# Resumen CCNA 200-125

## Contenido

## Modelos de referencia:

- Modelo OSI:
  - Aplicación — Telnet / HTTP / SNMP / POP3.
  - Presentación — JPG / MP3.
  - Sesión — NTFS
  - Transporte — TCP / UDP.
  - Red — IP / IPX / ICMP.
  - Enlace de Datos — Ethernet / PPP / HDLC / Frame Relay.
  - Física — RJ-45 / V-35.

- Modelo TCP/IP:
  - Procesos de Aplicación.
  - Transmisión.
  - Internet.
  - Acceso a Red.

- Encapsulación / Desencapsulación
  - Datos.
  - Segmento.
  - Paquete.
  - Trama
  - Bits.

- Estructura de una trama:
  - Encabezado de la trama.
  - Encabezado del paquete.
  - Encabezado del segmento.
  - Datos.
  - FCS.

## Capa física del modelo OSI:

- Medios de cobre.
  - Cable coaxial.
  - Cable de par trenzado de cobre.

- Fibra óptica.
  - Monomodo.
  - Multimodo.

- Wireless.
  - Satélite.
  - Wireless LAN por onda corta.

    - Wireless LAN infrarroja (IR).
    - Wireless LAN por microondas (WLAN).

- Normativa: EIA/TIA 568A y 568 B.
    - Cable derecho.
    - Cable cruzado.

## Estándares Ethernet:

- 10 Base X Ethernet de 10 Mbps
- 100 Base X FastEthernet: 100 Mbps
- 1000 Base X Gigabit Ethernet: 1Gbps
- 10 GBase X 10 Gigabit Ethernet: 10 Gbps

## Elementos comunes de Ethernet:

- Estructura de la trama
- Dimensiones de la trama
    - Mínima = 64 bytes
    - Máxima = 1518 bytes
- Método de acceso al medio: CSMA/CD
- Requerimiento de un slot time en conexiones half dúplex

## Estructura de una trama Ethernet II

- Dirección MAC de destino – 6 bytes.
- Dirección MAC de origen – 6 bytes.
- Tipo – 2 bytes.
- Datos.
- FCS – 4 bytes.

## Tipos de direcciones de destino:

- Unicast.
- Multicast.
- Broadcast.

## Direcciones MAC:

- Dirección física, de capa de enlace de datos.
- Ethernet: Dirección MAC (6 bytes).
    - OUI (3 bytes).
    - ID de puerto (3 bytes).

## Direcciones IPv4.

- Dirección lógica, de capa de red.
- 32 bits de longitud.
    - Notación binaria.
    - Notación decimal: 4 octetos decimales.

## Encabezado IPv4:

- Versión del protocolo IP.
- Tipo de servicio.
- TTL
- Protocolo.
- Dirección IP de origen.
- Dirección IP de destino.
- Longitud total del encabezado: 20 bytes.

## Servicios de capa de transporte:

- Multiplexación de sesiones.
- Segmentación.
- Control de flujo.
- Transporte orientado a la conexión.
- Identificación de aplicaciones.
- Protocolo UDP:
    - No orientado a la conexión.
    - Bajo overead.
    - Provee funciones básicas de transporte.
    - Verificación limitada de errores.
    - No garantiza la entrega de los datos al destino.
    - Longitud total del encabezado: 8 bytes.
- Protocolo TCP:
    - Orientado a la conexión.
    - Verifica potenciales errores.
    - Implementa un acknowledge que da confiabilidad.
    - Posibilita el reenvío de tráfico bajo petición.
    - Incluye un mecanismo de control de flujo.
    - Longitud total del encabezado: 20 bytes.

- Uso de los puertos:
    - 1 – 1023: Puertos bien conocidos.
    - 1024 – 49151: Puertos registrados.
    - 49152 – 65535: Puertos de asignación dinámica.

## Establecimiento de una sesión TCP:

- Verifica disponibilidad del servidor.
- Verifica disponibilidad del servicio.
- Informa al servidor que el cliente intenta una conexión.

## Ventana de TCP:

- El tamaño se negocia al inicio de la sesión.
- Cambia dinámicamente durante la sesión.
- Si es cero, se interrumpe temporalmente el intercambio.
- Si se pierde un segmento, se reduce a la mitad.
- Riesgo: sincronización de sesiones.

## Control de flujo TCP:

- Asegura que los segmentos se reciben sin errores y en orden.
- Indica al origen el segmento que debe enviar a continuación.

## Cierre de la sesión TCP:

- Lo inicia cualquiera de los extremos de la conexión.
- Libera los recursos.

IP es un protocolo no orientado a la conexión que provee direccionamiento de capa de red y enrutamiento a través de una red.

## Direcciones IPv4:

- Compuesta por 32 dígitos binarios en 4 octetos de 8 bits.
- Porción de red – 8 a 24 bits.
- Porción de nodo – 24 a 8 bits.

## Rangos de direcciones por clase:

- Clase A — Primer octeto: 1 a 127
  Red . Nodo . Nodo . Nodo
  0xxxx

- Clase B — Primer octeto: 128 a 191
  Red . Red . Nodo . Nodo
  10xxx

- Clase C — Primer octeto: 192 a 223
  Red . Red . Red . Nodo
  110xx

- Clase D — Primer octeto: 224 a 239
  Representan grupos de nodos (multicast).

- Clase E — Primer octeto: 240 a 255
  Bloqueadas sobre Internet.

## Direcciones IP privadas o RFC 1918:

- Clase A 10.0.0.0
- Clase B 172.16.0.0 a 172.31.0.0
- Clase C 192.168.0.0 a 192.168.255.0

## Composición del direccionamiento de una red:

- Dirección reservada de red: todos 0s en la porción del nodo.
- Dirección reservada de broadcast: todos 1s en la porción del nodo.
- Direcciones de nodo o útiles: el resto.
- Dirección IP de loopback 127.0.0.0
- Dirección IP de autoconfiguración: 169.254.0.0

## ARP:

- Protocolo que obtiene la dirección MAC de un nodo a partir de la dirección IP de destino.
- Permite obtener la dirección MAC para completar una trama Ethernet.
- Construye y mantiene una tabla caché ARP en la memoria RAM.
- Envía solicitudes en formato de broadcast.
- Si se trata de una dirección IP remota, el procedimiento es ARP Proxy.
- ARP Proxy permite obtener la dirección MAC del gateway para enrutar tráfico que tiene como destina una dirección IP de otra red.

## Procedimiento para obtener una dirección IP:

- Configuración manual.
- Configuración automática.
    - Protocolo RARP.
    - Protocolo BootP.
    - Protocolo DHCP.

## Protocolo RARP:

- Permite obtener una dirección IP a partir de la dirección MAC de la terminal.
- Requiere de un servidor RARP en la red.

## ICMP

- Protocolo que provee servicio de mensajería y mensajes de error para
- detectar y resolver problemas en la red de modo automático.
- Utiliza paquetes IP.
- Mensajes de error:
    - Echo request / Echo reply
    - Destino inalcanzable
    - Tiempo excedido
- Mensajes de control:
    - Redirect / Change request
    - Timestamp request
    - Information request
    - Address mask
    - Router advertisement / Selection
    - Source quench

## Direcciones IPv6.

- Direcciones de 128 bits de longitud.
- Se expresan con 32 dígitos hexadecimales agrupados en 8 campos.

## Tipos de direcciones IPv6:

- Direcciones de unicast.
    - Globales.
    - Link local.
    - Unique local.
    - Reservadas.
- Direcciones de anycast.
- Direcciones de multicast.

## Estructura de la dirección de unicast global:

- Prefijo de ruta global: 48 bits.
- ID de red local: 16 bits.
- ID de interfaz: 64 bits.

## Métodos de asignación de direcciones IPv6:

- Asignación estática:
    - Asignación manual.
    - Asignación utilizando ID EUI-64.
- Asignación dinámica:
    - Autoconfiguración o stateless.
    - DHCPv6.

## Mecanismos para la transición IPv4 a IPv6.

- Dual stack.
- Tunelizado.
    - Túnel manual IPv6-over-IPv4.
    - Dynamic 6to4.
    - ISATAP.
    - Teredo.

## Pasos para el diagnóstico de problemas de configuración de IP:

- Ping a la dirección de loopback (127.0.0.1)
- Ping a la dirección IP del mismo nodo.
- Ping al default gateway
- Ping al dispositivo remoto.

## Subredes IPv4:

- Se comportan dentro de la red como dominios de broadcast independientes.
- Se identifican utilizando al menos los 2 primeros bits de la porción del nodo de la dirección IP.
- Para indicar los bits que identifican la subred que utiliza una máscara de subred.

## La máscara de subred:

- Número binario de 32 dígitos.
- Cada bit de la máscara se corresponde con un bit de la dirección IP.
- Define cuántos bits en la dirección IP se reservan para identificar el nodo y cuántos para identificar las subredes.
- Los bits en 0 indican bits de la dirección IP que identifican los nodos.
- Los bits en 1 indican bits de la dirección IP que identifican las subredes.

## Dentro de cada subred:

- Una dirección reservada de subred.
- Una dirección reservada de broadcast.
- Las demás son direcciones útiles.

## Cálculo de subredes:

- Subredes posibles: $2^n$
- Subredes útiles: $2^n - 2$
- Direcciones IP / subred: $2^n$
- Direcciones de nodo útiles: $2^n – 2$

## Método sencillo para el cálculo de subredes:

1. ¿Cuántas subredes son necesarias?
2. ¿Cuántos nodos se necesitan por subred?
3. ¿Cuáles son los números reservados de subred?
4. ¿Cuáles son las direcciones reservadas de broadcast?
5. ¿Cuál es la primera dirección de nodo válida?
6. ¿Cuál es la última dirección de nodo válida?

## IP Subnet -Zero

- Feature de Cisco IOS que permite utilizar las 2 subredes inutilizables en esquemas tradicionales.
- Subredes útiles: $2^n$

## VLSM

- Solo con protocolos de enrutamiento classless.
- Varía la máscara de subred dentro de la red, en función de la cantidad de nodos.

## CIDR

- Prescinde de los límites de las clases para resumir múltiples rutas en una sola.
- Ventajas:
    - Reduce el tamaño de las tablas de enrutamiento.
    - Limita los requerimientos de RAM y procesamiento de los dispositivos.
    - Mejora la performance de los dispositivos.
    - Aumenta la estabilidad de las tablas de enrutamiento.
- Características del bloque de rutas sumarizadas:
    - Amplitud del rango de redes sumarizadas: potencia de 2.
    - Valor inicial del rango sumarizado: múltiplo de la potencia de 2.

## Conexión al dispositivo Cisco IOS:

- Vías de acceso:
    - Puerto consola.
    - Puerto auxiliar.
    - Puertos virtuales (Telnet – SSH).
    -

## Componentes de hardware de un dispositivo:

- CPU.
- Motherboard.
- Memoria.
    - ROM.
    - RAM.
    - NVRAM.
    - Flash.
    - Disk.

- Interfaces.
    - LAN.
    - WAN.
    - Gestión.

- Fuente de alimentación.
- BUS.
    - Bus del sistema.
    - Bus de CPU.
    -

## ¿Qué se almacena en cada componente de memoria?

- Memoria ROM.
    - POST.
    - Bootstrap.
    - Monitor de ROM.
- Memoria Flash.
    - Imagen de Cisco IOS.
    - CCP.
- Memoria RAM.
    - Archivo de configuración activa.
- Memoria NVRAM.
    - Archivo de configuración de respaldo.
    - Registro de configuración.

## Modos del sistema operativo.

- Modo setup o inicial.
    - Básico.
    - Extendido.
- Modo monitor de ROM. >_
- Modo EXEC.
    - Modo usuario. Router>
    - Modo privilegiado. Router#

## Modo setup

- Se activa automáticamente cuando no se encuentra un archivo de configuración válido en la NVRAM.
- Se invoca con el comando Router(config)#setup
- Se interrumpe con Ctrl+ C

## Modo de configuración global

- Permite acceder a los comandos de configuración de todo el dispositivo.
- Se accede con Router#configure terminal
- Para salir a modo privilegiado Router(config-if)#Ctrl+Z

## Sistema de ayuda.

- Menú de ayuda. ?
- Comandos de edición. Router>terminal editing
- Mensajes de error. % xxx
- Notificaciones de cambios de estado.

## Claves de acceso.

- Acceso a modo usuario.
  - Acceso por consola.
  - Acceso por puerto auxiliar.
  - Acceso por terminal virtual.
- Acceso a modo privilegiado.
  - Clave de acceso. Router(config)#enable password
  - Clave encriptada. Router(config)#enable secret

## Secuencia de arranque.

- Se enciende el dispositivo.
- Ejecuta el POST.
- Carga el bootstrap.
- Carga el Cisco IOS.
- Carga el archivo de configuración.

## Procedimiento de configuración de un router Cisco.

- Configuración de parámetros globales.
  - Nombre del dispositivo y otros parámetros globales.
  - Habilitación del acceso por consola y por terminal virtual.
  - Configuración de clave de acceso al modo privilegiado.
- Configuración de interfaces.
  - Interfaces LAN.
  - Interfaces WAN.
  - Interfaces lógicas.
- Configuración de enrutamiento.
  - Enrutamiento estático.
  - Ruta por defecto.
  - Enrutamiento dinámico.
- Configuración de IPv6.
  - Direccionamiento IPv6 de las interfaces.
  - Enrutamiento IPv6 dinámico.

## Posibles resultados de show interfaces

- Administratively down — interfaz no habilitada.
- down / down — problema de capa física.
- up / down — problema de capa de enlace de datos.
- up / up — interfaz operativa.

## Pruebas de conectividad de la red.

- Ping conectividad de capa 3.
- Traceroute descubrimiento de rutas.
- Telnet conectividad de capa 7.

## Secuencia de inicio de dispositivos IOS.

- Se enciende el dispositivo.
- Ejecuta el POST.
- Carga el bootstrap.
- Lee el registro de configuración.
- Carga la imagen de IOS.
- Carga el archivo de configuración.

## El registro de configuración:

- Registro de 16 bits guardado en la NVRAM.
- Valor por defecto — 0x2102.
- Ingresa al modo monitor de ROM — 0x2100.
- Para recuperación de claves — 0x2142.
- Cambia el registro de configuración — config-register 0x____.
- Verifica el valor del registro — show version.

## Posibles fallas durante el proceso de arranque:

- Comandos boot system incorrectos.
- Valor erróneo del registro de configuración.
- Imagen del Cisco IOS corrompida.
- Falla de hardware.

## Comando para hacer una copia de resguardo de archivos:

- copy [fuente]:[nombre] [destino]:[nombre]

## Procedimiento para la recuperación de claves:

- Encender el equipo.
- Ingresar en modo Monitor de ROM.
- Modificar el registro de configuración.
- Reiniciar el equipo.
- Evitar el modo setup.
- Ingresar al modo privilegiado.
- Recuperar el archivo de configuración desde la NVRAM.
- Modificar las claves.
- Modificar el registro de configuración a su valor original.
- Guardar los cambios.

## Cisco Discovery Protocol (CDP)

- Permite el descubrimiento de la plataforma y los protocolos de capa de red de los dispositivos directamente conectados.
- Propietario de Cisco.
- Protocolo de capa de enlace de datos.
- Soporta diferentes encapsulaciones de capa 2.
- Todas las interfaces son CDP activas por defecto.
- Comandos de monitoreo:
    - show cdp
    - show cdp neighbor
    - show cdp entry
    - show cdp neighbor detail

## Comandos relacionados con el acceso por terminal virtual:

- telnet
- connect
- disconnect
- exit
- clear line
- show sessions
- show users

Switch: dispositivo LAN de capa de enlace de datos basado en hardware basado

en circuitos ASICS:

- Conmuta tramas en función de la MAC de destino.
- Aprende direcciones MAC.
- Soluciona bucles de capa 2.
- Cuando recibe una trama con una dirección destino que desconoce, la reenvía por todos los puertos salvo el puerto de origen.
- Divide dominios de colisión.

## Métodos de conmutación de capa 2:

- Almacenamiento y envío.
- Método de corte.
    - Conmutación rápida.
    - Libre de fragmentos.

## Configuración básica del switch Catalyst 2960X.

- Configuración de claves de acceso.
    - Clave de acceso por terminal virtual.
    - Clave de acceso por consola.
    - Clave de acceso a modo privilegiado.
- Configuración de parámetros globales.
    - Nombre del dispositivo.
    - Dirección IP (en la VLAN de gestión).
    - Default gateway.
- Configuración de interfaces.
    - Half / full dúplex.
    - Velocidad.

## Control de acceso a la red.

- Entrada estática en la tabla de direcciones MAC.
- Seguridad por puerto.
    - Solo en puertos de acceso.
    - Cantidad máxima de direcciones MAC por puerto.
    - Modo de aprendizaje de las direcciones MAC.
    - Acción en caso de violación de la política.

## Optimización de performance de la red.

- Half/full dúplex.
- Velocidad.

## Implementación de redundancia en capa 2:

- Ventajas:
    - Confiabilidad.
    - Eliminación de un único punto de fallo.
- Problemas que genera:
    - Tormentas de broadcast.
    - Copias múltiples de una misma trama.
    - Inestabilidad en las tablas de direcciones MAC.

## Spanning Tree Protocol.

- Protocolo de capa de enlace de datos que permite administrar potenciales bucles en la red, permitiendo que sólo exista una única ruta activa entre dos estaciones.
- Estándar IEEE 802.1D.
- Utiliza BPDUs, que el switch raíz envía cada 2 segundos.
- Bridge ID = Prioridad | MAC.
- Prioridad por defecto: 32768.
- Varias evoluciones:
    - STP – IEEE 802.1D.
    - RSTP – IEEEE 802.1w.
    - MST – IEEE 802.1s.
    - PVST+ - Propietario de Cisco.
    - RPVST+ - Propietario de Cisco.

## Operación de STP:

- Se elige un bridge raíz.
    - Solo un bridge raíz por dominio de broadcast.
    - Todos los puertos del bridge raíz son puertos designados.
- Se elige un puerto raíz en los switches no raíz.
    - Cada switch no raíz tiene un puerto raíz.
    - El puerto raíz es el puerto de menor costo hacia el switch raíz.
    - El costo de los enlaces es función del ancho de banda.
- En cada segmento se elige un puerto designado.
    - Los puertos no designados quedan en estado bloqueado.
- Costo por defecto de los puertos:
    - 10 Mbps:100
    - 100 Mbps: 19
    - 1 Gbps: 4
    - 10 Gbps: 2
- Prioridad por defecto de los puertos: 128.

## Estado de los puertos STP.

- Bloqueado / Blocking.
- Escuchando / Listening.
  Estado transitorio.
- Aprendiendo / Learning.
  Estado transitorio.
- Enviando / Forwarding.
- Tiempo para pasar del estado de bloqueado a enviando: 50 segundos.

## Temporizadores STP.

- Hello time: 2 segundos.
- Forwarding delay: 15 segundos.
- Max Age: 20 segundos.

## Port Fast.

- Solo se aplica en puertos de acceso.
- El puerto inicia en estado forwarding.

## RSTP

- Estados de puertos:
  - Discarding.
  - Learning.
  - Forwarding.
- Roles de puertos:
  - Puerto raíz.
  - Puerto designado.
  - Puerto alternativo.
  - Puerto de backup.

## Operación STP en Catalyst 2960X por defecto.

- PVST+.
- Soportan: PVST+, PVRST+, MSTP.
- Está habilitado en todos los puertos.

## EtherChannel

- Agrupa 2 a 8 enlaces físicos.
- Se comporta como un único enlace para STP.
- Balancea tráfico entre los enlaces físicos.
- 2 protocolos de negociación: PAgP (propietario) y LACP (estándar).

## Administración de la imagen de IOS y el archivo de configuración.

- Es el sistema de archivos de IOS (igual a los routers).

## Borrar la configuración.

- Comando básico: erase startup-config.
- Archivo en la memoria flash: delete flash:config.txt
- Base de datos de VLANs: delete flash:vlan.dat

## VLANs.

- Cada VLAN constituye un dominio de broadcast diferente.
- La comunicación entre VLANs requiere del ruteo a través de un dispositivo de capa de red.

## Beneficios de las VLANs:

- Reducen el costo de administración.
- Controlan el tráfico de broadcast.
- Mejoran la seguridad de la red.
- Permiten agrupar de manera lógica a los usuarios.

## Modos de membrecía VLAN.

- Estática.
- Dinámica.

## Tipos de puertos o enlaces.

- Puertos de acceso.
- Puertos troncales. Enlace punto a punto que transporta múltiples VLANs que permiten interconectar switches optimizando el uso de los enlaces disponibles.

## Dynamic Trunk Protocol (DTP).

- Negocia dinámicamente el establecimiento de enlaces troncales.
- Los puertos pueden estar en 5 estados:
    - Dynamic auto.
    - Dynamic desirable.
    - Trunk.
    - Access.
    - Nonegotiate.

## Protocolos para la marcación de tramas sobre enlaces troncales:

- ISL.
    - Propietario Cisco
- IEEE 802.1Q.
    - Estándar de la IEEE.
    - Agrega un campo TAG de 4 bytes en el encabezado de la trama.
    - Puede identificar hasta 4096 VLANs.
    - Implementa una VLAN nativa.

## VLAN Trunk Protocol (VTP)

- Protocolo propietario de Cisco.
- Permite compartir información de la base de datos de VLANs entre switches que pertenecen a un mismo dominio de administración que se comunican a través de enlaces troncales.
- Utiliza tramas multicast de capa 2 para agregar, borrar y modificar las VLANs.
- Información de las publicaciones VTP:
    - Nombre del dominio administrativo.
    - Número de revisión.
    - Clave, cuando se activó el uso de autenticación.
    - Identidad del dispositivo.
- Modos VTP:
    - Servidor (modo por defecto en Catalyst).
    - Cliente
    - Transparente.

## Secuencia de configuración de VLANs

- Verificar la configuración de VTP.
- Crear las VLANs.
- Asignar cada puerto a la VLAN correspondiente.
- Verificar la asignación de puertos.
- Activar los puertos troncales.
- Verificar la configuración de los troncales.

## Configuración de router on stick.

- Permite enrutar tráfico entre VLANs utilizando un router.
- Requerimientos:
    - Mapear VLANs a subredes IP.
    - Llegar con todas las VLANs hasta el router (troncal).
- Configuración.
    - Troncal hasta el router.
    - Crear una subinterfaz para cada VLAN.
    - Asignar encapsulación y asociar la subinterfaz a la VLAN.
    - Configurar dirección IP y máscara de subred.

Enrutamiento: Proceso implementado por dispositivos de capa 3 para descubrir la ruta que ha de utilizar un paquete IP para alcanzar una red de destino.

## Información requerida para poder enrutar:

- Identificador de la red de destino.
- Dispositivo vecino.
- Rutas posibles a las redes remotas.
- Mejor ruta a cada red remota.

## Las tablas de enrutamiento se construyen:

- Dinámicamente a partir de otros dispositivos de enrutamiento.
- Estáticamente a través de la intervención del Administrador.

## Funciones del router:

- Determinar las rutas.
- Reenviar los paquetes.

Tabla de enrutamiento: conjunto ordenado de información de rutas para alcanzar diferentes redes de destino.

## Generación de la tabla de enrutamiento:

- Redes directamente conectadas.
  Las origina Cisco IOS.
- Rutas estáticas.
  Ingresadas manualmente.
- Rutas dinámicas.
  Generadas automáticamente.
- Ruta por defecto.
  Entrada que permite reenviar todo tráfico para el que no se encuentra una ruta explícita en la tabla de enrutamiento.

## Criterio para la selección de la mejor ruta:

- La menor distancia administrativa.
- A igual distancia administrativa, la menor métrica.
- A igual métrica, la de prefijo más largo.
- A igual métrica se balancea tráfico.

## La métrica:

- Es el parámetro que representa la distancia existente entre el dispositivo y la red de destino.
- Menor métrica = Mejor ruta.

## Distancia Administrativa

- Calificación de la calidad o confiabilidad de una fuente de información de enrutamiento.
- Valor entre 0 y 255.
- Menor distancia administrativa = Mejor ruta.

## Enrutamiento estático.

- Puede ser indicado cuando:
  - Se trata de una red pequeña.
  - Está conectada a Internet utilizando un único service provider.
  - Se trata de un modelo hub-and-spoke.
- No requiere procesamiento ni ancho de banda.
- Exigen una intervención mucho mayor del Administrador.
- Comando de configuración ip route
  ipv6 route

- En IPv6 se requiere activar antes el enrutamiento IPv6: ipv6 unicast-routing
- Monitoreo de rutas sh ip route

## Ruta por defecto

- Ruta utilizada para enrutar paquetes que tienen como destino una dirección perteneciente a una red para la cual no hay una ruta específica en la tabla de enrutamiento.
- ip route 0.0.0.0 0.0.0.0 x.x.x.x
  ipv6 route ::/0 x.x.x.x.x.x.x.x
- ip default-network x.x.x.x
- Redistribución de rutas estáticas redistribute static

## Protocolos de enrutamiento.

- Enrutamiento Interior.
  - RIPv1 y 2.
  - EIGRP.
  - OSPF.
  - IS-IS.
- Enrutamiento Exterior.
  - BGPv4.
- Sistema autónomo: conjunto de redes o dispositivos de enrutamiento que
- operan bajo una administración común.
  - EIGRP.
  - IS-IS.
  - BGPv4.

## Protocolos de enrutamiento por vector distancia:

- Implementan el algoritmo de Bellman-Ford para elegir la mejor ruta.
- Visualizan la red sólo desde la perspectiva de los vecinos.
- Realizan actualizaciones enviando la tabla de enrutamiento completa.
- Actualizaciones periódicas.
- Convergencia lenta.
- Requieren mucho ancho de banda.
- Sencillos para el diseño y la configuración.
- RIPv1 y 2, y EIGRP.

## Mecanismos de los protocolos de vector distancia para reparar bucles de enrutamiento:

- Cuenta al infinito.
- Horizonte dividido.
- Ruta envenenada.
- Temporizadores de espera.
- Actualizaciones desencadenadas.

## Protocolos de enrutamiento por estado de enlace:

- Implementan el algoritmo de Dijkstra o SPF.
- Cada dispositivo tiene una visión completa de la topología de la red.
- Transmiten solo actualizaciones del estado de los enlaces.
- Los eventos desencadenan una notificación.
- Convergencia rápida.
- Requieren poco ancho de banda, pero mucho procesamiento en los dispositivos.
- Son más complejos en cuanto a diseño y configuración.
- IS-IS y OSPF.

## EIGRP

- Protocolo de enrutamiento por vector distancia avanzado.
- Propietario de Cisco.
- Algoritmo de selección de rutas: DUAL.
- Soporta VLSM y sumarización de rutas.
- No sumariza rutas por defecto.
- Soporta autenticación con MD5.
- Soporta múltiples protocolos enrutados.
- Métrica compuesta (delay y ancho de bando por defecto) de 32 bits.
- Balancea tráfico entre rutas de diferente métrica (hasta 32).
- Número máximo de saltos: 224. 100 por defecto.
- Distancia administrativa 90.
- Distingue rutas internas y externas.
- Requiere la configuración de un ID de sistema autónomo.
- Utiliza actualizaciones parciales, incrementales y limitadas.
- Mantiene tablas de información:
    - Tabla de vecinos.
    - Tabla topológica.

## OSPF

- Protocolo de enrutamiento por estado de enlace estándar.
- Soporta VLSM y CIDR.
- Métrica: costo (por defecto considera el ancho de banda).
- Balancea tráfico entre rutas de igual métrica (hasta 16).
- Utiliza el algoritmo de Dijkstra.
- Distancia administrativa: 110
- Período de actualización
    - 10 segundos en redes multiacceso y punto a punto.
    - 30 segundos en redes NBMA.
- Sumarización de rutas manual.
- Soporta autenticación con texto plano o MD5.
- Requiere diseño jerárquico de la red.
- Intercambia paquetes LSA para intercambiar información sobre el estado de los enlaces.
- Hay varios tipos de LSA:
    - Tipo 1 – LSA de router.
    - Tipo 2 – LSA de red.
    - Tipo 3 – LSA sumario.
- Define un router ID siguiendo una secuencia:
    - Router ID configurado.
    - Dirección IP más alta de las interfaces de loopback.
    - Dirección IP más alta de las interfaces físicas activas.
- Segmenta el dominio de enrutamiento en áreas:
    - Requiere la definición de un ID de área para la configuración.
    - La red puede estas formada por múltiples áreas.
    - El área 0 es el área de backbone.
- Mantiene tablas de información:
    - Tabla de adyacencias.
    - Tabla topológica.
- Condiciones para establecer adyacencia entre 2 dispositivos:
    - Ambas interfaces deben estar en la misma subred.
    - Ambas interfaces deben utilizar la misma máscara de subred.
    - Ambas interfaces deben pertenecer a la misma área OSPF.
    - Ambos dispositivos deben utilizar los mismos valores de temporizadores.
- En redes multiacceso, OSPF elige:
    - Router designado (DR).
    - Router designado de respaldo (BDR).
- OSPFv2 enruta redes IPv4.
- OSPFv3 enruta redes IPv6.

## Comandos de monitoreo:

- show ip route.
- show ip protocols.

## Interfaces pasivas.

- No se envían actualizaciones o paquetes hello.
- Se ignoran las actualizaciones y paquetes hello que se reciben.
- Es posible pasivar las interfaces por defecto.

## Procesamiento de la decisión de reenvío del tráfico.

- Process switching.
- Fast switching.
- Cisco Express Forwarding (CEF).

## Redundancia en el primer salto.

- Requerimientos:
- Todas las terminales utilizan la misma IP de default gateway.
- Los gateways comparten una única IP virtual.
- Se intercambian mensajes para negociar cuál es el router activo.

## HSRP – Hot Standby Router Protocol

- Propietario de Cisco.
- Proporciona redundancia activo/standby.
- Puede determinarse cuál será el router activo utilizando prioridad.
- No brinda balanceo de tráfico.
- 1 IP virtual / 1 MAC virtual (0000.0c07.acxx).
- Permite generar varios grupos HSRP para distribuir tráfico.

## GLBP – Gateway Load Balancing Protocol

- Propietario de Cisco.
- Proporciona redundancia activo/activo.
- Elige dentro del grupo un AVG (Active Virtual Gateway).
- Brinda balanceo de tráfico.
- 1 IP virtual / múltiples MAC virtuales.

## Asignación de configuración IP de terminales:

- Configuración estática (IPv4/IPv6).
- Configuración estática utilizando EUI-64 (IPv6).
- Configuración automática utilizando autoconfiguración stateless (IPv6).
- Configuración automática utilizando DHCP(IPv4/IPv6).

## DHCPv4.

- 3 formas diferentes:
    - Asignación dinámica.
    - Asignación automática.
    - Asignación estática.
- Procedimiento de asignación:
    - DHCP Discovery.
    - DHCP Offer.
    - DHCP Request.
    - DHCP Acknowledgement.
- Configuración del servicio DHCPv4 en IOS:
    - Definición del pool de direcciones a asignar.
    - Definición de parámetros opcionales de la configuración.
    - Definición del período de asignación.

## DHCP Relay.

- Permite acceder a servidores DHCP que residen en redes o subredes diferentes a la del cliente.
- IOS permite que los dispositivos de red operen como DHCP Relay.
- Se define utilizando el comando ip helper-address.

## ICMP - Internet Control Message Protocol.

- Protocolo de la capa de Internet de TCP/IP.
- Permite el reporte de errores o limitaciones en las comunicaciones IP.
- En redes IPv6 se utiliza ICMPv6.
- Hay 2 tipos de mensajes:
    - Mensajes de error.
    - Mensajes de control.
- Programas que utilizan ICMP:
    - ping
    - trace route

## DNS - Domain Name System.

- Protocolo de capa de aplicación.
- Utiliza TCP y UDP puerto 53.
- Utiliza una estructura jerárquica de dominios de red independiente de la propia del direccionamiento IP.
    - El nivel más alto de la jerarquía es el de los dominios nacionales o geográficos (.ar, .cl, etc.).
- Nombres DNS: conjunto de etiquetas alfanuméricas separadas por puntos.
- Implementación de DNS en IPv6 requiere:
    - Actualizar clientes y servidor DNS.
    - Actualizar cliente y servidor para operar sobre IPv6.

## Listas de Control de Acceso.

- Es una enumeración secuencial de indicaciones de permiso y/o prohibición para determinadas direcciones y/o protocolos de capa superior.
- Reglas de funcionamiento:
    - Una sola ACL por interfaz, por sentido, por protocolo.
    - Cada lista se identifica con un ID.
    - Si es numérico además indica el tipo de lista de acceso.
    - Los paquetes son comparados secuencialmente con cada sentencia de la lista de acceso.
    - Si cumplen con una, se ejecuta la sentencia y no continúa el análisis.
    - Hay un deny any implícito al final de toda lista de acceso.
    - Los filtros de tráfico saliente no afectan el tráfico originado en el mismo router.

## Tipos de listas de acceso IP:

- Estándar Numeradas. 1 – 99 y 1300 – 1999
- Extendidas Numeradas. 100 – 199 y 2000 – 2699
- Nombradas.
- Tipos especiales:
    - Listas de acceso dinámicas.
    - Listas de accesos reflexivas.
    - Listas de acceso por tiempo.
- Máscara de wildcard.
    - El dígito en 0 indica una posición que debe ser comprobada.
    - El dígito en 1 indica una posición que no debe ser comprobada.
    - Siempre está asociada a una dirección IP de referencia.
    - Casos especiales:
        - Cuando se desea filtrar una red o subred completa, la máscara de wildcard es el complemento de la máscara de subred.
        - host = 0.0.0.0

        - any = 255.255.255.255
- Procedimiento de configuración:
    - Crear la lista de acceso.
    - Asociar la lista de acceso a una interfaz.
- Aplicación a los puertos virtuales:
- Solo se utilizan listas de acceso numeradas.
- Se aplican al puerto virtual con el comando access-class.
- Tips
    - Cuando se agrega una sentencia, si no se indica número de secuencia, se agrega al final de la lista.
    - Toda lista de acceso debe incluir al menos una sentencia permit.
    - Las listas de acceso estándar se aplican lo más cerca posible del destino.
    - Las listas de acceso extendidas se aplican lo más cerca posible del origen.

## NAT - Network Address Translation.

- Procedimiento estándar que modifica la dirección IP de origen traduciéndola por una dirección IP compatible con la red de destino.
- Terminología:
    - Red inside.
    - Red outside.
    - Dirección inside local.
    - Dirección inside global.
    - Dirección outside local.
    - Dirección outside global.
- Modalidades de NAT:
    - NAT estático.
    - NAT dinámico.
    - NAT overload o PAT.
- Configuración de NAT:
    - Identificación de la interfaz conectada a la red inside.
    - Identificación de la interfaz conectada a la red outside.
    - Definición de los parámetros de traducción.

## Amenazas a la seguridad de la red.

- Amenazas internas.
- Amenazas externas.

## Requerimientos básicos de seguridad:

- Confidencialidad.
    - Autenticación.
    - Cifrado.
- Integridad.
- Disponibilidad.

## Best practices de seguridad:

- Implementar management out of band.
- Utilizar protocolos encriptados (SSH y HTTPS).
- Implementar cuentas de usuario con diferentes niveles de privilegio.
- Implementar gestión centralizada de usuarios.
- Resguardar el registro de eventos en servidores dedicados.
- Utilizar claves cifradas.
- Utilizar SNMPv3.
- Apagar los puertos del switch que no están en uso.
- Cambiar la VLAN nativa por defecto en los enlaces troncales.

## SSH.

- Brinda un servicio de acceso a la CLI de los dispositivos asegurado con autenticación y cifrado.
- Su implementación requiere:
    - Habilitar los dispositivos de red como servidores SSH.
    - Programas emuladores de terminal con soporte SSH.

## Registro de eventos.

- Syslog es un protocolo de capa de aplicación.
- Los mensajes pueden enviarse a:
    - Consola.
    - Sesiones Telnet o SSH.
    - Servidor de Syslog.
    - Buffer de memoria.
- Diferentes niveles de severidad:
    - 0 - Emergency
    - 1- Alert
    - 2 - Critical
    - 3 - Error
    - 4 - Warning
    - 5 - Notification
    - 6 - Informational
    - 7 - Debugging

## NTP - Network Time Protocol.

- Permite que múltiples dispositivos utilicen un único reloj como fuente de sincronía.

## SNMP - Simple Network Management Protocol.

- Arquitectura:
  - SNMP Manager.
  - SNMP Agent.
  - MIB.
- Tipos de mensajes:
  - GET.
  - SET.
  - Trap.
- Versiones:
  - SNMPv1.
  - SNMPv2c.
  - SNMPv3

## NetFlow.

- Aplicación embebida en IOS para relevar estadísticas de tráfico en la red.
- Releva estadística de comunicaciones utilizando el concepto de flujo (flow).
- Flujo: Stream unidireccional de paquetes entre un sistema de origen y un sistema destino específicos.
- Arquitectura:
  - Interfaz de un dispositivo con NetFlow habilitado.
  - NetFlow collector

## WAN: servicio de conectividad en distancias amplias y con ancho de banda limitado.

- Operan a nivel de capa 1 y capa 2 del modelo OSI.

## Terminología WAN:

- Punto de demarcación.
- Bucle local.
- POP – Punto de presencia.
- CO – Oficina Central.
- CPE – conecta al bucle local del proveedor de servicio.
    - CSU/DSU.
    - Módem.
- DTE – Dispositivo de salida de la LAN (router).
- DCE – Proveedor de servicio.

## Tipos de conexión WAN:

- Líneas dedicadas.
- Redes de paquetes conmutados.
    - Frame Relay.
    - X.25.
- Redes de celdas conmutadas.
    - ATM.
- Redes Ethernet WAN.
    - EoMPLS.
    - MetroE.
    - VPLS.
- MPLS.
    - MPLS VPN.
- Redes de acceso a Internet.
    - Dial up asincrónico.
    - ISDN.
    - xDSL
    - Cablemódem.

## Interfaces físicas WAN:

- Serial asincrónica.
- Serial sincrónica.
    - DB-60.
    - Smart-Serial.

## Protocolos de encapsulación WAN:

- HDLC.
    - Protocolo propietario de Cisco.
    - No puede utilizarse para interconexión con dispositivos de otros fabricantes.
    - Opera sobre enlaces seriales sincrónicos.
    - No proporciona servicios de autenticación u otros.
    - Opción por defecto en las interfaces seriales.
- PPP.
    - Protocolo estándar
    - Opera sobre enlaces seriales sincrónicos y asincrónicos.
    - LCP – Para la negociación del enlace.
    - NCP – Para la negociación de los protocolos de capa de red.
    - HDLC – Para el transporte de datos.
    - Múltiples opciones de operación con LCP:
        - Autenticación: PAP / CHAP
        - Compresión: Stacker / Predictor.
        - Detección de errores: Quality / Magic Number.
        - Multilink.
    - Etapas del establecimiento de una sesión PPP:
        - Establecimiento de la conexión. (LCP)
        - Autenticación (opcional). (LCP)
        - Negociación del protocolo de red. (NCP)
        - Transferencia de datos. (HDLC)
        - Fase de cierre de la sesión. (LCP)

- PPPoE.
    - Permite utilizar PPP sobre redes de medio compartido como Ethernet.
    - Utilizar una interfaz virtual asociada a la interfaz física.
    - La interfaz virtual encapsula PPP.
    - La interfaz física encapsula Ethernet.
    - Requiere un cliente PPPoE.

## QoS:

- Modelos de calidad de servicio
  - Best Effort
    No se implementan políticas de QoS
  - Integrated Services (IntServ) Resource Reservation Protocol (RSVP)
    Se usa para reservar ancho de banda perflow en todos los nodos en una ruta
  - Differentiated Services (DiffServ)
    Los paquetes se clasifican y marcan individualmente; las decisiones de política se toman de forma independiente por cada nodo en una ruta
- Layer 2 QoS Markings
  - Ethernet — Class of Service (CoS) — 3-bit 802.1p field in 802.1Q header
  - Frame Relay — Discard Eligibility (DE) — 1-bit drop eligibility flag
  - ATM — Cell Loss Priority (CLP) — 1-bit drop eligibility flag
  - MPLS — Traffic Class (TC) — 3-bit field compatible with 802.1p
- IP QoS Markings
  - IP Precedence
    Los primeros tres bits del campo IP TOS; limitado a 8 clases de tráfico
  - Differentiated Services Code Point (DSCP)
    Los primeros seis bits de IP TOS se evalúan para proporcionar más granularidad en la clasificación; compatible con versiones anteriores con Precedencia de IP
- Terminología
  - Per-Hop Behavior (PHB)
    La acción individual de QoS realizada en cada nodo DiffServ independiente
  - Trust Boundary
    Más allá de esto, las marcas entrantes de QoS no son de confianza
  - Tail Drop
    Se produce cuando se descarta un paquete porque una cola está llena
  - Policing
    Impone un techo artificial sobre la cantidad de ancho de banda que puede ser consumado; el tráfico que excede la tasa se reclasifica o se descarta
  - Shaping
    Similar a policing, pero almacena el exceso de tráfico; hace un uso más eficiente del ancho de banda, pero introduce un retraso
  - TCP Synchronization
    Los flujos se ajustan a los tamaños de las ventanas TCP en sincronía, haciendo un uso eficiente de un enlace
- Comportamientos de DSCP Per-Hop
  - Class Selector (CS) " Compatible con versiones anteriores con valores de precedencia de IP
  - Assured Forwarding (AF) " Cuatro clases con preferencias variables de drop
  - Expedited Forwarding (EF) " Colas prioritarias para el tráfico sensible al retraso

- Precedence/DSCP
  - 

| | Binary | DSCP | Prec. |
|---|---|---|---|
| **56** | 111000 | Reserved | 7 |
| **48** | 110000 | Reserved | 6 |
| **46** | 101110 | EF | 5 |
| **32** | 100000 | CS4 | 4 |
| **34** | 100010 | AF41 | |
| **36** | 100100 | AF42 | |
| **38** | 100110 | AF43 | |
| **24** | 011000 | CS3 | 3 |
| **26** | 011010 | AF31 | |
| **28** | 011100 | AF32 | |
| **30** | 011110 | AF33 | |
| **16** | 010000 | CS2 | 2 |
| **18** | 010010 | AF21 | |
| **20** | 010100 | AF22 | |
| **22** | 010110 | AF23 | |
| **8** | 001000 | CS1 | 1 |
| **10** | 001010 | AF11 | |
| **12** | 001100 | AF12 | |
| **14** | 001110 | AF13 | |
| **0** | 000000 | BE | 0 |

- Congestion Avoidance
  - Random Early Detection (RED)
  - Los paquetes se eliminan aleatoriamente antes de que una cola esté llena para evitar que la cola se caiga; mitiga la sincronización TCP
  - Weighted RED (WRED)
    ROJO con la capacidad adicional de reconocer el tráfico priorizado basado en su marcado
  - Class-Based WRED (CBWRED)
    WRED empleado dentro de una cola WFQ basada en la clase (CBWFQ)