

PREGUNTAS OFICIALES EXAMEN ESCRITO CCNA 2

Tema 1:

1. ¿Qué es un router? Funcionamiento de un router. Capas.

El router es una computadora diseñada para fines especiales que desempeña un rol clave en el funcionamiento de cualquier red de datos.

La principal responsabilidad de un router es dirigir los paquetes destinados a redes locales y remotas mediante:

- La determinación del mejor camino para enviar paquetes
- El reenvío de los paquetes a su destino

El router usa su tabla de enrutamiento para determinar el mejor camino para reenviar el paquete. Cuando el router recibe un paquete, examina su dirección IP de destino y busca la mejor coincidencia con una dirección de red en la tabla de enrutamiento del router. La tabla de enrutamiento también incluye la interfaz que se utilizará para reenviar el paquete. Cuando se encuentra una coincidencia, el router encapsula el paquete IP en la trama de enlace de datos de la interfaz de salida. Luego, el paquete se reenvía hacia su destino.

Es muy probable que un router reciba un paquete encapsulado en un tipo de trama de enlace de datos, como una trama de Ethernet, y al reenviar el paquete, el router lo encapsulará en otro tipo de trama de enlace de datos, como el Protocolo punto a punto (PPP, Point-to-Point Protocol). La encapsulación de enlace de datos depende del tipo de interfaz del router y del tipo de medio al que se conecta. Las diferentes tecnologías de enlace de datos a las que se conecta un router pueden incluir tecnologías LAN, como Ethernet, y conexiones seriales WAN, como la conexión T1 que usa PPP, Frame Relay y Modo de transferencia asíncrona (ATM).

Los routers usan protocolos de rutas estáticas y de enrutamiento dinámico para detectar redes remotas y crear sus tablas de enrutamiento. Estas rutas y protocolos representan el enfoque principal del curso y se analizarán en detalle en los siguientes capítulos junto con el proceso que usan los routers al buscar en sus tablas de enrutamiento y al reenviar los paquetes.

2. Componentes de un router.

Componentes del router y sus funciones:

Al igual que una PC, un router también incluye:

- Unidad Central de Proceso (CPU)
- Memoria de acceso aleatorio (RAM)
- Memoria de sólo lectura (ROM)

Desplácese con el mouse sobre los componentes en la figura para ver una breve descripción de cada uno.

CPU

La CPU ejecuta las instrucciones del sistema operativo, como la inicialización del sistema y las funciones de enrutamiento y conmutación.

RAM

La RAM almacena las instrucciones y los datos necesarios que la CPU debe ejecutar. La RAM se usa para almacenar estos componentes:

- Sistema operativo: el sistema operativo Internetwork (IOS, Internetwork Operating System) de Cisco se copia a la RAM durante el arranque.
- Archivo de configuración en ejecución: éste es el archivo de configuración que almacena los comandos de configuración que el IOS del router utiliza actualmente. Salvo algunas excepciones, todos los comandos configurados en el router se almacenan en el archivo de configuración en ejecución, conocido como running-config.
- Tabla de enrutamiento IP: este archivo almacena información sobre redes remotas y conectadas directamente. Se usa para determinar el mejor camino para reenviar el paquete.
- Caché ARP: este caché contiene la dirección IPv4 para el mapeo de direcciones MAC, similar al caché ARP en una PC. El caché ARP se usa en routers que tienen interfaces LAN como las interfaces Ethernet.

- **Búfer de paquete:** los paquetes se almacenan temporalmente en un búfer cuando se reciben en una interfaz o antes de salir de ésta.

La RAM es una memoria volátil que pierde el contenido cuando se apaga o reinicia el router. Sin embargo, el router también contiene áreas de almacenamiento permanentes, como la ROM, la flash y la NVRAM.

ROM

La ROM es una forma de almacenamiento permanente. Los dispositivos Cisco usan la memoria ROM para almacenar:

- Instrucciones bootstrap
- Software básico de diagnóstico
- Versión más básica del IOS

La ROM usa firmware, un software incorporado dentro del circuito integrado. El firmware incluye el software que normalmente no necesita modificarse ni actualizarse, como las instrucciones de inicio. Muchas de estas funciones, incluso el software del monitor de la ROM, se analizarán en otro curso. Esta memoria no pierde sus contenidos cuando se apaga o reinicia el router.

Memoria Flash

La memoria Flash es una memoria no volátil de la computadora que se puede almacenar y borrar de manera eléctrica. La memoria flash se usa como almacenamiento permanente para el sistema operativo, Cisco IOS. En la mayoría de los routers Cisco, el IOS se almacena en forma permanente en la memoria flash y se copia en la RAM durante el proceso de arranque, donde entonces es ejecutado por la CPU. Algunos modelos anteriores de routers Cisco ejecutan el IOS directamente desde la memoria flash. La memoria flash consiste en tarjetas SIMM o PCMCIA, que pueden actualizarse para aumentar la cantidad de memoria flash.

Esta memoria no pierde sus contenidos cuando se apaga o reinicia el router.

NVRAM

La NVRAM (RAM no volátil) no pierde su información cuando se desconecta la alimentación eléctrica. Esto se opone a las formas más comunes de RAM, como la DRAM, que requiere alimentación eléctrica continua para mantener su información. El Cisco IOS usa la NVRAM como almacenamiento permanente para el archivo de configuración de inicio (startup-config). Todos los cambios de configuración se almacenan en el archivo running-config en la RAM, y salvo pocas excepciones, son implementados inmediatamente por el IOS. Para guardar esos cambios en caso de que se apague o reinicie el router, el running-config debe estar copiado en la NVRAM, donde se almacena como el archivo startup-config. Retiene sus contenidos incluso cuando el router se recarga o se apaga.

Las memorias ROM, RAM, NVRAM y flash se analizan en la siguiente sección que presenta el IOS y el proceso de arranque. También se analizan con más profundidad en un curso posterior relacionado con la administración del IOS.

Para un profesional de sistemas de redes es más importante comprender la función de los principales componentes internos de un router que la ubicación exacta de esos componentes dentro de un router específico. La arquitectura física interna variará de un modelo a otro.

3. Proceso de arranque de un router. Esquema.

Proceso de arranque:

El proceso de arranque está conformado por cuatro etapas principales:

1. Ejecución del POST (Autodiagnóstico al encender)
2. Carga del programa bootstrap
3. Ubicación y carga del software Cisco IOS
4. Ubicación y carga del archivo de configuración de inicio o ingreso al modo setup

1. Ejecución del POST (Autodiagnóstico al encender)

La prueba de Autodiagnóstico al encender (POST) es un proceso común que ocurre en casi todas las computadoras durante el arranque. El proceso de POST se utiliza para probar el hardware del router. Cuando se enciende el router, el software en el chip de la ROM ejecuta el POST. Durante esta autocomprobación, el router ejecuta diagnósticos desde la ROM a varios componentes de hardware, entre ellos la CPU, la RAM y la NVRAM. Una vez finalizado el POST, el router ejecuta el programa bootstrap.

2. Carga del programa bootstrap

Después del POST, el programa bootstrap se copia de la ROM a la RAM. Una vez en la RAM, la CPU ejecuta las instrucciones del programa bootstrap. La tarea principal del programa bootstrap es ubicar al Cisco IOS y cargarlo en la RAM.

Nota: en este momento, si existe una conexión de consola al router, comenzarán a aparecer los resultados en la pantalla.

3. Ubicación y carga del Cisco IOS

Ubicación del software Cisco IOS. El IOS normalmente se almacena en la memoria flash, pero también puede almacenarse en otros lugares como un servidor de protocolo de transferencia de archivos trivial (TFTP, Trivial File Transfer Protocol).

Si no se puede localizar una imagen completa del IOS, se copia una versión más básica del IOS desde la ROM a la RAM. Esta versión del IOS se usa para ayudar a diagnosticar cualquier problema y puede usarse para cargar una versión completa del IOS en la RAM.

Carga del IOS. Algunos de los routers Cisco más antiguos ejecutan el IOS directamente desde la memoria flash, pero los modelos actuales copian el IOS a la RAM para que la CPU lo ejecute.

4. Ubicación y carga del archivo de configuración

Ubicación del archivo de configuración de inicio. Después de cargar el IOS, el programa bootstrap busca en la NVRAM el archivo de configuración de inicio, conocido como startup-config. El archivo contiene los parámetros y comandos de configuración previamente guardados, entre ellos:

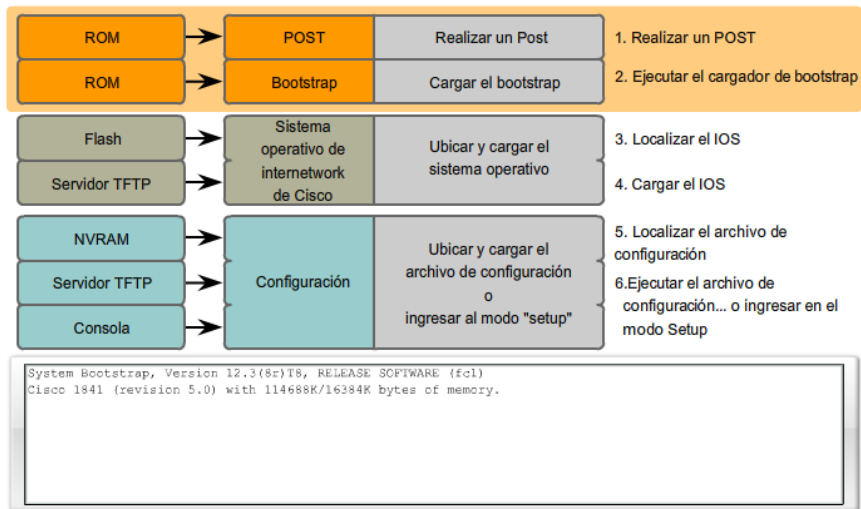
- direcciones de interfaz
- información de enrutamiento
- contraseñas
- cualquier otra configuración guardada por el administrador de red

Si el archivo de configuración de inicio, startup-config, se encuentra en la NVRAM, se copia a la RAM como el archivo de configuración en ejecución, running-config.

Nota: si el archivo de configuración de inicio no existe en la NVRAM, el router puede buscar un servidor TFTP. Si el router detecta que tiene un enlace activo a otro router configurado, envía un broadcast en busca de un archivo de configuración a través del enlace activo.

Ejecución del archivo de configuración. Si se encuentra un archivo de configuración de inicio en la NVRAM, el IOS lo carga en la RAM como el running-config y ejecuta los comandos del archivo, de a una línea por vez. El archivo running-config contiene direcciones de interfaz, inicia los procesos de enrutamiento, configura las contraseñas del router y define otras características del router.

Ingreso al modo Setup (opcional): si no puede localizarse el archivo de configuración de inicio, el router indica al usuario que ingrese en el modo Setup. El modo Setup consiste en una serie de preguntas que solicitan al usuario información de configuración básica. El modo Setup no tiene como fin utilizarse para ingresar a configuraciones complejas del router y los administradores de red normalmente no lo usan.



4. Principios de la tabla de enrutamiento de un router.

Principios de la tabla de enrutamiento

En algunas secciones de este curso haremos referencia a tres principios relacionados con las tablas de enrutamiento que lo ayudarán a comprender, configurar y solucionar problemas de enrutamiento. Estos principios se extraen del libro de Alex Zinin, Cisco IP Routing.

1. Cada router toma sus propias decisiones en forma independiente, según la información de su propia tabla de enrutamiento.
2. El hecho de que un router tenga cierta información en su tabla de enrutamiento no significa que los otros routers tengan la misma información.
3. La información de enrutamiento acerca de una ruta de una red a otra no proporciona información de enrutamiento acerca de la ruta inversa o de retorno.

5. Describe el proceso de conmutación de los paquetes en un router.

Después de que el router ha determinado la interfaz de salida utilizando la función de determinación de ruta, el router debe encapsular el paquete en la trama de enlace de datos de la interfaz de salida.

La función de conmutación es el proceso utilizado por un router para aceptar un paquete en una interfaz y reenviarlo hacia otra interfaz. Una responsabilidad clave de la función de conmutación es la de encapsular los paquetes en el tipo de trama de enlace de datos correcto para el enlace de datos de salida.

¿Qué hace un router cuando recibe un paquete desde una red que está destinado a otra red? El router ejecuta los siguientes tres pasos principales:

1. Desencapsula el paquete de la Capa 3 eliminando el encabezado y el tráiler de la trama de Capa 2.
2. Examina la dirección IP de destino del paquete IP para encontrar el mejor camino en la tabla de enrutamiento.
3. Encapsula el paquete de la Capa 3 en una nueva trama de Capa 2 y reenvía la trama a través de la interfaz de salida.

Tema 2:

1. Describe las conexiones y conectores LAN y WAN de un router.

Conexiones del router

La conexión de un router a una red requiere que un conector de interfaz del router esté acoplado a un conector de cable. Como puede verse en la figura, los routers Cisco admiten diversos tipos de conectores.

Conectores seriales

Para las conexiones WAN, los routers Cisco admiten los estándares EIA/TIA-232, EIA/TIA-449, V.35, X.21 y EIA/TIA-530 para conectores seriales, como se muestra. No es importante memorizar estos tipos de conexiones. Sólo debe saber que un router tiene un puerto DB-60 que puede admitir cinco estándares de cableado diferentes. Debido a que admite cinco tipos de cableado diferentes, este puerto a veces se denomina puerto serial cinco en uno. El otro extremo del cable serial cuenta con un conector adecuado para uno de los cinco estándares posibles.

Los routers más nuevos admiten la interfaz serial inteligente que permite reenviar una mayor cantidad de datos a través de una menor cantidad de pins de cable. El extremo serial del cable serial inteligente es un conector de 26 pins. Es mucho más pequeño que el conector DB-60 que se utiliza para conectarse a un puerto serial cinco en uno. Estos cables de transición admiten los mismos cinco estándares seriales y están disponibles en configuraciones DTE o DCE.

Estas designaciones de cables sólo serán de su interés cuando configure su equipo de laboratorio para simular un entorno "real". En un entorno de producción, usted determina el tipo de cable según el servicio WAN que utilice.

Conectores Ethernet

Se utiliza un conector diferente en un entorno LAN basado en Ethernet. El conector RJ-45 para el cable de par trenzado no blindado (UTP) es el conector que se utiliza con mayor frecuencia para conectar interfaces LAN. En cada extremo de un cable RJ-45 debe haber ocho tiras de colores o pins. El cable Ethernet utiliza los pins 1, 2, 3 y 6 para transmitir y recibir datos.

Los cables de conexión directa se usan para conectar:

- Un switch a un router
- Un switch a una PC
- Un hub a una PC
- Un hub a un servidor

Los cables de conexión cruzada se usan para conectar:

- Un switch a otro switch
- Una PC a otra PC
- Una switch a un hub
- Un hub a otro hub
- Un router a otro router
- Un router a un servidor

2. Conceptos de la tabla de enrutamiento.

El comando `show ip route` muestra el contenido de la tabla de enrutamiento. Revisemos el objetivo de una tabla de enrutamiento. Una tabla de enrutamiento es una estructura de datos que almacena información de enrutamiento obtenida de diferentes orígenes. El objetivo principal de una tabla de enrutamiento es proporcionarle al router rutas para llegar a diferentes redes de destino.

La tabla de enrutamiento consiste en una lista de direcciones de red "conocidas", es decir, aquellas direcciones que están conectadas directamente, configuradas estáticamente y que se detectan de manera dinámica. R1 y R2 sólo tienen rutas para redes conectadas directamente.

3. ¿Que es CDP?. Funcionamiento.

El protocolo de descubrimiento de Cisco (CDP) es una poderosa herramienta de monitoreo y resolución de problemas de redes. El CDP es una herramienta de recopilación de información utilizada por administradores de red para obtener información acerca de los dispositivos Cisco conectados directamente. El CDP es una herramienta patentada que le permite acceder a un resumen de información de protocolo y dirección sobre los dispositivos Cisco conectados directamente. De manera predeterminada, cada dispositivo Cisco envía mensajes periódicos, conocidos como publicaciones CDP, a dispositivos Cisco conectados directamente. Estas publicaciones contienen información acerca de los tipos de dispositivos que están conectados, las interfaces del router a las que están conectadas, las interfaces utilizadas para realizar las conexiones y los números de modelo de los dispositivos.

Por naturaleza, la mayoría de los dispositivos de red no funcionan de manera aislada. Un dispositivo Cisco a menudo tiene como vecinos a otros dispositivos Cisco en la red. La información obtenida de otros dispositivos puede ayudarlo a tomar decisiones relacionadas con el diseño de la red, solucionar problemas y realizar cambios en el equipo. El CDP puede utilizarse como una herramienta de descubrimiento de redes que le permite crear una topología lógica de una red cuando falta dicha documentación o cuando no tiene información suficiente.

El CDP funciona sólo en la Capa 2. Por lo tanto, los vecinos del CDP son dispositivos Cisco que están conectados físicamente en forma directa y comparten el mismo enlace de datos.

Funcionamiento del CDP

Examine los resultados de los comandos `show cdp neighbors` y `show cdp neighbors detail` en la figura. Observe que R3 ha recopilado información detallada acerca de R2 y el switch conectado a la interfaz Fast Ethernet de R3.

El CDP se ejecuta en la capa de enlace de datos que conecta los medios físicos a los protocolos de capa superior (ULP). Dos o más dispositivos de red Cisco, tales como los routers que admiten diferentes protocolos de capa de red (por ejemplo, IP y Novell IPX) pueden obtener información uno del otro debido a que el CDP funciona en la capa de enlace de datos.

Cuando arranca un dispositivo Cisco, el CDP se inicia de manera predeterminada. El CDP descubre automáticamente los dispositivos Cisco que ejecutan el CDP, independientemente de qué protocolo o conjunto de aplicaciones se ejecuta. El CDP intercambia información del hardware y software del dispositivo con sus vecinos CDP conectados directamente.

El CDP brinda la siguiente información acerca de cada dispositivo vecino de CDP:

- Identificadores de dispositivos: por ejemplo, el nombre host configurado de un switch.
- Lista de direcciones: hasta una dirección de capa de red para cada protocolo admitido
- Identificador de puerto: el nombre del puerto local y remoto en forma de una cadena de caracteres ASCII, como por ejemplo, ethernet0
- Lista de capacidades: por ejemplo, si el dispositivo es un router o un switch
- Plataforma: la plataforma de hardware del dispositivo; por ejemplo, un router Cisco serie 7200

4. Características del enrutamiento estatico.

Un router puede obtener información sobre redes remotas de dos maneras:

- Manualmente, a partir de las rutas estáticas configuradas
- Automáticamente, a partir de un protocolo de enrutamiento dinámico

Las rutas estáticas se utilizan generalmente cuando se enruta desde una red a una red de conexión única. Una red de conexión única es una red a la que se accede por una sola ruta.

Tema 3:

1. Enumera y clasifica lo protocolos de enrutamiento dinámico. Tabla 3.1.1.

	Protocolos de gateway interior			Protocolos de gateway exterior	
	Protocolos de enrutamiento vector distancia	Protocolos de enrutamiento de link-state		Vector ruta	
Con clase	RIP	IGRP		EGP	
Sin clase	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGPv4 para IPv6

2. Funciones y proposito de los protocolos de enrutamiento dinámico.

Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la elección de los mejores caminos que realiza el protocolo. El propósito de un protocolo de enrutamiento incluye:

- Descubrir redes remotas
- Mantener la información de enrutamiento actualizada
- Escoger el mejor camino hacia las redes de destino
- Poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible

Todos los protocolos de enrutamiento tienen el mismo propósito: obtener información sobre redes remotas y adaptarse rápidamente cuando ocurre un cambio en la topología. El método que usa un protocolo de enrutamiento para lograr su propósito depende del algoritmo que use y de las características operativas de ese protocolo. Las operaciones de un protocolo de enrutamiento dinámico varían según el tipo de protocolo de enrutamiento y el protocolo de enrutamiento en sí. En general, las operaciones de un protocolo de enrutamiento dinámico pueden describirse de la siguiente manera:

- El router envía y recibe mensajes de enrutamiento en sus interfaces.
- El router comparte mensajes de enrutamiento e información de enrutamiento con otros routers que están usando el mismo protocolo de enrutamiento.
- Los routers intercambian información de enrutamiento para obtener información sobre redes remotas.
- Cuando un router detecta un cambio de topología, el protocolo de enrutamiento puede anunciar este cambio a otros routers.

3. ¿Cuáles son los componentes de los protocolos de enrutamiento dinámicos?.

- Estructuras de datos: algunos protocolos de enrutamiento usan tablas y/o bases de datos para sus operaciones. Esta información se guarda en la RAM.
- Algoritmo: un algoritmo es una lista limitada de pasos que se usan para llevar a cabo una tarea. Los protocolos de enrutamiento usan algoritmos para facilitar información de enrutamiento y para determinar el mejor camino.
- Mensajes del protocolo de enrutamiento: los protocolos de enrutamiento usan varios tipos de mensajes para descubrir routers vecinos, intercambiar información de enrutamiento y otras tareas para aprender y conservar información precisa sobre la red.

4. Diferencias entre el protocolo de enrutamiento estatico y dinamico. Tabla.

	Enrutamiento dinámico	Enrutamiento estático
Complejidad de la configuración	Por lo general es independiente del tamaño de la red	Se incrementa con el tamaño de la red
Conocimientos requeridos del administrador	Se requiere de un conocimiento avanzado	No se requieren conocimientos adicionales
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere la intervención del administrador
Escalamiento	Adecuado para las topologías simples y complejas	Adecuada para topologías simples
Seguridad	Es menos seguro	Más segura
Uso de recursos	Utiliza CPU, memoria y ancho de banda de enlace	No se requieren recursos adicionales
Capacidad de predicción	La ruta depende de la topología actual	La ruta hacia el destino es siempre la misma

5. Tipos de protocolos de Gateway interior (IGP) y funcionamiento.

Un sistema autónomo (AS), conocido también como dominio de enrutamiento, es un conjunto de routers que se encuentran bajo una administración común.

Los IGP se usan para el enrutamiento dentro de un dominio de enrutamiento, aquellas redes bajo el control de una única organización. Un sistema autónomo está comúnmente compuesto por muchas redes individuales que pertenecen a empresas, escuelas y otras instituciones. Un IGP se usa para enrutar dentro de un sistema autónomo, y también se usa para enrutar dentro de las propias redes individuales.

Los IGP para IP incluyen RIP, IGRP, EIGRP, OSPF e IS-IS.

Los protocolos de enrutamiento, y más específicamente el algoritmo utilizado por ese protocolo de enrutamiento, utilizan una métrica para determinar el mejor camino hacia una red. La métrica utilizada por el protocolo de enrutamiento RIP es el conteo de saltos, que es el número de routers que un paquete debe atravesar para llegar a otra red. OSPF usa el ancho de banda para determinar la ruta más corta.

6. Diferencias entre un protocolo de enrutamiento con clase y sin clase. Problemática.

Protocolos de enrutamiento con clase

Los protocolos de enrutamiento con clase no envían información de la máscara de subred en las actualizaciones de enrutamiento. Los primeros protocolos de enrutamiento, como el RIP, tenían clase. En aquel momento, las direcciones de red se asignaban en función de las clases; clase A, B o C. No era necesario que un protocolo de enrutamiento incluyera una máscara de subred en la actualización de enrutamiento porque la máscara de red podía determinarse en función del primer octeto de la dirección de red.

Los protocolos de enrutamiento con clase aún pueden usarse en algunas de las redes actuales, pero dado que no incluyen la máscara de subred, no pueden usarse en todas las situaciones. Los protocolos de enrutamiento con clase no se pueden usar cuando una red se divide en subredes utilizando más de una máscara de subred; en otras palabras, los protocolos de enrutamiento con clase no admiten máscaras de subred de longitud variable (VLSM).

Existen otras limitaciones de los protocolos de enrutamiento con clase, entre ellas la imposibilidad de admitir redes no contiguas. Los protocolos de enrutamiento con clase, las redes no contiguas y VLSM se analizarán en capítulos posteriores.

Los protocolos de enrutamiento con clase incluyen RIPv1 e IGRP.

Protocolos de enrutamiento sin clase

Estos protocolos de enrutamiento incluyen la máscara de subred con la dirección de red en sus actualizaciones de enrutamiento. Las redes de la actualidad ya no se asignan en función de las clases y la máscara de subred no puede determinarse según el valor del primer octeto. La mayoría de las redes de la actualidad requieren protocolos de enrutamiento sin clase porque admiten VLSM, redes no contiguas y otras funciones que se analizarán en capítulos posteriores.

En la figura, observe que la versión sin clase de la red está usando máscaras de subred /30 y /27 en la misma topología. Además, observe que esta topología está usando un diseño no contiguo.

Los protocolos de enrutamiento sin clase son RIPv2, EIGRP, OSPF, IS-IS y BGP.

7. ¿Qué es la convergencia de un router?

La convergencia ocurre cuando todas las tablas de enrutamiento de los routers se encuentran en un estado de uniformidad. La red ha convergido cuando todos los routers tienen información completa y precisa sobre la red. El tiempo de convergencia es el tiempo que los routers tardan en compartir información, calcular las mejores rutas y actualizar sus tablas de enrutamiento. Una red no es completamente operativa hasta que la red haya convergido; por lo tanto, la mayoría de las redes requieren tiempos de convergencia breves.

La convergencia es cooperativa e independiente al mismo tiempo. Los routers comparten información entre sí pero deben calcular en forma independiente los impactos del cambio de topología en sus propias rutas. Dado que establecen un acuerdo con la nueva topología en forma independiente, se dice que convergen sobre este consenso.

Las propiedades de convergencia incluyen la velocidad de propagación de la información de enrutamiento y el cálculo de los caminos óptimos. Los protocolos de enrutamiento pueden clasificarse en base a la velocidad de convergencia; cuanto más rápida sea la convergencia, mejor será el protocolo de enrutamiento. Por lo general, RIP e IGRP tienen convergencia lenta, mientras que EIGRP y OSPF tienen una convergencia más rápida.

8. Métricas en los protocolos de enrutamiento IP.

Las métricas utilizadas en los protocolos de enrutamiento IP incluyen:

- **Conteo de saltos:** una métrica simple que cuenta la cantidad de routers que un paquete tiene que atravesar.
- **Ancho de banda:** influye en la selección de rutas al preferir la ruta con el ancho de banda más alto.
- **Carga:** considera la utilización de tráfico de un enlace determinado.
- **Retardo:** considera el tiempo que tarda un paquete en atravesar una ruta.
- **Confiabilidad:** evalúa la probabilidad de una falla de enlace calculada a partir del conteo de errores de la interfaz o las fallas de enlace previas.
- **Costo:** un valor determinado ya sea por el Cisco IOS o por el administrador de red para indicar la preferencia de una ruta. El costo puede representar una métrica, una combinación de las mismas o una política.

9. Distancias administrativas y métricas predeterminadas.

Tema 4:

1. Características del protocolo de enrutamiento RIP.

RIP

El protocolo de información de enrutamiento (RIP), se mencionó originalmente en el RFC 1058. Sus características principales son las siguientes:

- Utiliza el conteo de saltos como métrica para la selección de rutas.

- Si el conteo de saltos de una red es mayor de 15, el RIP no puede suministrar una ruta para esa red.
- De manera predeterminada, se envía un broadcast o multicast de las actualizaciones de enrutamiento cada 30 segundos.

2. Características del protocolo de enrutamiento EIGRP.

El IGRP mejorado (EIGRP) es un protocolo de enrutamiento vector distancia patentado por Cisco. Las características principales del EIGRP son las siguientes:

- Puede realizar un balanceo de carga con distinto costo.
- Utiliza el Algoritmo de actualización por difusión (DUAL) para calcular la ruta más corta.
- No existen actualizaciones periódicas, como sucede con el RIP y el IGRP. Las actualizaciones de enrutamiento sólo se envían cuando se produce un cambio en la topología.

3. Funcionamiento de los protocolos de enrutamiento de vector distancia.

Funcionamiento de los protocolos de enrutamiento vector distancia

Algunos protocolos de enrutamiento vector distancia solicitan al router que envíe periódicamente un broadcast de toda la tabla de enrutamiento a cada uno de los vecinos. Este método no es eficiente porque las actualizaciones no sólo consumen ancho de banda sino también los recursos de la CPU del router para procesar las actualizaciones.

Los protocolos de enrutamiento vector distancia comparten ciertas características.

Las actualizaciones periódicas se envían a intervalos regulares (30 segundos para RIP y 90 segundos para IGRP). Incluso si la topología no ha cambiado en varios días, las actualizaciones periódicas continúan enviándose a todos los vecinos.

Los vecinos son routers que comparten un enlace y que están configurados para usar el mismo protocolo de enrutamiento. El router sólo conoce las direcciones de red de sus propias interfaces y las direcciones de red remota que puede alcanzar a través de sus vecinos. No tiene un conocimiento más amplio de la topología de la red. Los routers que utilizan el enrutamiento vector distancia no tienen información sobre la topología de la red.

Las actualizaciones de broadcast se envían a 255.255.255.255. Los routers vecinos que están configurados con el mismo protocolo de enrutamiento procesarán las actualizaciones. Todos los demás dispositivos también procesarán la actualización hasta la Capa 3 antes de descartarla. Algunos protocolos de enrutamiento vector distancia usan direcciones de multicast en vez de direcciones de broadcast.

Las actualizaciones de toda la tabla de enrutamiento se envían periódicamente a todos los vecinos, salvo algunas excepciones que analizaremos más adelante. Los vecinos que reciban estas actualizaciones deben procesar toda la actualización para encontrar información pertinente y descartar el resto. Algunos protocolos de enrutamiento vector distancia, como el EIGRP, no envían actualizaciones periódicas de la tabla de enrutamiento.

Propósito de enrutar los algoritmos

- Envío y recepción de actualizaciones
- Calcular el mejor camino e instalarlo
- Detectar cambios en la topología y reaccionar a ellos

4. Ventajas y desventajas de los protocolos de enrutamiento. Tabla 4.1.4.

Ventajas:	Desventajas:
Implementación y mantenimiento simples. No se requiere de mucho conocimiento para implementar y posteriormente mantener una red con protocolo vector distancia.	Convergencia lenta. La utilización de actualizaciones periódicas puede hacer que la convergencia sea más lenta. Incluso si se utilizan técnicas avanzadas, como por ejemplo, los triggered updates (que se analizarán más adelante), la convergencia general aún sigue siendo más lenta en comparación con los protocolos de enrutamiento de link-state.
Pocos requisitos de recursos. Los protocolos vector distancia generalmente no requieren una gran cantidad de memoria para almacenar información. Tampoco requieren de una CPU muy potente. Dependiendo del tamaño de la red y del direccionamiento IP implementado, generalmente tampoco requieren de un alto nivel de ancho de banda de enlace para enviar actualizaciones de enrutamiento. Sin embargo, esto puede representar un problema si se implementa un protocolo vector distancia en una gran red.	Escalabilidad limitada. La convergencia lenta puede limitar el tamaño de la red porque las redes más grandes requieren más tiempo para propagar la información de enrutamiento.
	Loops de enrutamiento. Los loops de enrutamiento pueden ser el resultado de tablas de enrutamiento incongruentes que no se han actualizado debido a la lenta convergencia de una red sujeta a cambios.

5. Temporizadores RIP.

Temporizadores del RIP

Además del temporizador de actualización, el IOS aplica tres temporizadores adicionales para el RIP:

- De invalidez
- De purga
- De espera

Temporizador de invalidez Si no se recibió una actualización para renovar la ruta existente una vez que hayan transcurrido 180 segundos (predeterminado), la ruta se marca como no válida y la métrica se configura en 16. Se retiene la ruta en la tabla de enrutamiento hasta que se vence el temporizador de purga.

Temporizador de purga De manera predeterminada, el temporizador de purga se configura en 240 segundos, es decir, 60 segundos más que el temporizador de invalidez. Cuando vence el temporizador de purga, la ruta se elimina de la tabla de enrutamiento.

Temporizador de espera Este temporizador estabiliza la información de enrutamiento y ayuda a evitar loops de enrutamiento durante los períodos en los que la topología converge en la nueva información. Una vez que se marca una ruta como inalcanzable, ésta debe permanecer en espera el tiempo suficiente como para que todos los routers de la topología aprendan sobre la red inalcanzable. De manera predeterminada, el temporizador de espera está configurado en 180 segundos.

6. ¿Qué es un Loop de enrutamiento?. Describe los modos utilizados para evitarlo.

¿Qué es un loop de enrutamiento?

Es una condición en la que un paquete se transmite continuamente dentro de una serie de routers sin que nunca alcance la red de destino deseada. Un loop de enrutamiento se puede producir cuando dos o más routers tienen información de enrutamiento que indica erróneamente que existe una ruta válida a un destino inalcanzable.

El loop puede ser el resultado de lo siguiente:

- Rutas estáticas configuradas incorrectamente
- Redistribución de rutas configuradas incorrectamente (la redistribución es un proceso de envío de la información de enrutamiento desde un protocolo de enrutamiento a otro y se analizará en los cursos de nivel CCNP)

- Tablas de enrutamiento incongruentes que no se actualizan debido a una convergencia lenta en una red cambiante
- Rutas de descarte configuradas o instaladas incorrectamente

Los protocolos de enrutamiento vector distancia tienen un funcionamiento simple. Su simplicidad origina algunas desventajas, como por ejemplo, los loops de enrutamiento. Los loops de enrutamiento no generan demasiados problemas con los protocolos de enrutamiento de link-state, pero se pueden presentar en determinadas circunstancias.

¿Qué consecuencias tienen los loops de enrutamiento?

Un loop de enrutamiento puede tener un efecto devastador en una red y producir un menor rendimiento o incluso un tiempo de inactividad de dicha red.

Un loop de enrutamiento puede producir las siguientes condiciones:

- El ancho de banda del enlace se utilizará para el tráfico que se transmita de un sitio a otro entre los routers de un loop.
- La CPU de un router estará exigida debido a los paquetes con loops.
- La CPU de un router se cargará con el reenvío inútil de paquetes, lo que afectará negativamente la convergencia de la red.
- Las actualizaciones de enrutamiento pueden perderse o no ser procesadas de manera oportuna. Estas condiciones podrían originar otros loops de enrutamiento, lo que empeoraría aún más la situación.
- Los paquetes pueden perderse en "agujeros negros".

Existen varios mecanismos disponibles para eliminar los loops de enrutamiento, principalmente con los protocolos de enrutamiento vector distancia. Estos mecanismos incluyen:

- Definición de una métrica máxima para evitar una cuenta a infinito: La cuenta a infinito es una condición que se produce cuando las actualizaciones de enrutamiento inexactas aumentan el valor de la métrica a "infinito" para una red que ya no se puede alcanzar.
- Temporizadores de espera:

Los temporizadores de espera funcionan de la siguiente manera:

1. Un router recibe una actualización de un vecino que indica que una red que anteriormente era accesible ahora no lo es más.
 2. El router marca la red como posiblemente desactivada e inicia el temporizador de espera.
 3. Si se recibe una actualización con una métrica mejor para esa red desde cualquier router vecino durante el período de espera, la red se reinstala y se elimina el temporizador de espera.
 4. Si se recibe una actualización desde cualquier otro vecino durante el período de espera con la misma métrica o una métrica peor para esa red, se ignorará dicha actualización. Por consiguiente, se dispone de más tiempo para que se propague la información acerca del cambio.
5. Los routers continúan reenviando paquetes a las redes de destino marcadas como posiblemente desactivadas. Esto permite que el router supere cualquier dificultad relacionada con la conectividad intermitente. Si realmente la red de destino no está disponible y los paquetes se envían, se crea un enrutamiento de agujero negro y dura hasta que venza el temporizador de espera.
- Horizonte dividido: La regla de horizonte dividido establece que un router no debería publicar una red a través de la interfaz por la cual provino la actualización.
 - Envenenamiento de ruta o envenenamiento en reversa: El envenenamiento de ruta se utiliza para marcar la ruta como inalcanzable en una actualización de enrutamiento que se envía a otros routers.
 - Triggered updates:

7. Diferencias entre el protocolo de enrutamiento RIP y EIGRP.

Para los protocolos de enrutamiento vector distancia, sólo existen realmente dos opciones: RIP o EIGRP. La decisión acerca de qué protocolo de enrutamiento se utilizará en una situación determinada depende de varios factores, entre los que se incluyen:

- El tamaño de la red
- La compatibilidad entre los modelos de routers
- El requisito de conocimientos administrativos

RIP

Con el tiempo, el RIP ha pasado de ser un protocolo de enrutamiento con clase (RIPv1) a un protocolo de enrutamiento sin clase (RIPv2). El RIPv2 es un protocolo de enrutamiento estandarizado que funciona en un entorno de router de fabricante mixto. Los routers fabricados por empresas diferentes pueden comunicarse utilizando el RIP. Éste es uno de los protocolos de enrutamiento más fáciles de configurar, lo que lo convierte en una buena opción para las redes pequeñas. Sin embargo, el RIPv2 todavía tiene limitaciones. Tanto el RIPv1 como el RIPv2 tienen una métrica de ruta que se basa sólo en el conteo de saltos y que se limita a 15 saltos.

Características del RIP:

- Admite el horizonte dividido y el horizonte dividido con envenenamiento en reversa para evitar loops.
- Es capaz de admitir un balanceo de carga de hasta seis rutas del mismo costo. El valor predeterminado es de cuatro rutas del mismo costo.

El RIPv2 introdujo las siguientes mejoras al RIPv1:

- Incluye una máscara de subred en las actualizaciones de enrutamiento, lo que lo convierte en un protocolo de enrutamiento sin clase.
- Tiene un mecanismo de autenticación para la seguridad de las actualizaciones de las tablas.
- Admite una máscara de subred de longitud variable (VLSM).
- Utiliza direcciones multicast en vez de broadcast.
- Admite sumarización manual de ruta.

EIGRP

El IGRP mejorado (EIGRP) se desarrolló a partir del IGRP, otro protocolo vector distancia. El EIGRP es un protocolo de enrutamiento vector distancia sin clase que tiene características propias de los protocolos de enrutamiento de link-state. Sin embargo, y a diferencia del RIP o el OSPF, el EIGRP es un protocolo patentado desarrollado por Cisco y sólo se ejecuta en los routers Cisco.

Estas características incluyen:

- Triggered updates (el EIGRP no tiene actualizaciones periódicas).
- Utilización de una tabla de topología para mantener todas las rutas recibidas de los vecinos (no sólo los mejores caminos).
- Establecimiento de adyacencia con los routers vecinos utilizando el protocolo Hello EIGRP.
- Admite VLSM y la sumarización manual de ruta. Esta característica le permite al EIGRP crear grandes redes estructuradas jerárquicamente.

Ventajas del EIGRP:

Si bien las rutas se propagan como un vector distancia, la métrica se basa en el ancho de banda mínimo y en el retardo acumulado de la ruta en lugar del conteo de saltos.

Rápida convergencia debido al cálculo de ruta mediante Algoritmo de actualización por difusión (DUAL). El DUAL permite la inserción de rutas de respaldo en la tabla de topología de EIGRP. Éstas se utilizan en caso de falla de la ruta principal. Puesto que se trata de un procedimiento local, el cambio a la ruta de respaldo es inmediato y no implica ninguna acción en ningún otro router.

Las actualizaciones limitadas significan que el EIGRP utiliza menos ancho de banda, especialmente en grandes redes con muchas rutas.

El EIGRP admite múltiples protocolos de capa de red a través de los Módulos dependientes de protocolos, que incluyen la admisión de IP, IPX y AppleTalk.

Tema 5:

1. Características del protocolo de enrutamiento RIP v1 y limitaciones.

La porción de datos de un mensaje de RIP se encapsula en un segmento UDP, con los números de puerto de origen y destino establecidos en 520. El encabezado IP y los encabezados de enlace de datos agregan direcciones de destino de broadcast antes de enviar el mensaje a todas las interfaces configuradas con RIP.

- Rutas estáticas e interfaces nulas
- Redistribución de ruta
- Incompatibilidad con VLSM
- Incompatibilidad con CIDR

Tema 6:

1. ¿Qué es VLSM? ¿Qué es CIDR?

El CIDR permitía:

- El uso más eficaz del espacio de direcciones IPv4.
- El agregado de prefijos, que redujo el tamaño de las tablas de enrutamiento.

Para los routers compatibles con CIDR, la clase de dirección no tiene sentido. A la porción de red de la dirección la determina la máscara de subred de la red, también conocida como prefijo de red o duración de prefijo (/8, /19, etc.). La clase de dirección ya no determina la dirección de red.

CIDR usa máscaras de subred de longitud variable (VLSM) para asignar direcciones IP a subredes de acuerdo con la necesidad individual en lugar de hacerlo según la clase. Este tipo de asignación permite que el borde de la red/del host se produzca en cualquier bit de la dirección. Las redes, a su vez, se pueden subdividir o dividir en subredes cada vez más pequeñas.

CIDR es una forma de sumarización de ruta y es sinónimo del término creación de superredes.

Superredes: Combinación de varias direcciones de red IP en una única dirección IP. La creación de superredes reduce el número de entradas en una tabla de enrutamiento y se realiza en el direccionamiento CIDR como así también en redes internas.

VLSM simplemente subdivide una subred. Se puede considerar a VLSM como una división en sub-subredes.

Tema 7:

1. Características del protocolo de enrutamiento RIP v2.

RIPv2 se define en RFC 1723. Al igual que la versión 1, RIPv2 se encapsula en un segmento UDP mediante el puerto 520 y puede transportar hasta 25 rutas. Si bien RIPv2 tiene el mismo formato de mensaje básico que RIPv1, se agregan dos extensiones importantes.

La primera extensión en el formato de mensaje de RIPv2 es el campo de la máscara de subred que permite que una máscara de 32 bits se incluya en la entrada de ruta de RIP. Como resultado, el router receptor ya no depende de la máscara de subred de la interfaz entrante ni de la máscara con clase al determinar la máscara de subred para una ruta.

La segunda extensión importante para el formato de mensaje de RIPv2 es la adición de la dirección de siguiente salto. La dirección del siguiente salto se usa para identificar una dirección de siguiente salto mejor que la dirección del router emisor, si es que existe. Si el campo se establece todo en ceros (0.0.0.0), la dirección del router emisor es la mejor dirección del siguiente salto.

Tema 8:

1. Estructura de la tabla de enrutamiento de router Cisco.

La tabla de enrutamiento consta de entradas de ruta de los siguientes orígenes:

- Redes conectadas directamente
- Rutas estáticas
- Protocolos de enrutamiento dinámico

El origen de la ruta no afecta la estructura de la tabla de enrutamiento. La figura muestra un ejemplo de tabla de enrutamiento con rutas dinámicas, estáticas y conectadas directamente.

La tabla de enrutamiento IP de Cisco no es una base de datos plana. La tabla de enrutamiento, en realidad, es una estructura jerárquica que se usa para acelerar el proceso de búsqueda cuando se ubican rutas y se reenvían paquetes.

Una ruta de nivel 1 puede funcionar como:

- Ruta predeterminada: una ruta predeterminada es una ruta estática con la dirección 0.0.0.0/0.
- Ruta de superred: una ruta de superred es una dirección de red con una máscara menor que la máscara con clase.
- Ruta de red: una ruta de red es una ruta que tiene una máscara de subred igual a la de la máscara con clase. Una ruta de red también puede ser una ruta principal. Las rutas principales se analizarán en la siguiente sección.

El origen de la ruta de nivel 1 puede ser una red conectada directamente, una ruta estática o un protocolo de enrutamiento dinámico.

Las rutas secundarias de nivel 2 también se consideran rutas finales porque contienen la dirección IP del siguiente salto y/o la interfaz de salida.

2. Proceso de búsqueda en la tabla de enrutamiento de router Cisco.

Proceso de búsqueda de rutas

Siga estos pasos en la figura para ver el proceso de búsqueda de rutas. No se preocupe si no comprende completamente los pasos en este momento. Entenderá mejor este proceso cuando examinemos algunos ejemplos de las siguientes secciones.

Haga clic en Paso 1.

El router examina las rutas de nivel 1, incluidas las rutas de red y las rutas de superred, en busca de la mejor coincidencia con la dirección IP de destino del paquete.

Haga clic en Paso 1a.

Si la mejor coincidencia es una ruta final de nivel 1 (superred, red con clase o ruta predeterminada) esta ruta se usa para reenviar el paquete.

Haga clic en Paso 1b.

Si la mejor coincidencia es una ruta principal de nivel 1, continúe con el Paso 2.

Haga clic en Paso 2.

El router examina las rutas secundarias (las rutas de subred) de la ruta principal en busca de una mejor coincidencia.

Haga clic en Paso 2a.

Si hay una coincidencia con una ruta secundaria de nivel 2, esa subred se usará para reenviar el paquete.

Haga clic en Paso 2b.

Si no hay coincidencia con ninguna de las rutas secundarias de nivel 2, continúe con el Paso 3. Haga clic en Paso 3. ¿El router está implementando un comportamiento de enrutamiento con clase o sin clase?

Haga clic en Paso 3a.

Comportamiento del enrutamiento con clase: Si el comportamiento de enrutamiento con clase está en vigencia, termine el proceso de búsqueda y descarte el paquete.

Haga clic en Paso 3b.

Comportamiento del enrutamiento sin clase: Si el comportamiento de enrutamiento sin clase está en vigencia, continúe buscando las rutas de superred de nivel 1 en la tabla de enrutamiento para ver si hay alguna coincidencia, incluida la ruta predeterminada, si así fuera.

Haga clic en Paso 4.

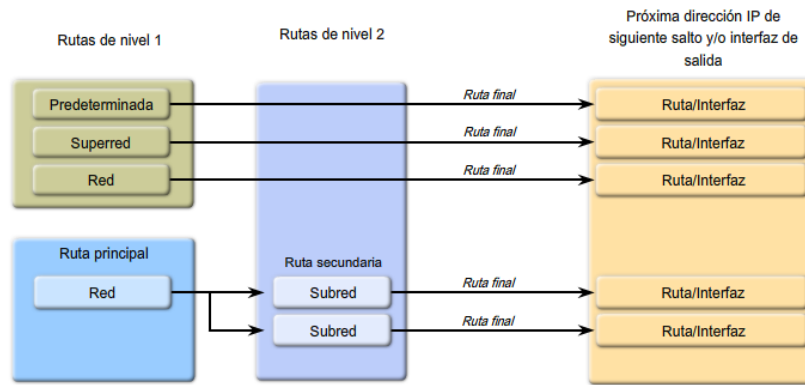
Si ahora hay una coincidencia menor con las rutas predeterminadas o de superred de nivel 1, el router usa esa ruta para reenviar el paquete.

Haga clic en Paso 5.

Si no hay coincidencia con ninguna ruta de la tabla de enrutamiento, el router descarta el paquete.

El comportamiento del enrutamiento con clase y sin clase se analizará con mayor detalle en una sección posterior.

Nota: una ruta que sólo hace referencia a una dirección IP del siguiente salto y no a una interfaz de salida debe resolverse con una ruta con una interfaz de salida. Se realiza una búsqueda recurrente en la dirección IP del siguiente salto hasta que la ruta se resuelva con una interfaz de salida.



Tema 9:

1. Formatos de mensajes EIGRP.

La porción de datos de un mensaje EIGRP se encapsula en un paquete. Este campo de datos se denomina Tipo/Longitud/Valor o TLV. Como se muestra en la figura, los tipos de TLV relevantes para este curso son Parámetros EIGRP, Rutas internas IP y Rutas externas IP. Los componentes del campo de datos TLV se analizan en mayor profundidad en la próxima página.

El encabezado del paquete EIGRP se incluye con cada paquete EIGRP, independientemente de su tipo. Luego, el encabezado del paquete EIGRP y TLV se encapsulan en un paquete IP. En el encabezado del paquete IP, el campo Protocolo se establece en 88 para indicar EIGRP, y la dirección de destino se establece en multicast 224.0.0.10. Si el paquete EIGRP se encapsula en una trama de Ethernet, la dirección MAC de destino es también una dirección multicast: 01-00-5E-00-00-0A.

2. Tablas del protocolo de enrutamiento EIGRP.

EIGRP tiene la capacidad de realizar el enrutamiento de distintos protocolos, incluidos IP, IPX y Apple Talk, mediante el uso de módulos dependientes de protocolo (PDM). Los PDM son responsables de las tareas de enrutamiento específicas de cada protocolo de capa de Red.

3. ¿Qué es un sistema autónomo?.

Un sistema autónomo (AS) es un conjunto de redes bajo el control administrativo de una única entidad que presenta una política de enrutamiento común para Internet.

4. Conceptos de sucesor, sucesor factible y condicion de factibilidad.

Un sucesor es un router vecino que se utiliza para el reenvío de paquetes y es la ruta menos costosa hacia la red de destino. La dirección IP del sucesor se muestra en una entrada de tabla de enrutamiento justo después de la palabra via.

La Distancia factible (FD) es la métrica calculada más baja para llegar a la red de destino. FD es la métrica enumerada en la entrada de la tabla de enrutamiento como el segundo número dentro de paréntesis. De la misma manera que con otros protocolos de enrutamiento también se conoce como la métrica de la ruta.

La condición de factibilidad (FC) se cumple cuando la distancia notificada (RD) de un vecino hacia una red es menor que la distancia factible del router local hacia la misma red de destino. La distancia notificada o la distancia publicada es simplemente una distancia factible EIGRP de vecinos a la misma red de destino. La distancia notificada es la métrica que un router informa a un vecino acerca de su propio costo hacia esa red.

Tema 10:

1. Funcionamiento de los protocolos de enrutamiento de estado enlace.

Los protocolos de enrutamiento de link-state son conocidos por presentar una complejidad bastante mayor que sus vectores distancia equivalentes. Sin embargo, la funcionalidad y configuración básicas de los protocolos de enrutamiento de link-state no son complejas en absoluto.

2. Proceso de enrutamiento de estado enlace. Tabla. 10.1.

Proceso de enrutamiento de link-state

1. Cada router aprende de cada una de sus propias redes conectadas directamente.
2. Cada router tiene la responsabilidad de "saludar" a sus vecinos en redes conectadas directamente.
3. Cada router crea un Paquete de estado de enlace (LSP) que contiene el estado de cada enlace conectado directamente.
4. Cada router inunda el LSP hacia todos sus vecinos, quienes luego almacenan en una base de datos todos los LSP recibidos.
5. Cada router utiliza la base de datos para construir un mapa topológico completo y calcula la mejor ruta para cada red de destino.

3. Ventajas de los protocolos de enrutamiento de estado enlace.

Ventajas de los protocolos de enrutamiento de link-state

- Cada router crea su propio mapa topológico de la red para determinar la ruta más corta.
- La saturación inmediata de los LSP logra una convergencia más rápida.
- Sólo se envían LSP cuando se produce un cambio en la topología y éstos únicamente contienen la información relacionada con tal cambio.
- Diseño jerárquico utilizado cuando se implementan varias áreas.

Tema 11:

1. Características del protocolo de enrutamiento OSPF.

El encabezado del paquete OSPF se incluye con cada paquete OSPF, independientemente de su tipo. El encabezado del paquete OSPF y los datos específicos según el tipo de paquete específico se encapsulan luego en un paquete IP. En el encabezado del paquete IP, el campo Protocolo se establece en 89 para indicar el OSPF y la dirección de destino se establece para una de dos direcciones multicast: 224.0.0.5 ó 224.0.0.6. Si el paquete OSPF se encapsula en una trama de Ethernet, la dirección MAC de destino es también una dirección multicast: 01-00-5E-00-00-05 o 01-00-5E-00-00-06.

2. Tipos de paquetes OSPF.

Tipo	Nombre del paquete	Descripción
1	Saludo	Descubre los vecinos y construye adyacencias entre ellos
2	Descriptores de bases de datos (DBD)	Controla la sincronización de la base de datos entre routers
3	Solicitud de link-state (LSR)	Solicita registros específicos de link-state de router a router
4	Actualización de link-state (LSU)	Envía los registros de link-state específicamente solicitados
5	Acuse de recibo de link-state (LSAck)	Reconoce los demás tipos de paquetes

3. Como determinar la ID del router en el protocolo de enrutamiento de OSPF.

El ID del router OSPF se utiliza para identificar de forma única el router en el dominio de enrutamiento OSPF. El ID de un router es simplemente una dirección IP. Los routers Cisco obtienen el ID del router conforme a tres criterios y con la siguiente prioridad:

1. Dirección IP configurada con el comando OSPF router-id.
2. Si router-id no está configurado, el router elige la dirección IP más alta de cualquiera de sus interfaces loopback.
3. Si no hay ninguna interfaz loopback configurada, el router elige la dirección IP activa más alta de cualquiera de sus interfaces físicas.

PRACTICA:

SUBNETTING

VLSM

RIP

EIGRP

OSPF

COMANDOS

LIBRE