v0.93.9 firmware o anterior
PSK2-Empresa, o WPA2-Empresa en v0.93.9 firmware o anterior
RADIUS
Deshabilitado

Cuando vea "Personal" en un modo de seguridad, no se está utilizando un servidor AAA. "Empresa" en d modo seguridad significa un servidor AAA y la utilización de una autenticación EAP.

Aprendió que el WEP es un modo de seguridad con fallas. PSK2, que es lo mismo que WPA2 o IEEE 802.11i, es la opción preferida para una mejor seguridad. Si WPA2 es la mejor, se preguntará por qué hay tantas otras opciones. La respuesta es que muchas LAN inalámbricas admiten dispositivos viejos. Dado que todos los dispositivos de clientes que se asocian a un punto de acceso deben ejecutar el mismo modo de seguridad que ejecuta el punto de acceso, éste debe estar configurado para admitir el dispositivo que ejecuta el modo de seguridad más débil. Todos los dispositivos de LAN inalámbricas fabricados luego de marzo de 2006 deben poder admitir WPA2 o, en el caso de los routers Linksys, PSK2; por lo que en el tiempo, a medida que se mejoren los dispositivos, será capaz de conmutar el modo de seguridad de su red a PSK2.

La opción RADIUS que está disponible para un router Linksys inalámbrico permite utilizar un servidor RADIUS en combinación con WEP.

Haga clic en los botones a lo largo de la parte inferior de la figura para ver el GUI para cada configuración.

Para configurar la seguridad, realice lo siguiente:

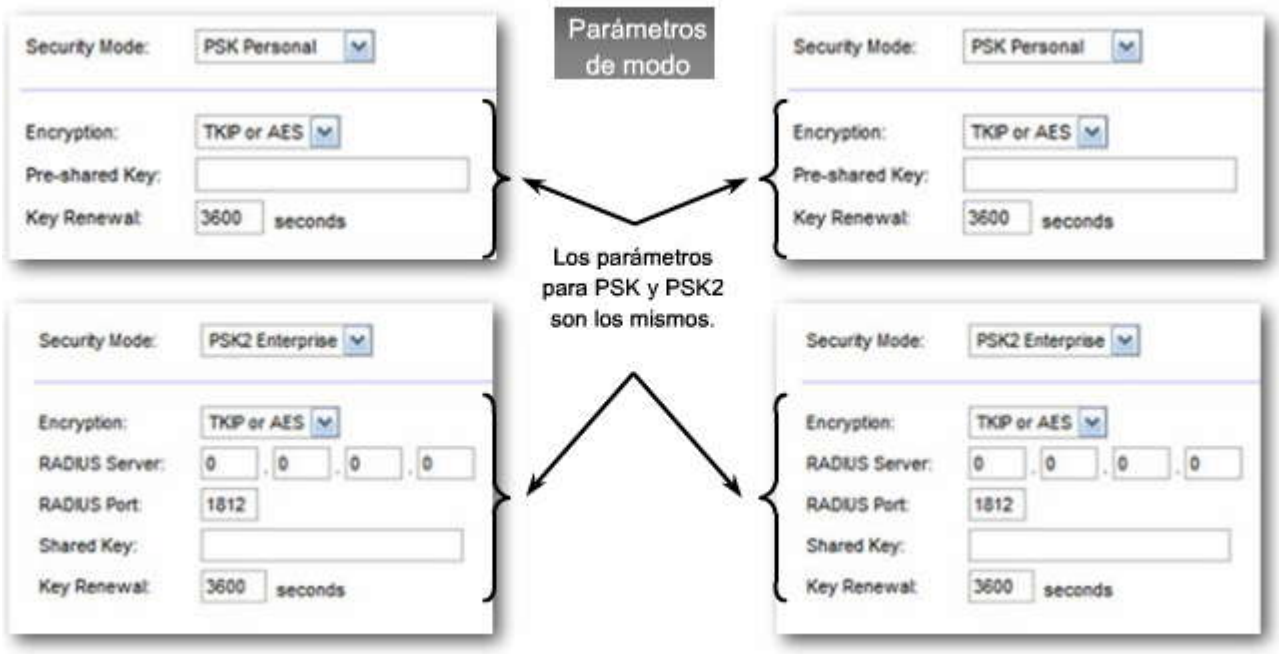
Modo seguridad - Seleccione el modo que quiera utilizar: PSK-Personal, PSK2-Personal, PSK-Empresa, PSK2-Empresa, RADIUS, o WEP.
Modo Parámetros - Cada uno de los modos PSK y PSK2 tiene parámetros que puede configurar. Si selecciona la versión de seguridad PSK2-Empresa, debe tener un servidor RADIUS adjunto a su punto de acceso. Si tiene esta configuración, necesita configurar el punto de acceso para que apunte al servidor RADIUS. Dirección IP del servidor RADIUS- Ingrese la dirección IP del servidor RADIUS. Puerto del servidor RADIUS - Ingrese el número de puerto utilizado por el servidor

RADIUS. De manera predeterminada, es 1812.

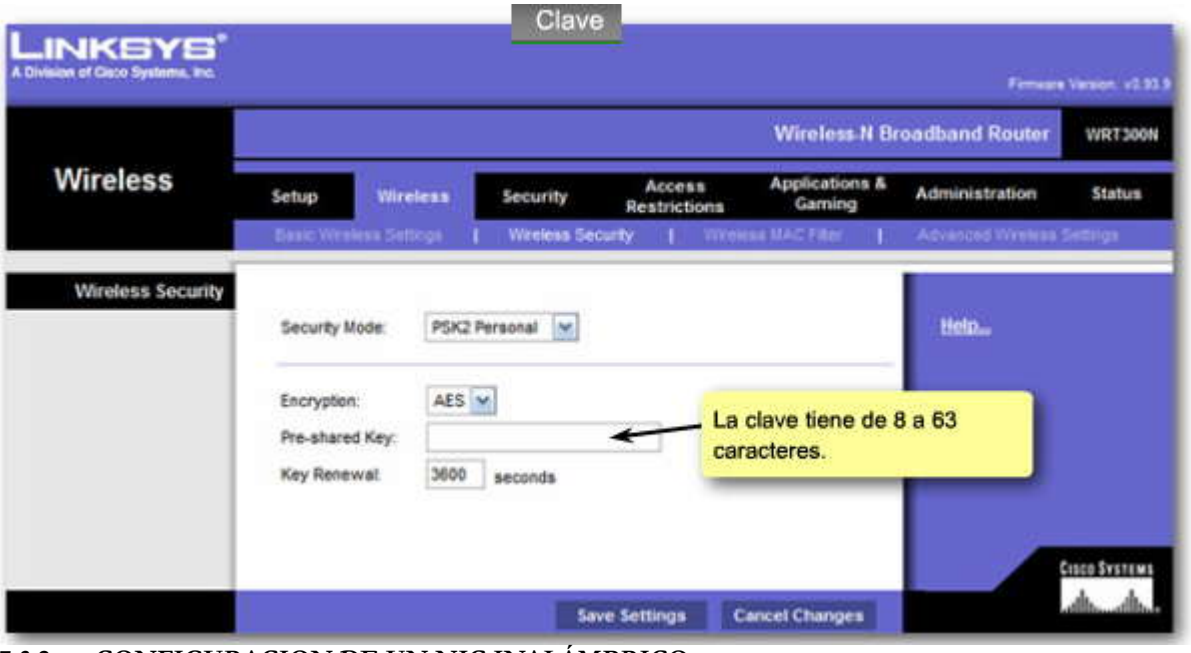
Encriptación - Seleccione el algoritmo que quiere utilizar, AES o TKIP. (AES es un método de encriptación más sólido que TKIP.)
Clave precompartida - Ingrese la clave compartida por el router y sus otros dispositivos de red. Debe tener entre 8 y 63 caracteres. Renovación de la clave - Ingrese el período de renovación de la clave, que le dirá al router con qué frecuencia debe cambiar las claves de encriptación.

Cuando termine de realizar los cambios a esta pantalla, haga clic en el botón Guardar cambios , o haga clic en el botón Cancelar cambios para deshacer sus cambios.

Configuración de seguridad



Los modos empresa no se configuran en este capítulo.



7.3.2 CONFIGURACION DE UN NIC INALÁMBRICO.-

Busque los SSID

Cuando se haya configurado un punto de acceso, necesitará configurar el NIC inalámbrico en un dispositivo cliente para permitirle conectase a la red inalámbrica. Deberá verificar, además, que el cliente inalámbrico se haya conectado exitosamente a la red inalámbrica correcta, especialmente porque pueden existir muchas WLAN disponibles a las cuales conectarse. También introducimos algunos pasos básicos de resolución de problemas e identificación de problemas comunes asociados con la conectividad WLAN.

Si su PC está equipada con un NIC inalámbrico, debe estar listo para buscar redes inalámbricas. Las PC que ejecutan Windows XP tienen monitor de redes inalámbricas y utilidades de cliente incorporados. Puede tener instalada una utilidad diferente en lugar de la versión de Microsoft Windows XP.

Los pasos que se mencionan a continuación indican cómo utilizar el dispositivo Ver redes inalámbricas en Microsoft Windows XP.

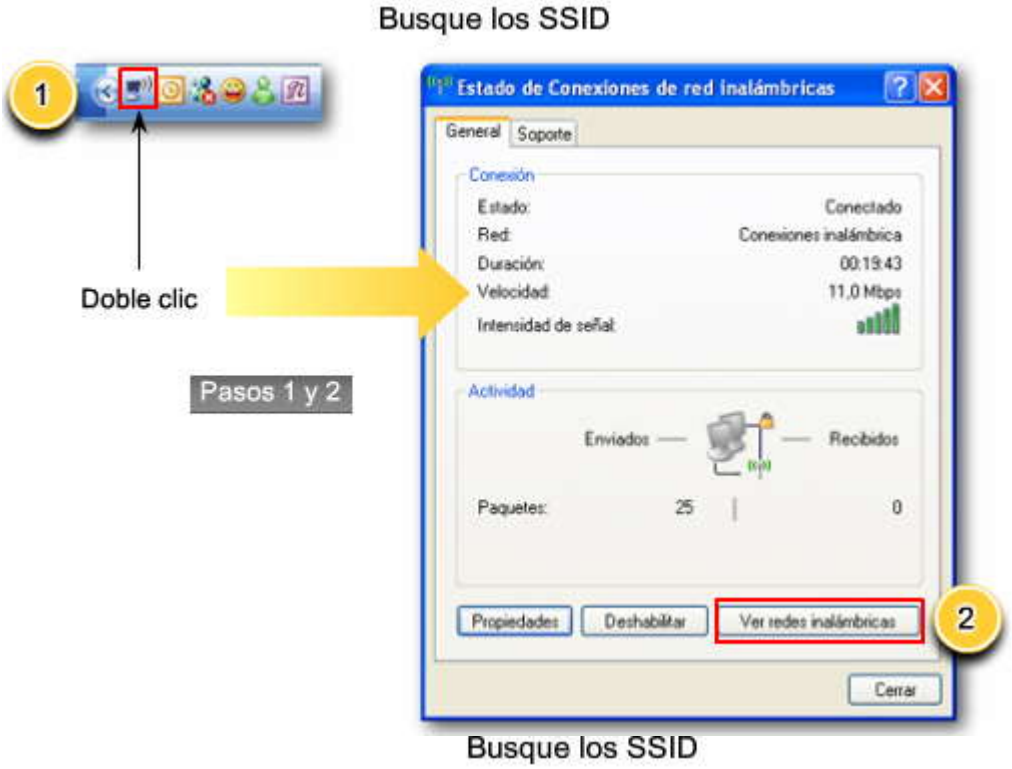
Haga clic en los pasos numerados en la figura para seguir el proceso.

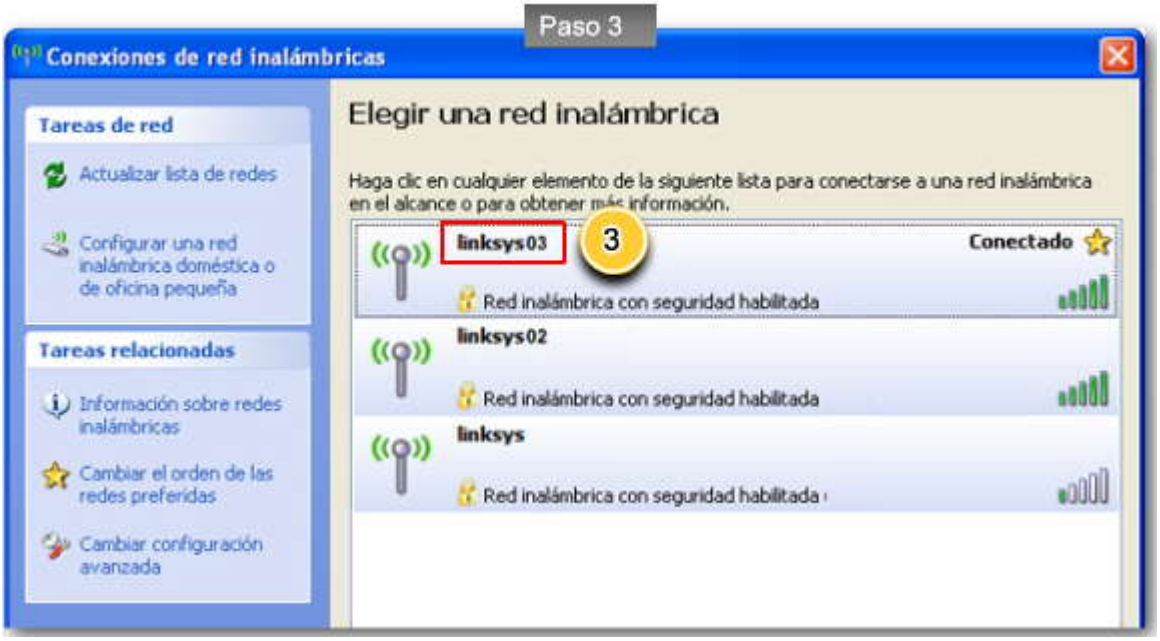
Paso 1. En la barra de herramientas de la bandeja del sistema de Microsoft Windows XP, ubique el ícono de conexión en red similar al que se muestra en la figura. Haga doble clic en el ícono para abrir el cuadro de diálogo de Conexiones de red.

Paso 2. Haga clic en el botón Ver redes inalámbricas en el cuadro de diálogo.

Paso 3. Observe las redes inalámbricas que puede detectar su NIC inalámbrico.

Si tiene una WLAN que no puede verse en la lista de redes, puede que tenga deshabilitada el broadcast SSID en el punto de acceso. Si este el caso, debe ingresar manualmente el SSID.





Seleccione el protocolo de seguridad inalámbrica

Luego de haber configurado su punto de acceso para autenticar clientes con un tipo de seguridad sólida, debe coincidir la configuración del cliente con los parámetros del punto de acceso. Los siguientes pasos describen cómo configurar los parámetros de seguridad de su red inalámbrica en el cliente:

Paso 1. Haga doble clic en el ícono de conexiones de red en la bandeja del sistema de Microsoft Windows XP.

Paso 2. Haga clic en el botón Propiedades en el cuadro de diálogo Estado de conexiones de red inalámbricas.

Paso 3. En el cuadro de diálogo Propiedades, haga clic en la etiqueta Redes inalámbricas.

Paso 4. En la etiqueta Redes inalámbricas, haga clic en el botón Agregar. Además, podrá guardar perfiles inalámbricos múltiples con diferentes parámetros de seguridad, lo que le permite conectarse rápidamente a las WLAN que pueda utilizar regularmente.

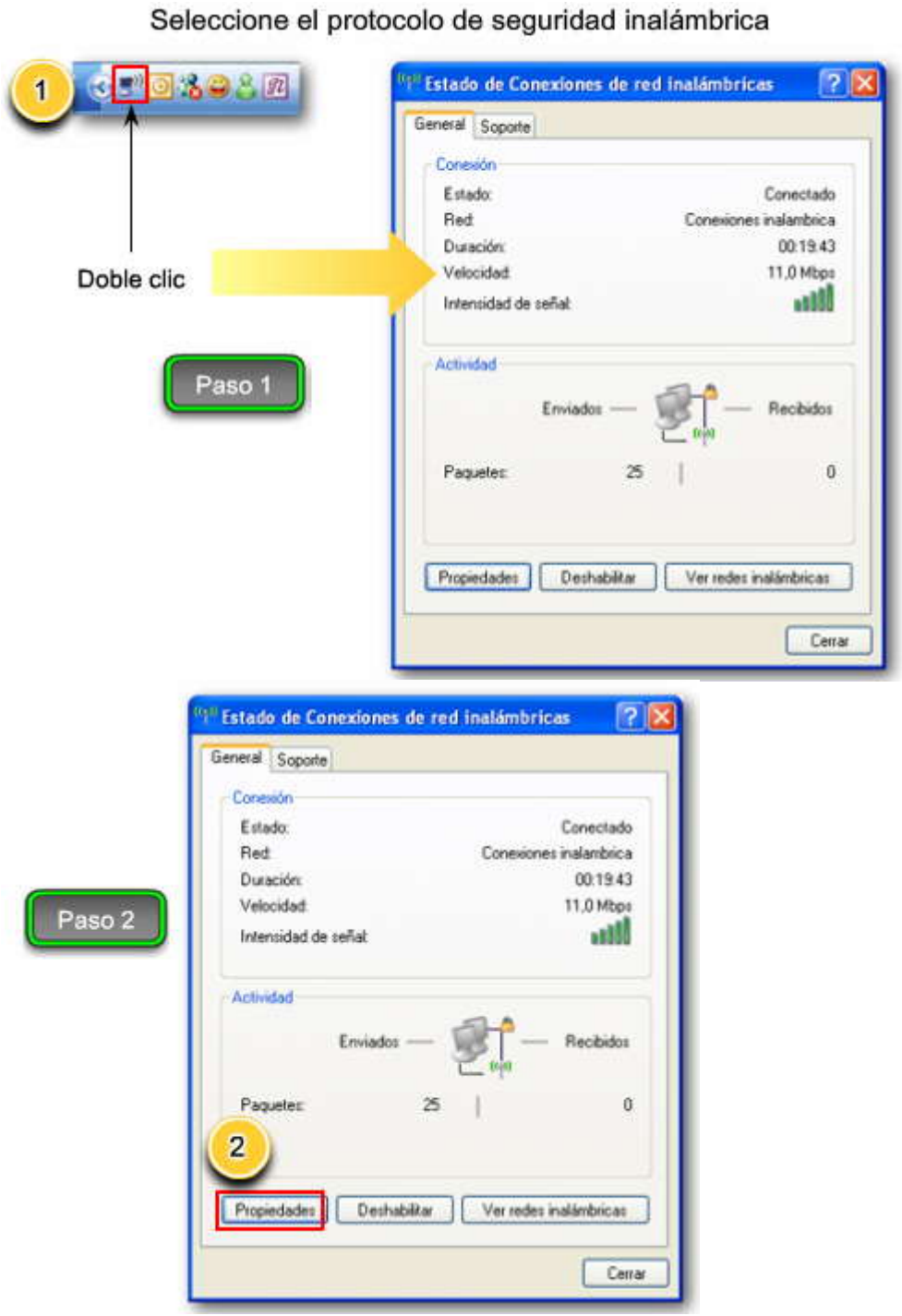
Paso 5. En el cuadro de diálogo de Propiedades de red inalámbrica, ingrese el SSID de la WLAN que quiere configurar.

Paso 6. En el cuadro de clave de red inalámbrica, seleccione su método de autenticación preferido del menú desplegable Autenticación de red. Se prefieren WPA2 y PSK2 por su solidez.

Paso 7. Seleccione el método de Encriptación de datos del menú desplegable. Recuerde que el AES es un código más sólido que TKIP, pero debe coincidir con la configuración de su punto de acceso aquí en su PC.

Luego de seleccionar el método de encriptación, ingrese y confirme la Clave de red. Nuevamente, éste es un valor que debe ingresar en el punto de acceso.

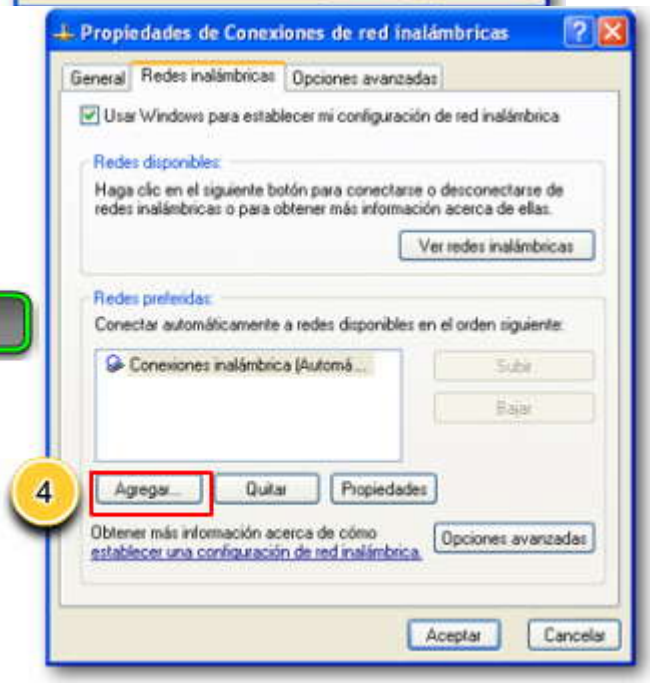
Paso 8. Haga clic en Aceptar.



Paso 3


3
Propiedades de Conexiones de red inalámbricas
General
Redes inalámbricas
Opciones avanzadas
Conectar usando:
Sweex Wireless Lan USB2.0 Adapter
Configurar...
Esta conexión utiliza los siguientes elementos:
Cliente para redes Microsoft
Compartir impresoras y archivos para redes Microsoft
Programador de paquetes QoS
Protocolo Internet (TCP/IP)
Instalar...
Desinstalar
Propiedades
Descripción
Permite a su equipo tener acceso a los recursos de una red Microsoft.
Mostrar icono en el área de notificación al conectarse
Notificarme cuando esta conexión tenga conectividad limitada o nula
Aceptar
Cancelar

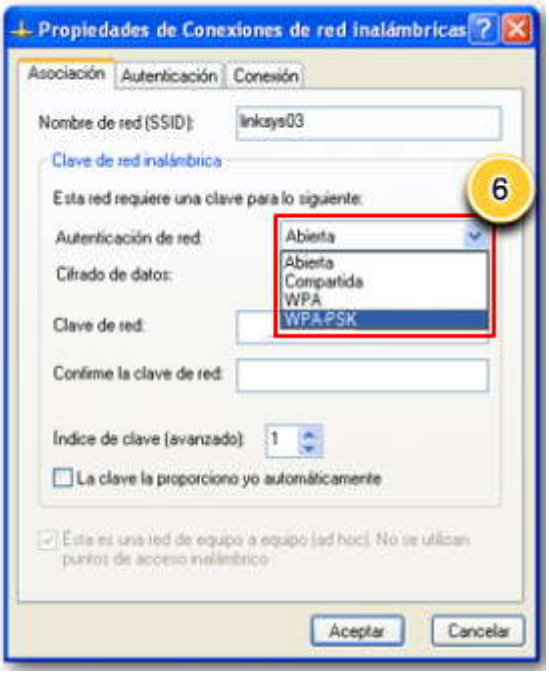
Paso 4


Propiedades de Conexiones de red inalámbricas
General
Redes inalámbricas
Opciones avanzadas
Usar Windows para establecer mi configuración de red inalámbrica
Redes disponibles:
Haga clic en el siguiente botón para conectarse o desconectarse de redes inalámbricas o para obtener más información acerca de ellas.
Ver redes inalámbricas
Redes preferidas:
Conectar automáticamente a redes disponibles en el orden siguiente:
Conexiones inalámbrica (Automá...
Subir
Bajar
4
Agregar...
Quitar
Propiedades
Obtener más información acerca de cómo establecer una configuración de red inalámbrica
Opciones avanzadas
Aceptar
Cancelar

Paso 5


Propiedades de Conexiones de red inalámbricas
Asociación
Autenticación
Conexión
5
Nombre de red (SSID):
Clave de red inalámbrica
Esta red requiere una clave para lo siguiente:
Autenticación de red:
Abierta
Cifrado de datos:
WEP
Clave de red:
Confirme la clave de red:
Índice de clave (avanzado):
1
La clave la proporciono yo automáticamente
Esta es una red de equipo a equipo (ad hoc). No se utilizan puntos de acceso inalámbrico
Aceptar
Cancelar

Paso 6

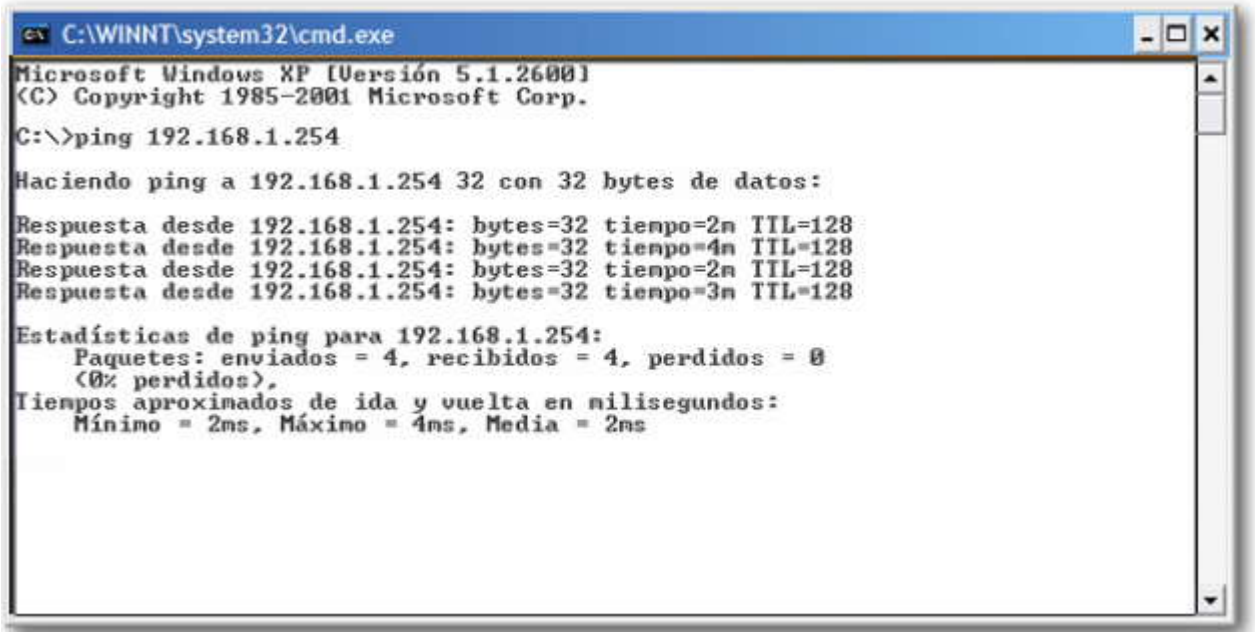

Propiedades de Conexiones de red inalámbricas
Asociación
Autenticación
Conexión
Nombre de red (SSID):
linksys03
Clave de red inalámbrica
6
Esta red requiere una clave para lo siguiente:
Autenticación de red:
Abierta
Cifrado de datos:
Abierta
Compartida
WPA
WPA-PSK
Clave de red:
Confirme la clave de red:
Índice de clave (avanzado):
1
La clave la proporciono yo automáticamente
Esta es una red de equipo a equipo (ad hoc). No se utilizan puntos de acceso inalámbrico
Aceptar
Cancelar

Verifique la conectividad a la LAN inalámbrica

Con las configuraciones establecidas para el punto de acceso y el cliente, el próximo paso es confirmar la conectividad. Esto se realiza enviando un ping a los dispositivos en la red.

Abra la ventana petición de entrada del comando DOS en la PC.

Trate de hacer ping a una dirección IP conocida para el dispositivo en la red. En la figura, la dirección IP es 192.168.1.254. El ping fue exitoso, lo que indica una conexión exitosa.



7.4 RESOLUCIÓN DE PROBLEMAS DE WLAN SIMPLES.-

7.4.1 RESOLVER EL RADIO DE PUNTO DE ACCESO Y TEMAS DE FIRMWARE.-

Un enfoque sistemático a la resolución de problemas de WLAN

La resolución de problemas de cualquier tipo de problema de red debe seguir un enfoque sistemático y trabajar la stack de TCP/IP desde la capa Física hasta la Capa de aplicación. Esto ayuda a eliminar cualquier inconveniente que pueda resolver usted mismo.

Haga clic en el botón Enfoque en la figura.

Ya debe estar familiarizado con los primeros tres pasos de un enfoque sistemático de la resolución de problemas, dado que trabajó con las LAN 802.3 Ethernet. Se repiten aquí en el contexto de la WLAN:

Paso 1 - Eliminar la PC del usuario como origen del problema.

Intente determinar la severidad del problema. Si no hay conectividad, compruebe lo siguiente:

Confirme la configuración de la red en la PC mediante el comando ipconfig. Verifique que la PC recibió una dirección IP a través de DHCP o está configurada con una dirección IP estática.
Confirme que el dispositivo puede conectarse a una red conectada por cable. Conecte el dispositivo a la LAN conectada por cable y envíe un ping a una dirección IP conocida.
Puede ser necesario intentar un NIC inalámbrico diferente. De ser necesario, recargue los controladores y firmware como sea apropiado para el dispositivo cliente.
Si el NIC inalámbrico del cliente funciona, compruebe el modo seguridad y la configuración de encriptación en el cliente. Si las configuraciones de seguridad no concuerdan, el cliente no podrá acceder a la WLAN.

Si la PC del usuario funciona pero lo hace con poco rendimiento, compruebe lo siguiente:

¿Cuán lejos está la PC del punto de acceso? ¿La PC está fuera del área de cobertura (BSA) planeada?
Compruebe la configuración de canal en el cliente. El software cliente debe detectar el canal apropiado siempre y cuando el SSID sea correcto.
Compruebe la presencia de otros dispositivos en el área que operen en la banda de 2,4 GHz. Ejemplos de otros dispositivos son los teléfonos inalámbricos, monitores de bebé, hornos de microondas, sistemas de seguridad inalámbricos y puntos de acceso no autorizados potenciales. Los datos de estos dispositivos pueden causar interferencia en la WLANy problemas de conexión intermitente entre un cliente y un punto de acceso.

Paso 2 - Confirme el estado físico de los dispositivos.

¿Todos los dispositivos están en su lugar? Considere un tema de seguridad física posible.
¿Hay energía en todos los dispositivos y están encendidos?

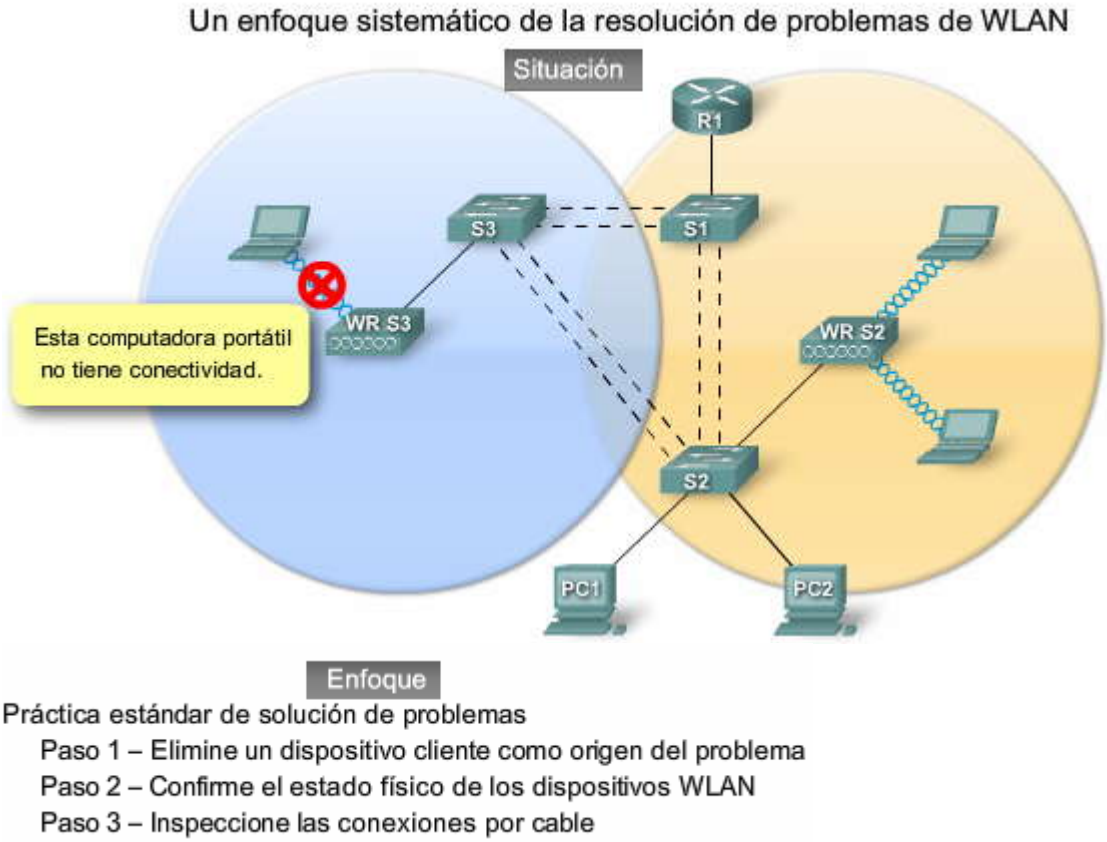
Paso 3 - Inspeccione los enlaces.

Inspeccione los enlaces entre los dispositivos conectados por cable buscando conectores dañados o que no funcionen o cables faltantes.
Si la planta física está ubicada correctamente, utilice la LAN conectada por cables para ver si puede hacer ping a los dispositivos, incluido el punto de acceso.

Si aún falla la conectividad en este punto, probablemente hay algo mal con el punto de acceso o su configuración.

Mientras soluciona problemas en una WLAN, se recomienda un proceso de eliminación que trabaje desde posibilidades físicas a las relacionadas con las aplicaciones. Cuando alcance el punto donde ya eliminó la PC del usuario como problema y también confirmó el estado físico de los dispositivos, comience a investigar el rendimiento del punto de acceso. Compruebe el estado de energía del punto de acceso.

Cuando se confirmó la configuración del punto de acceso, si la radio continúa fallando, intente conectarse a otro punto de acceso. Puede intentar instalar nuevos controladores de radio y firmware, como se explica a continuación.



7.4.2 CONFIGURACION DE CANAL INCORRECTA.-

Actualizar el Firmware del punto de acceso

Precaución: No actualice el firmware a menos que experimente problemas con el punto de acceso o que el nuevo firmware tenga una característica que quiera utilizar.

El firmware para un dispositivo Linksys, como el utilizado en las prácticas de laboratorio de este curso, se actualiza con una utilidad basada en la web. Siga las siguientes instrucciones:

Haga clic en el botón Descargar firmware en la figura.

Paso 1. Descargue el firmware desde la web. Para un Linksys WTR300N, diríjase a http://www.linksys.com.

Haga clic en el botón Seleccionar firmware para instalar, en la figura.

Paso 2. Extraiga el archivo del firmware en su computadora.

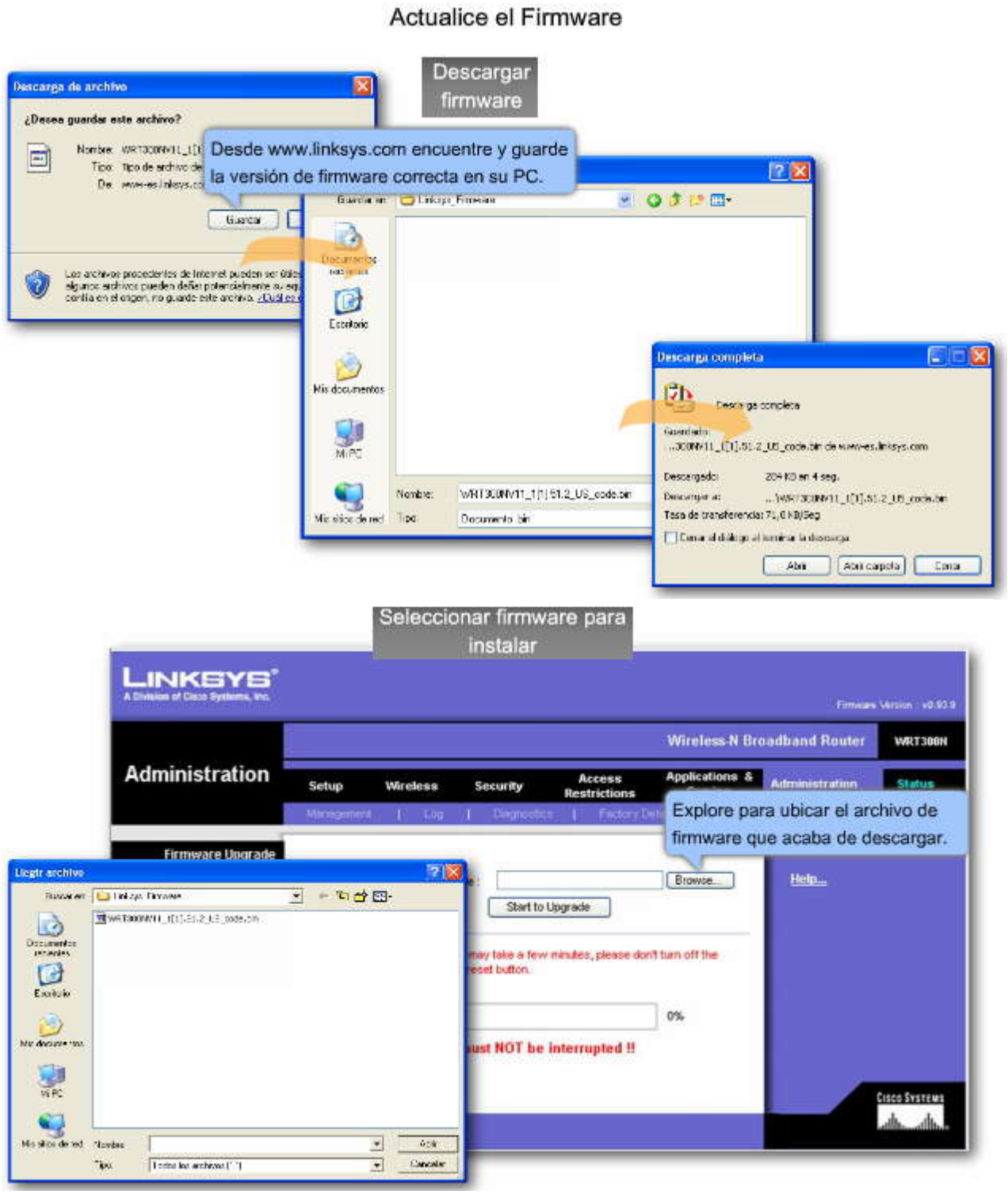
Paso 3. Abra la utilidad basada en la web y haga clic en la etiqueta Administración.

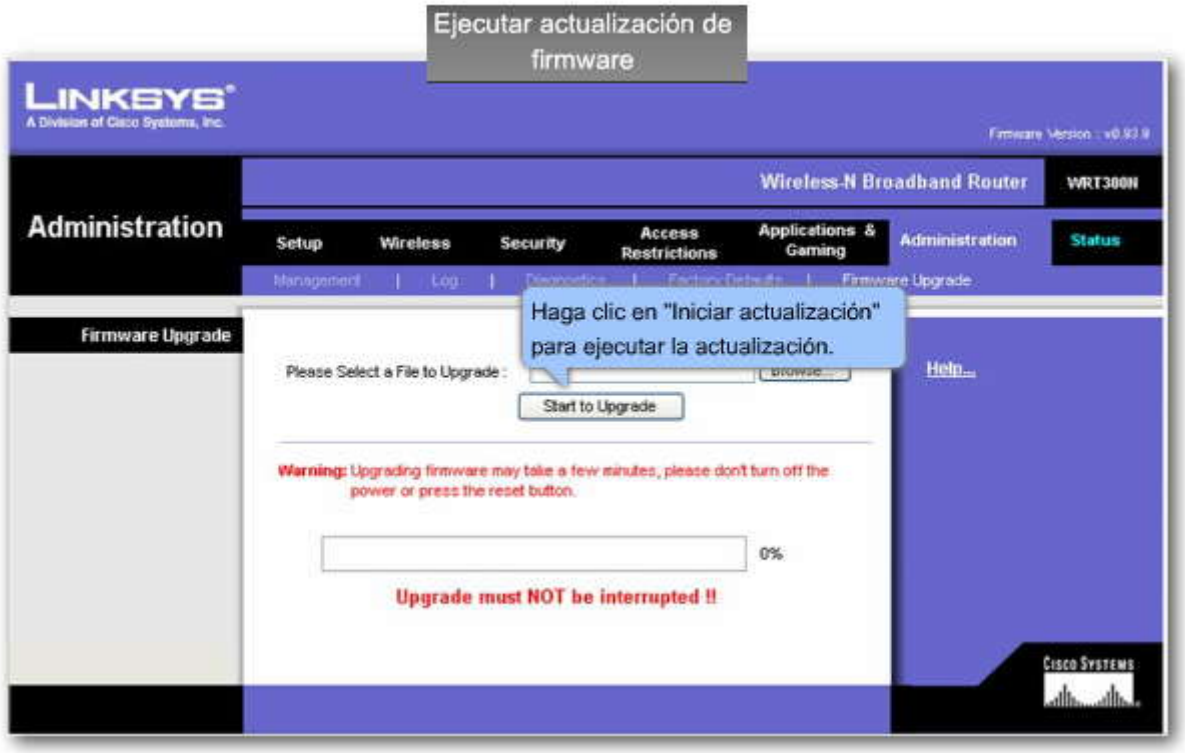
Paso 4. Seleccione la etiqueta Actualización de firmware.

Paso 5. Ingrese la ubicación del archivo de firmware o haga clic en el botón Explorar para encontrar el archivo.

Haga clic en el botón Ejecutar actualización de firmware en la figura.

Paso 6. Haga clic en el botón Iniciar actualización y siga las instrucciones.





Haga clic en el botón Problema en la figura.

Si los usuarios informan que existen problemas de conectividad en el área entre los puntos de acceso en un conjunto de servicios extendidos WLAN, puede haber un problema de configuración de canal.

Haga clic en el botón Razón en la figura.

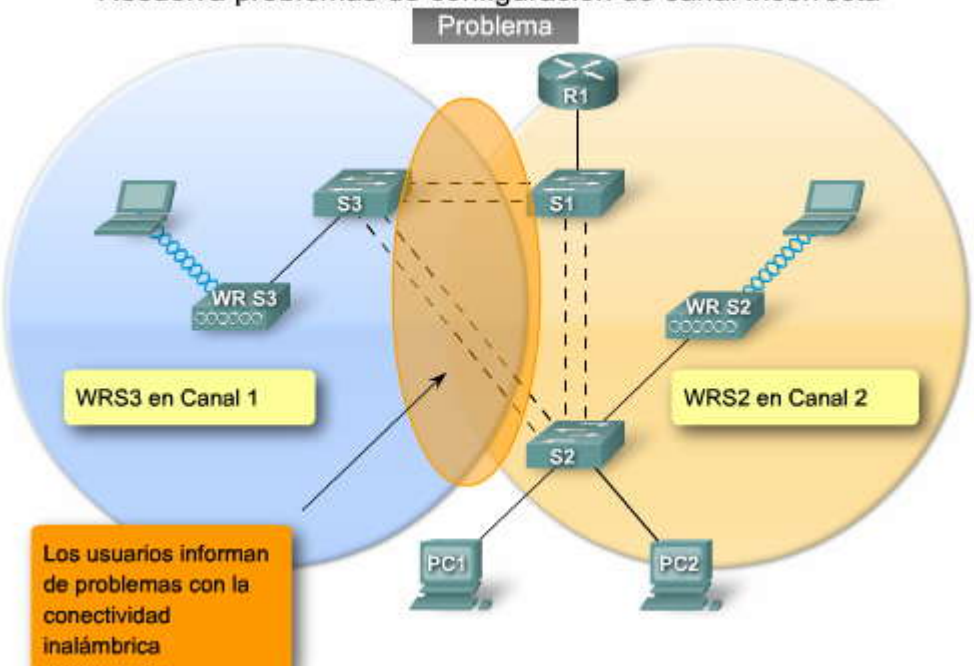
La mayoría de las WLAN operan en la banda de 2,4 GHz, que puede tener hasta 14 canales, cada uno ocupando un ancho de banda de 22 MHz. La energía no está distribuida en forma pareja en los 22 MHz, sino que el canal es más fuerte en su frecuencia central y la energía disminuye hacia los bordes del canal. El concepto de energía menguante en un canal se muestra en la línea curva utilizada para indicar cada canal. El punto alto en el medio de cada canal es el punto de mayor energía. La figura provee una representación gráfica de los canales en la banda de 2,4 GHz.

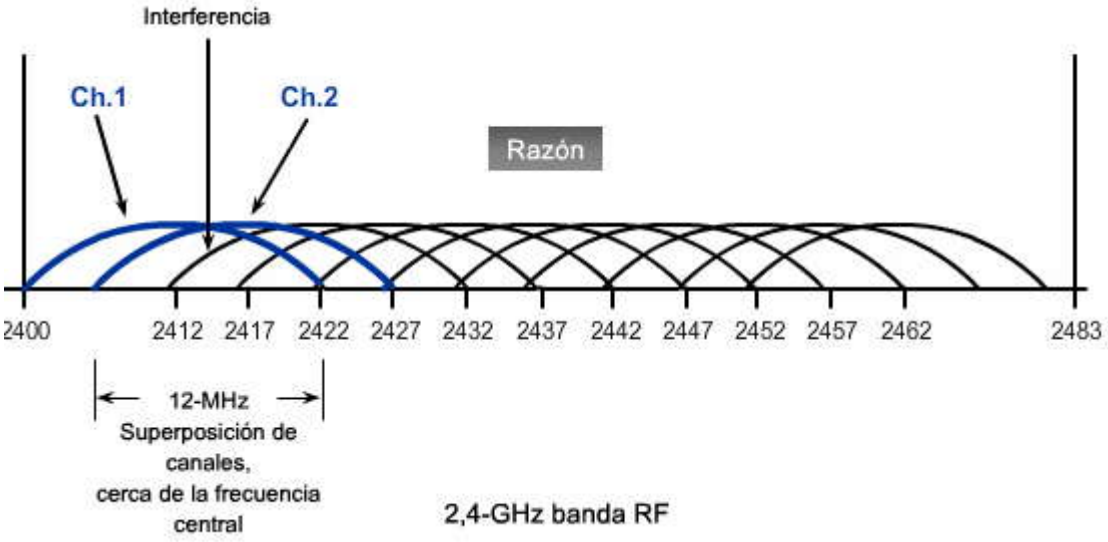
Una explicación completa de la manera en que la energía se dispersa a través de las frecuencias en un canal excede el alcance de este curso.

Haga clic en el botón Solución que se muestra en la figura.

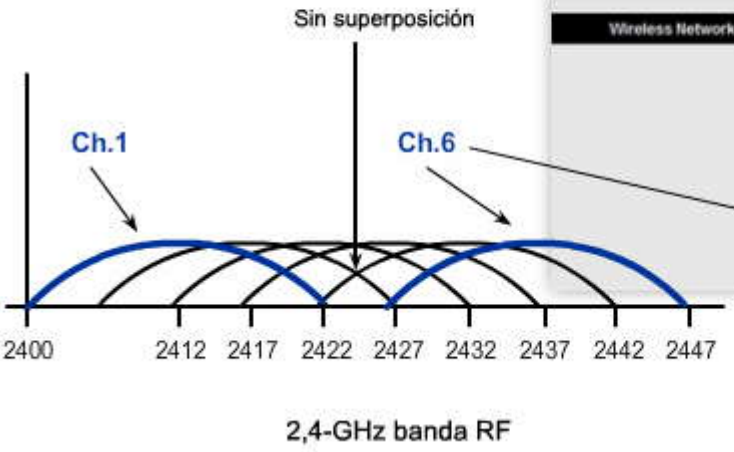
Puede producirse interferencia cuando hay una superposición de canales. Es peor si los canales se superponen cerca del centro de las frecuencias, pero, incluso si la superposición es menor, las señales interferirán una con la otra. Establezca los canales a intervalos de cinco canales, como canal 1, canal 6 y canal 11.

Resuelva problemas de configuración de canal incorrecta





Solución



Restablezca los puntos de acceso a canales no superpuestos

7.4.3 RESOLVER EL RADIO DE PUNTO DE ACCESO Y TEMAS DE FIRMWARE.-

Resolver la interferencia RF

La configuración incorrecta de canales es parte de un grupo de problemas mayores con la interferencia RF.Los administradores de WLAN pueden controlar la interferencia causada por la configuración de canal con buen planeamiento, incluida la distancia apropiada entre canales.

Haga clic en el botón Problema en la figura.

Se pueden hallar otros orígenes de interferencia RF alrededor del espacio de trabajo o en el hogar. Tal vez haya experimentado la interrupción tipo lluvia de una señal de televisión cuando alguien cercano al televisor utiliza una aspiradora. Dicha interferencia puede ser moderada con un buen planeamiento. Por ejemplo: planee ubicar los hornos de microondas lejos de los puntos de acceso y clientes potenciales. Desafortunadamente, el rango total de problemas de interferencia RF posible no puede planearse porque simplemente hay demasiadas posibilidades.

Haga clic en el botón Razón en la figura.

El problema con dispositivos como los teléfonos inalámbricos, monitores de bebé y hornos de microondas, es que no son parte de un BSS, por lo que no compiten por el canal, simplemente lo utilizan. ¿Cómo puede descubrir qué canales en un área son los más congestionados?

En un ambiente WLAN pequeño, intente configurar su punto de acceso WLAN al canal 1 u 11. Muchos artículos, como los teléfonos inalámbricos, operan en el canal 6.

Relevamientos del sitio

En ambientes más congestionados, se puede necesitar un relevamiento del sitio. A pesar de no conducir relevamientos del sitio como parte de este curso, debe saber que hay dos categorías de relevamientos del sitio: manual y asistida por utilidades.

Los relevamientos manuales del sitio pueden incluir evaluación del sitio seguido por un relevamiento del sitio más profundo asistido por utilidades. Una evaluación de sitio involucra la inspección del área con el objetivo de identificar temas potenciales que pueden tener un impacto en la red. Específicamente, busque la presencia de WLAN múltiples, estructuras de edificio únicas, como pisos abiertos y atrios, y grandes variaciones de utilización de cliente, como aquellas causadas por las diferencias en niveles de turnos de personal de día y de noche.

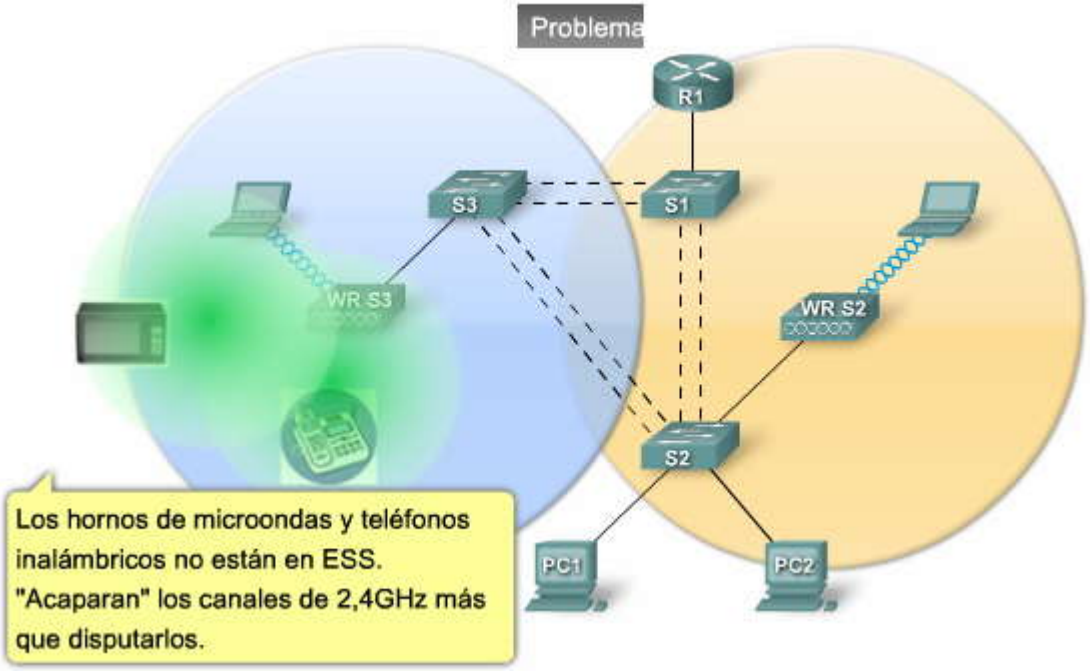
Haga clic en el botón Solución que se muestra en la figura.

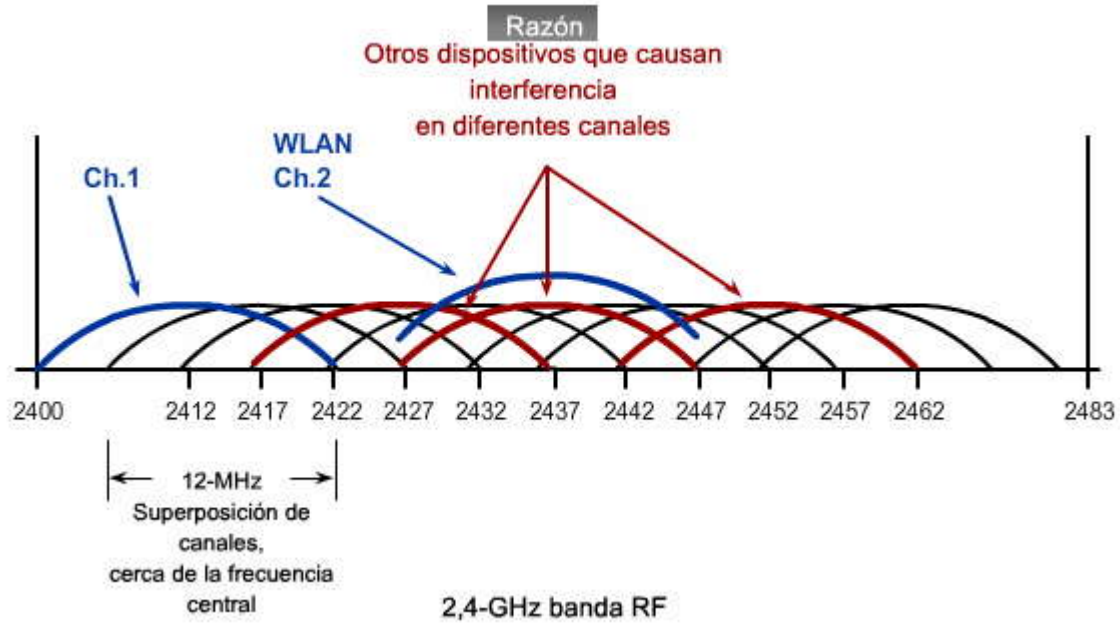
Hay muchos enfoques para realizar los relevamientos del sitio asistidos por utilidades. Si no tiene acceso a las herramientas dedicadas al relevamiento del sitio, como Airmagnet, puede montar puntos de acceso en trípodes y establecerlos en ubicaciones que cree son apropiadas y de acuerdo con el plan proyectado del sitio. Con los puntos de acceso montados, puede moverlos en las instalaciones mediante un medidor de relevamientos del sitio en la utilidad WLAN de cliente de su PC, como se muestra en la captura de pantalla 1 en la figura.

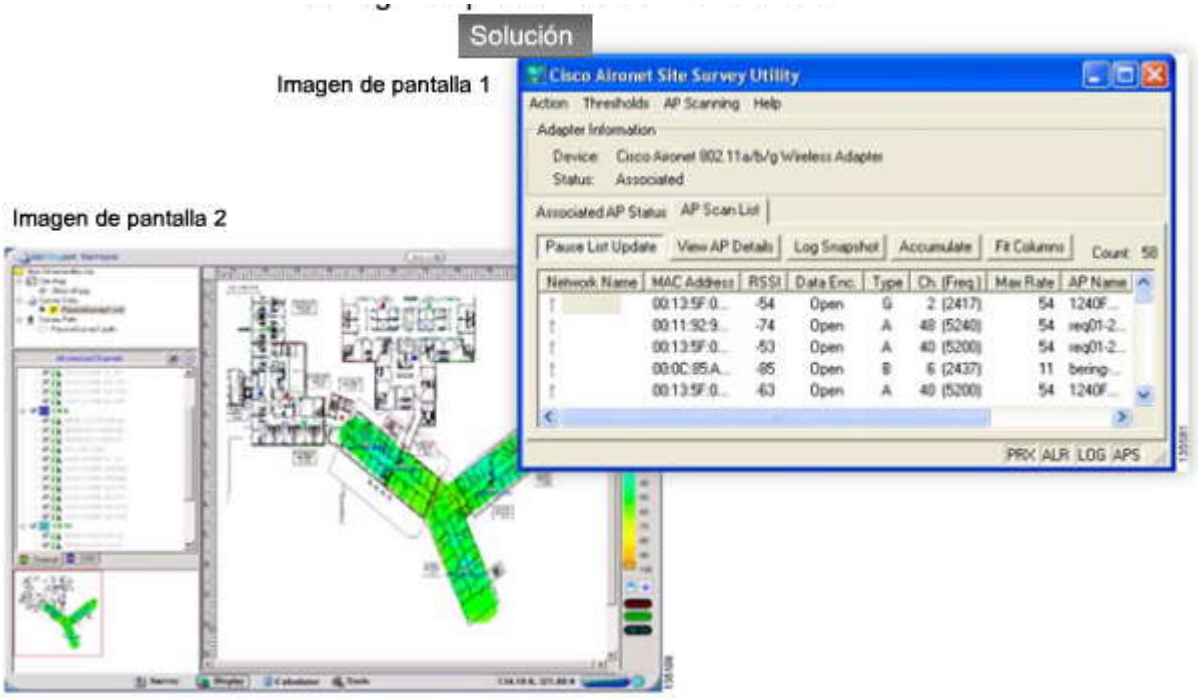
Alternativamente, existen herramientas sofisticadas que le permiten entrar a un plano de planta de las instalaciones. Puede entonces iniciar un registro de las características RF del sitio, que luego se muestran en el plano de planta, a medida que se mueve a través de las instalaciones con su computadora portátil inalámbrica. Un ejemplo del resultado de un relevamiento del sitio Airmagnet se muestra en la captura de pantalla 2 en la figura.

Parte de la ventaja de realizar relevamientos del sitio asistidos por utilidades es que la actividad RF en los diferentes canales de las bandas sin licencia (900 MHz, 2,4 GHz, y 5 GHz) se documenta y luego el usuario puede elegir los canales para su WLAN, o al menos identificar las áreas de actividad RF alta y tomar las precauciones necesarias.

Corregir los problemas de interferencia RF







7.4.4 RESOLVER EL RADIO DE PUNTO DE ACCESO Y TEMAS DE FIRMWARE.-

Identificar problemas de mala ubicación de puntos de acceso

En este tema, aprenderá cómo identificar cuándo un punto de acceso está mal ubicado y cómo ubicarlo correctamente en una empresa pequeña o mediana.

Haga clic en el botón Problema en la figura.

Pudo haber experimentado una WLAN que simplemente no parecía funcionar como debería. Tal vez pierda constantemente la asociación con un punto de acceso, o su transferencia de datos es mucho menor a lo que debería ser. Incluso puede haber realizado un paseo rápido por las instalaciones para confirmar que realmente puede ver los puntos de acceso. Una vez confirmado que están allí, se pregunta por qué el servicio sigue siendo pobre.

Haga clic en el botón Razón en la figura.

Existen dos problemas importantes de implementación que pueden producirsecon la ubicación de los puntos de acceso:

La distancia que separa los puntos de acceso es demasiada como para permitir la superposición de cobertura.
La orientación de la antena de los puntos de acceso en los vestíbulos y esquinas disminuye la cobertura

Haga clic en el botón Solución que se muestra en la figura.

Ubique el punto de acceso de la siguiente manera:

Confirme la configuración de energía y rangos operacionales de los puntos de acceso y ubíquelos para un mínimo de 10 a 15% de superposición de celdas, como aprendió anteriormente en este capítulo.

Cambie la orientación y posición de los puntos de acceso:

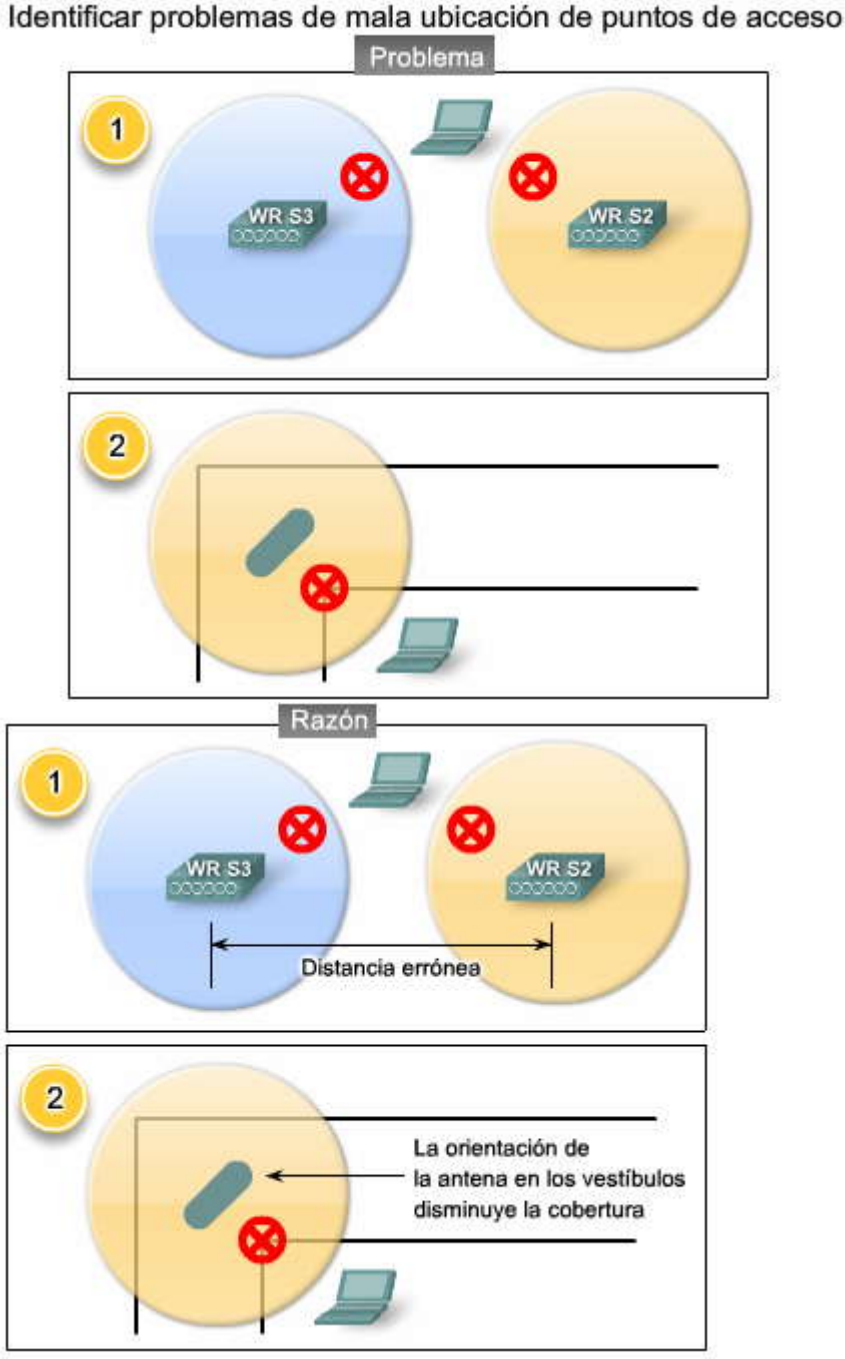
Posicione los puntos de acceso sobre las obstrucciones.
Posicione los puntos de acceso en forma vertical, cerca del techo en el centro de cada área de cobertura, de ser posible.
Posicione los puntos de acceso en las ubicaciones donde se espera que estén los usuarios. Por ejemplo: las salas grandes son una mejor ubicación para los puntos de acceso que un vestíbulo.

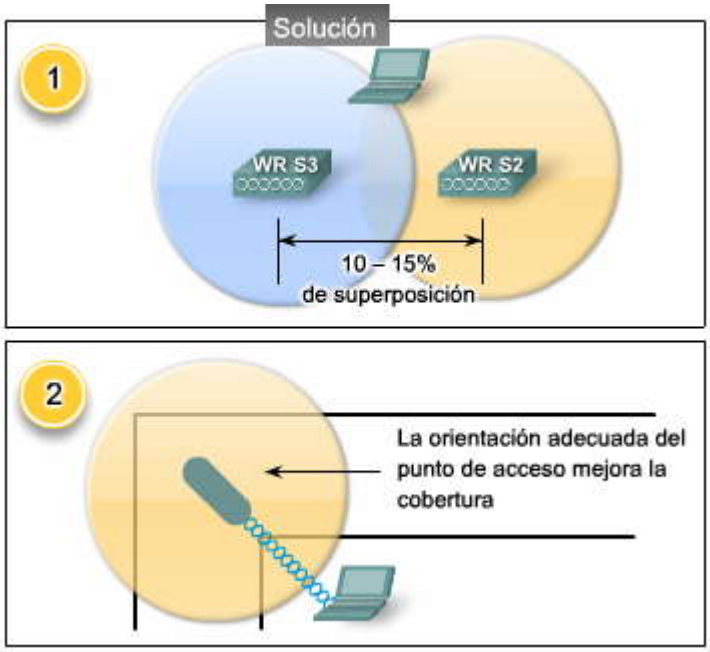
La figura explora estos temas en la secuencia problema, motivo y solución.

Haga clic en los botones para avanzar a través de la gráfica.

Algunos detalles específicos adicionales concernientes a la ubicación del punto de acceso y de la antena son los siguientes:

Asegúrese de que los puntos de acceso no estén montados a menos de 7,9 pulgadas (20 cm) del cuerpo de cualquier persona.
No monte el punto de acceso dentro de un radio de 3 pies (91,4 cm) de obstrucciones metálicas.
Instale el punto de acceso lejos de hornos de microondas. Los hornos de microondas operan en la misma frecuencia que los puntos de acceso y pueden causar interferencia en la señal.
Siempre monte el punto de acceso de manera vertical (parado o colgando).
No monte el punto de acceso fuera de los edificios.
No monte el punto de acceso en las paredes perimetrales de edificios, a menos que se desee cobertura fuera de éste.
Cuando monte un punto de acceso en la esquina derecha de un vestíbulo con intersección a la derecha, hágalo a un ángulo de 45° hacia ambos vestíbulos. Las antenas internas de los puntos de acceso no son omnidireccionales y cubren un área mayor si se los monta de esa manera.





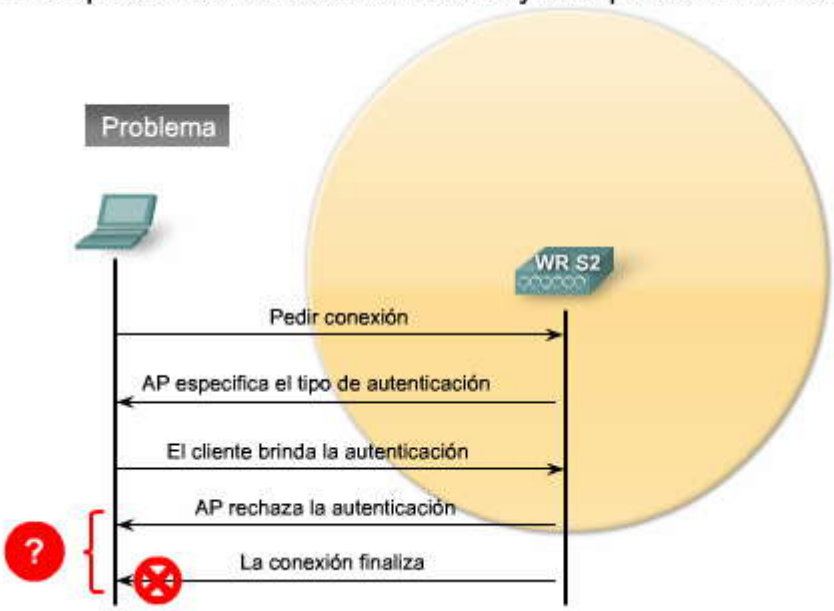
7.4.5 PROBLEMAS CON LA AUTENTIFICACION Y ENCRIPTACION.-

Los problemas de autenticación y encriptación de la WLAN que más probablemente vaya a enfrentar y que podrá resolver son causados por configuraciones de cliente incorrectas. Si un punto de acceso espera un tipo de encriptación y el cliente ofrece uno diferente, el proceso de autenticación falla.

Los problemas de encriptación que involucran la creación de claves dinámicas y las conversaciones entre un servidor de autenticación, como un servidor RADIUS y un cliente a través de un punto de acceso, están fuera del alcance de este curso.

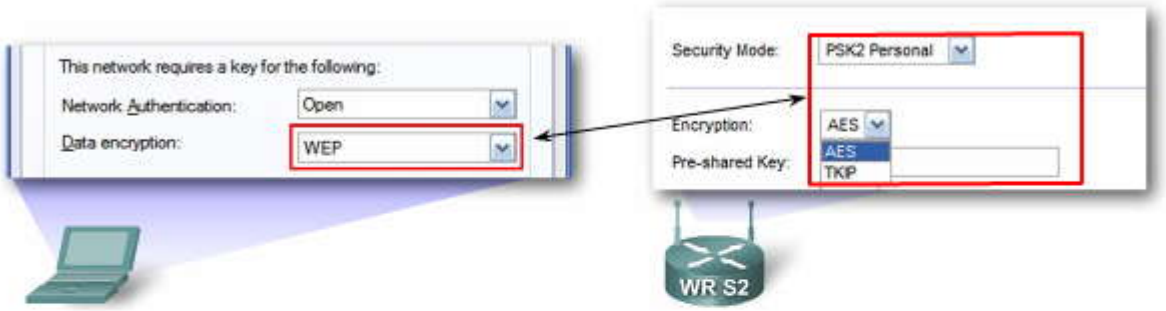
Recuerde que todos los dispositivos que se conectan a un punto de acceso deben utilizar el mismo tipo de seguridad que el configurado en el punto de acceso. Por lo tanto, si un punto de acceso está configurado para WEP, tanto el tipo de encriptación (WEP) como la clave compartida deben coincidir entre el cliente y el punto de acceso. Si se utiliza WPA, el algoritmo de encriptación es TKIP. De manera similar, si se utiliza WPA2 u 802.11i, se requiere AES como algoritmo de encriptación.

Resolución de problemas con la autenticación y encriptación LAN inalámbrica

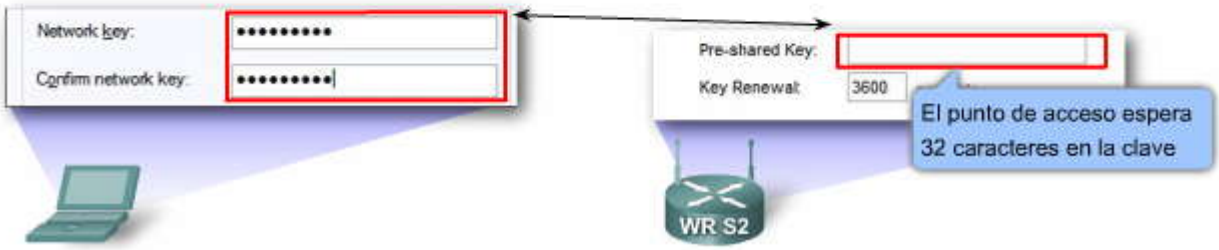


Motivo

1. Tipo de encriptación incorrecta establecida en el cliente



2. Credenciales incorrectas suministradas



3. Existe otro problema que no es la encriptación

Solución

1. Tipo de encriptación incorrecta establecida en el cliente: hacer coincidir el tipo de encriptación

2. Credenciales incorrectas suministradas: hacer coincidir las credenciales entre el cliente y el punto de acceso

3. Existe otro problema que no es la encriptación: continúe con la resolución de problemas