Resumen Router Cisco

1. ¿Qué es el Router?

- Son computadoras que **envían paquetes a través de redes de datos** → Seleccionan **la mejor ruta** para la transmisión de paquetes → Actúan en la capa 3 del modelo OSI, pero funcionan en las capas 1 y 2 tambíen.
- Tienen dos conexiones → **WAN** y **LAN**.
- Examina la dirección IP de destino y, con la **tabla de enrutamiento**, determina la mejor ruta.

1.1 Componentes

CPU	Ejecuta instrucciones
RAM	Contiene la copia del archivo de configuración Almacena tabla de enrutamiento El contenido se pierde al apagar el router
ROM	Contiene el software de diagnóstico Contiene el programa bootstrap
NVRAM	Almacena la configuración de inicio → IP
FLASH	Contiene el sistema operativo
Interfaces	Hay distintas interfaces (ethernet, seriales, administración)

1.2 Inicio del Router

1. **Realizar un POST** → ROM → POST.
2. **Ejecuta el cargador bootstrap** → ROM → Bootstrap.
3. **Localiza el IOS** → FLASH → Ubica el SO.
4. **Carga el IOS** → Servidor TFTP → Carga el SO.
5. **Localiza el archivo de configuración** → NVRAM.
6. **Ejecuta el archivo** → Consola.

- Para verificar el proceso de inicio del router → **Show versión**.

1.3 Interfaces

- Es un **conector físico** que permite que el router envíe o reciba paquetes.
- Se conecta a una red diferente.
- **LAN** →
  - Conectan el router con una red LAN.
  - Dirección MAC de capa 2.
  - Se le asigna IP de capa 3.
  - Conector RJ45.
- **WAN** →
  - Conectar el router con una red externa que unen redes LAN.
  - Es posible utilizar dirección de capa 2.
  - Usan IP de capa 3.

1.4 Tabla de Direcciones

- Tienen la siguiente topología:
  - **Nombre del dispositivo**.
  - **Interfaces usadas**.
  - **Direcciones IP**.
  - **Gateway**.

1.5 Configuración Básica

- Contiene la siguiente información:
  - **Nombre del router** → Hostname.
  - **Título** → Banner motd #texto#.
  - **Contraseñas** → Service password-encryption.
  - **Configuración de interfaces** → Int (interfaz):
    - Tipo.
    - Dirección IP.
    - Máscara de subred.
    - Cuando tiene DCE → Clock rate.
- Tras la configuración básica → **Verificar**.
- **Guardar** los cambios del router.

1.6 Rutas Estáticas en la Tabla de Enrutamiento

- Incluyen:
  - **Dirección Red**.
  - **Máscara Subred**.
  - **Dirección IP** del siguiente router.
- Se indican con el **código S**.
- Deben tener conectadas redes directamente usadas para conectar redes remotas.

1.7 Protocolos de Enrutamiento Dinámico

- Se usan para **agregar redes remotas** a una tabla de enrutamiento.
- Se usan para **detectar redes**.
- Se usan para la **actualización y mantenimiento** de las tablas de enrutamiento.
- Comparten información de enrutamiento entre routers.
- **RIP** y **OSPF** son protocolos de enrutamiento dinámico.

1.8 Función de Conmutación

- Es el proceso que usa un router para **conmutar un paquete** de una interfaz de entrada a una interfaz de salida en el mismo router.
- Al recibir un paquete
  - Se **eliminan** los encabezados de **capa 2**.
  - Se **analiza** la dirección IP de destino ubicada en el encabezado de **capa 3**.
  - Se vuelve a **encapsular el paquete de capa 3** en una **trama de capa 2**.
  - Se reenvía la trama a través de la interfaz de salida.

2. Protocolo DHCP

- **D**ynamic **H**ost **C**onfiguration **P**rotocol → **Protocolo servidor/cliente** que permite a los clientes de una red IP, obtener sus parámetros de configuración automáticamente.

2.1 Pasos para Configurar

1. **Definir un ámbito** → ip dhcp pool nombre.
2. **Definir conjunto** de direcciones → network direcciónRed máscaraSubred.
3. **Excluir** direcciones IP **utilizadas** → ip dhcp excluded-address direccionIP.
4. Establecer valores de **parámetros necesarios**.

3. Configuración PPP

- Es un protocolo de capa 2, utilizados en conexiones WAN, que ofrece autenticación, comprensión y detección de errores.
- Para ello se utiliza el comando encapsulation ppp.
- Puede tener 2 tipos de autenticaciones
  - **PAP** → Password Authentication Protocol → Envía credenciales en texto plano, **menos seguro**.
  - **CHAP** → Challenge Handshake Authentication Protocol → Cifrado de mayor seguridad, **más seguro**.

4. Enrutamiento Dinámico

	Protocolos de Gateway Interior				Protocolos de Gateway Exterior
	Vector Distancia		Estado de Enlace		Vector Ruta
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP IPv6	OSPFv3	IS-IS IPv6	BGP-MP

- **Vector Distancia** → Su **métrica** se basa en lo que se le llama "**Número de Saltos**" → Cantidad de routers por los que tiene que pasar el paquete para llegar a la red destino.
- **Estado de Enlace** → Su **métrica** se basa en el **retardo**, **ancho de banda**, **carga** y **confiabilidad** de los distintos enlaces para llegar a un destino en base a esos conceptos, el protocolo decide una ruta u otra.

4.1 Propósitos

- **Facilitan el intercambio** de información de enrutamiento entre los routers.
- **Descubrir** redes remotas.
- Mantener la información **actualizada**.
- **Escoger** el **mejor** camino hacia las redes de destino.

4.2 Componentes Principales

- **Estructura de Datos** → Tablas de enrutamiento → RAM.
- **Mensajes** → Descubrir routers vecinos, intercambiar información, etc.
- **Algoritmo** → Facilitan la información de routing.

4.3 Ventajas y Desventajas del Routing Dinámico

Ventajas	Desventajas
Adecuado para cualquier topología	Implementación compleja
Independiente del tamaño de la red	Menos seguro que la estática
Adapta automáticamente la topología para enrutar el tráfico	La ruta depende de la topología actual
	Requiere CPU, RAM y ancho de banda

4.4 Ventajas y Desventajas del Routing Estático

Ventajas	Desventajas
Implementación fácil	Topologías simples
Muy seguro	Mayor complejidad con tamaños de red mayores
La ruta es siempre la misma	Requiere intervención manual para enrutar el tráfico de nuevo
No requiere CPU ni RAM	

5. Protocolo OSPF

- **O**pen **S**hortest **P**ath **F**irst → **Protocolo de enrutamiento de estado de enlace**, ampliamente utilizado en redes IP.
- Publicado en 1989.
- Usa algoritmo SPF para calcular las rutas más cortas basándose en una métrica llamada **costo** → 10^8 / ancho de banda (100 Mbps).
- La **distancia administrativa** es de 110.

5.1 Componentes Principales

5.1.1 Estructura de Datos

- Mantienen una base de datos de estado de enlace → **LSDB** → contiene información sobre la topología de la red.
- Los datos de intercambian → **LSA** → Link State Advertisements.

5.1.2 Tipos de Paquetes

- **Saludo** → Detectan vecinos y establecen adyacencias.
- **DBD** → Controla la sincronización de la base de datos entre routers.
- **LSR** → Solicita registros de estado de enlace de router a router.
- **LSU** → Envía los registros de estado de enlace solicitados.
- **LSAck** → Reconoce los demás tipos de paquetes.

5.1.3 Encapsulación

- Los paquetes se encapsulan en IP con el protocolo número **89**.

5.2 Selección del DR y BDR

- En redes de acceso múltiple, se selecciona un **Router Designado** (DR) y un **Router Designado de Respaldo** (BDR) para reducir el tráfico → Incluido en los paquetes Saludo.

6. OSPF vs RIP

OSPF	RIP
Protocolo de estado de Enlace → Detección inicial o cambios en la red	Protocolo de Vector Distancia → Broadcast Periódicos
Más rápida → convergencia y escalabilidad	Más lenta → convergencia
Utiliza concepto de áreas	Número de saltos → 15 máx
Cuanto mayor sea la velocidad, menor costo de OSPF tendrá en enlace	Necesita routers con menos memoria y potencia de procesamiento
Selecciona la ruta más rápida y no tiene bucles de árbol SPF	
Distancia administrativa de 110	Distancia administrativa de 120
Autentifica y encripta la información de enrutamiento	
No usa TCP ni UDP → IP → Protocolo 89	

7. Protocolo BGP

- **B**order **G**ateway **P**rotocol → Protocolo mediante el cual **se intercambia información de encaminamiento o ruteo entre sistemas autónomos** → Proveedores de servicio.
- Este intercambio de información se realiza entre los routers externos de cada sistema autónomo, los cuales deben soportar BGP.
- Garantiza una elección de rutas **libres de bucles**.
- Admite encaminamiento entre dominios sin clase (**CIDR**) y agregado de rutas.
- **No utiliza métricas** como números de saltos, ancho de banda o retardo.
- Toma decisiones de encaminamiento basándose en políticas de red o reglas que utilizan varios atributos de ruta BGP

8. Protocolo ARP (Capa de Enlace)

- Protocolo de capa de enlace de datos → **Encuentra la dirección MAC** que corresponde a una determinada dirección IP.
- **Envía paquete ARP request** a la dirección de difusión de la red que contiene la dirección IP por la que pregunta → La máquina responde con **ARP replay**.
- Mantiene un caché con las direcciones traducidas para reducir el retardo.

9. Protocolo ICMP (Capa de Red)

- **I**nternet **C**ontrol **M**essage **P**rotocol → Protocolo de Mensajes de Control de Internet → **Subprotocolo de control** y **notificación** de errores del Protocolo IP → **Envía mensajes de error** indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.
- No se utiliza directamente por las aplicaciones de usuario en la red.
- **Tiempo de Vida → TTL** → Concepto usado en redes de computadores para indicar por cuantos nodos puede pasar un paquete antes de ser descartado por la red → **Es reducido en cada salto**.

10. Protocolo TCP (Capa de Transporte)

- Tiene 3 etapas conocidas como **Handshake**:
  - **Establecimiento de Conexión** → Se configuran algunos parámetros como el número de secuencia de la conexión para asegurar la entrega ordenada de los datos.
  - **Transferencia de datos**.
  - **Fin de la Conexión**.

11. MTU

- **M**aximum **T**ransmission **U**nit → **Tamaño máximo** de un paquete (**PDU**) que puede enviarse a través de una red sin dividirse en partes más pequeñas.

11.1 Características

- **Fragmentación** → Si un paquete excede el MTU, se **fragmenta** en unidades más pequeñas → Reduce el rendimiento y aumenta la sobrecarga.
- **Estándares**:
  - **Ethernet** → 1500 bytes.
  - **PPP** → 1492 bytes.
- **Configuración** → El valor MTU puede ajustarse manualmente o mediante **PMTUD**, que detecta automáticamente el tamaño óptimo para evitar fragmentación

11.2 Comparativa Windows y Linux

Aspectos	**Linux**	**Windows**
Modificación del MTU	ip o ipconfig	netsh
Comandos Principales	sudo IP link set dev <interfaz> mtu <valor>	netsh interface ipv4 set subinterface “<nombre> mtu=<valor> store=persistent
Verificación del Valor	ip link show	netsh interface ipv4 show subinterfaces
Flexibilidad	Más opciones disponibles para ajustes avanzados o scripting	Menos opciones directas Requiere herramientas externas
Soporte Automático	Compatible con PMTUD	Soporta PMTUD

12. Medios de Transmisión

- Las LAN son sistemas de comunicación entre ordenadores en áreas limitadas → Utilizan medios guiados (**cables**) o no guiados (**inalámbricos**).

12.1 Medios de Transmisión Guiados

- **Par sin Trenzar**
  - Dos hilos de cobre paralelos con aislamiento plástico.
  - Usado en telefonía → RJ-11.
  - Poca protección a interferencias.
  - Es semidúplex.
- **Par Trenzado**
  - Ocho hilos trenzados en pares para reducir interferencias (**blanco-azul/azul, blanco-naranja/naranja, blanco-verde/verde, blanco-marrón/marrón**)
  - Clasificación en categorías (1 a 7).
  - Tipos
    - UTP → No apantallado, económico y fácil de instalar.
    - STP → Apantallado, reduce interferencias, más complejo y costoso.
    - FTP → Híbrido con blindaje metálico.
  - No recomendado para largas distancias o alta seguridad.
- **Cable Coaxial**
  - Mejor blindaje que el par trenzado, mayor velocidad y distancia.
  - Tipos
    - Banda base → Transmisión digital.
    - Banda ancha → Transmisión analógica.
- **Fibra Óptica**
  - Transmite datos mediante pulsos de luz modulados en un núcleo de vidrio o plástico.
  - Tipos
    - Monomodo → Luz en línea recta.
    - Multimodo → Reflexión interna.
    - Multimodo de Índice Gradual → Refracción gradual.
  - Ventajas → Alta velocidad, baja atenuación y seguridad frente a interferencias.
  - Desventajas → Alto costo y complejidad en instalación.

12.2 Medios de Transmisión no Guiados

- **Ondas de Radio**
  - Propagación Multidireccional → Atraviesas materiales sólidos.
  - Usadas en Tecnologías → WiFi y Bluetooth.
- **Microondas**
  - Ondas electromagnéticas que viajan en línea recta → Requiere alineación entre emisor y receptor.
  - Limitadas por la curvatura terrestre → Máx 80km entre repetidores.
- **Ondas Infrarrojas**
  - Direccionales → No atraviesan objetos sólidos → Transmisiones cortas y portátiles.
- **Ondas de Luz (láser)**
  - Unidireccionales → Usadas para conectar edificios cercanos mediante emisores láser y fotodetectores.

12.3 Comparativa

Características	Coaxial Grueso/Fino	UTP	STP/FTP
Velocidad Máx.	10 Mbps / 1 Gbps	Hasta 100 Mbps	Hasta 1 Gbps
Longitud Máx.	500 m / 200 m	Hasta 100 m	Hasta 100 m
Inmunidad a Interfer	Muy buena / Regular	Regular - Mala	Buena
Flexibilidad	Baja / Media	Alta	Media
Coste	Alto / Bajo	Muy bajo	Bajo

13. Cableado Estructurado

- **Organiza** la instalación de cableado de comunicaciones en edificios.
- Abarca **aplicaciones** como voz, datos y megafonía.
- **Confiabilidad** → Garantía de desempeño hasta 20 años.
- **Modularidad** → Permite crecimiento futuro.
- **Fácil Administración** → Dividido en partes manejables para detección rápida de fallas.
- **Seguridad** → Instalaciones protegidas contra accesos no autorizados.
- **Estética** → Materiales adaptables a necesidades y diseño.

13.1 Estándares

- **ANSI / EIA / TIA-568** → EEUU → Define cableado comercial, incluyendo par trenzado y fibra óptica.
- **ISO/IEC 11801** → Internacional → Estándar genérico para instalaciones en edificios.
- **EN 50173** → Europa → Basado en ISO/IEC 11801 → Especifico sistemas de cableado estructurado.

13.2 Subsistemas del Cableado Estructurado

- **Área de Trabajo** → Conexión entre dispositivos y enchufes de pared, con al menos dos conexiones (voz y datos).
- **Cableado Horizontal** → Desde las rosetas hasta los armarios de comunicaciones. Se diseña previamente según la distribución del edificio.
- **Cableado Troncal o Backbone** → Comunica elementos del edificio mediante cableado vertical y conexiones exteriores. Utiliza UTP, FTP o fibra óptica según la distancia y ancho de banda requerido.
- **Entrada del Edificio** → Punto donde se conectan cables exteriores con interiores.
- **Armarios de Distribución** → Contienen concentradores, conmutadores y paneles de parcheo organizados en racks estandarizados.
- **Sala de Equipamiento** → Confluencia de todas las conexiones del edificio.
- **Cableado de Campus** → Extiende redes locales entre edificios utilizando fibra óptica.

13.3 Componentes del Cableado

- **Dispositivos de conexión**:
  - Conectores RJ11, RJ45, AUI, BNC para cables UTP/STP/FTP y coaxial.
  - Conectores SC y ST para fibra óptica.
  - Rack y latiguillos para organizar conexiones.
- **Elementos de instalación**:
  - Canaletas para proteger cables.
  - Falsos suelos/techos para estética y limpieza.
- **Instalación eléctrica**:
  - Sistemas SAI (alimentación ininterrumpida) para proteger equipos frente a cortes eléctricos.

14. Protocolos Capa de Aplicación y Transporte

14.1 Capa de Aplicación

- Es la capa superior de los modelos OSI y TCP/IP, proporcionando la interfaz entre las aplicaciones del usuario y la red subyacente.
- **Componentes principales**:
  - **Aplicaciones** → Programas que inician la transferencia de datos (ej., navegadores, correo electrónico).
  - **Servicios** → Conexión entre la capa de aplicación y las capas inferiores.
  - **Protocolos** → Reglas que aseguran la comunicación entre dispositivos.

14.1.1 Protocolos comunes en la Capa de Aplicación

- **DNS (Domain Name System)** → Traduce nombres de dominio en direcciones IP.
- **HTTP (Hypertext Transfer Protocol)** → Transfiere archivos para páginas web.
- **SMTP (Simple Mail Transfer Protocol)** → Envía correos electrónicos.
- **TELNET** → Proporciona acceso remoto a servidores.
- **FTP (File Transfer Protocol)** → Transfiere archivos entre sistemas.

14.1.2 Funciones de los protocolos de aplicación

1. Definen procesos en ambos extremos de la comunicación.
2. Especifican tipos, sintaxis y significado de los mensajes.
3. Determinan cómo se envían mensajes y se gestionan respuestas.

14.2 Capa de Transporte

- Su función principal es **dividir** datos en segmentos → **agregar** encabezados para identificar cada segmento → **recomponerlos** en datos completos para las aplicaciones.
- Utiliza números de puerto para identificar aplicaciones origen y destino.

14.3 Concepto de Puerto y Socket

- Un puerto es un identificador numérico asociado a una aplicación o servicio.
- Un socket combina el número de puerto con una dirección IP para identificar un proceso específico en un dispositivo.

14.3.1 Tipos de Puertos

1. **Bien conocidos (0-1023)** → Reservados para servicios estándar como HTTP (80) o FTP (21).
2. **Registrados (1024-49151)** → Asignados a procesos específicos.
3. **Dinámicos o privados (49152-65535)** → Usados temporalmente por aplicaciones cliente.

14.4 Protocolos TCP y UDP

14.4.1 UDP (User Datagram Protocol)

- Protocolo sin conexión, simple y rápido, con baja sobrecarga.
- Usado en aplicaciones como DNS, streaming y VoIP.
- No garantiza entrega ni orden de los datos.

14.4.2 TCP (Transmission Control Protocol)

- Protocolo orientado a conexión, confiable pero con mayor sobrecarga.
- Garantiza entrega, reenvío de datos perdidos y orden correcto.
- Usado en navegadores web, correo electrónico y transferencia de archivos.

14.4.3 Diferencias entre TCP y UDP

Características	TCP	UDP
Conexión	Orientado a conexión	Sin conexión
Confiabilidad	Alta, con acuses de recibo	Baja, sin acuse
Sobrecarga	Alta	Baja
Reenvío de datos	Sí	No
Uso típico	Navegadores, email, FTP	Streaming, DNS, VoIP
Orden de entrega	Garantizado	No garantizado