Fast Note CCNA

(Apunte Rápido CCNA)
versión 2.2

CONTENIDOS

1. INTERNETWORKING

Modelo OSI:

Creado por la ISO a fines de la década de 1970 para solucionar los problemas surgidos por el desarrollo de diferentes estándares de la mano de diferentes fabricantes (SNA de IBM, Modelo de DECNet, etc.).

Es el modelo de arquitectura primaria para redes. Describe cómo los datos y la información de la red fluyen desde una terminal, a través de los medios de red, hasta otra terminal.

Para esto, divide el proceso global en grupos lógicos más pequeños de procesos a los que denomina "capas" o "layers". Por este motivo se habla de una "arquitectura de capas".

7	**Aplicación**
6	**Presentación**
5	**Sesión**
4	**Transporte**
3	**Red**
2	**Enlace de Datos**
1	**Física**

Ventajas de un modelo de capas:

- Permite la interoperabilidad de diferentes fabricantes.
- Divide las operaciones complejas de la red en capas más fácilmente administrables.
- Permite introducir cambios en una capa sin requerir cambios en la totalidad.
- Define interfaces estándar para la integración "plug and play" de diferentes fabricantes.

Capa de Aplicación - 7

La principal función de la Capa de Aplicación es brindar servicios de red al usuario final. Ofrece servicios a tres tipos principales de aplicaciones:

1. Aplicaciones de red diseñadas específicamente para trabajar sobre una red.
2. Aplicaciones no diseñadas para trabajar en red, sino para utilización en terminales no conectadas.
3. Aplicaciones embebidas, es decir, programas que tienen aplicaciones de red incorporadas como es el caso de los procesadores de texto.

Protocolos que operan en esta capa: http, correo electrónico, ftp, telnet, quake.

Capa de Presentación - 6

Provee servicios de formateo de datos a la capa de aplicación. No todas las aplicaciones de red requieren de este tipo de servicios.

Algunos servicios de esta capa son la encripción de datos, compresión y traslación. Determina la sintaxis de la transferencia de datos.

Protocolos que operan en esta capa: pict, tiff, jpeg, midi, mpeg, quicktime, EBCDIC y ASCII

Capa de Sesión - 5

Establece, administra y termina las sesiones de comunicación entre aplicaciones en diferentes hosts. Ofrece algunos mecanismos de recuperación y control de datos entre las aplicaciones coordinadas de los hosts.

Protocolos que operan en esta capa: NFS, SQL, RPC, X-Windows, ASP (Appletalk Session Protocol).

Capa de Transporte - 4

Esta capa requiere de software adicional en la terminal que opera como cliente de red. Este software recibe el flujo de datos desde la aplicación y lo divide en pequeñas piezas denominadas "segmentos".

Cada segmento recibe un encabezado que identifica la aplicación de origen utilizando puertos.

Los protocolos de capa de transporte pueden asegurar comunicaciones end to end provistas de control de flujo utilizando el método de ventana deslizante y corrección de errores. Además asegura la fiabilidad de los datos utilizando el números de secuencia y de reconocimiento (acknowledge).

TCP utiliza un handshake de triple vía para las pruebas de Transporte.

Multiplexado: Indica la capacidad de que múltiples aplicaciones compartan una única conexión de transporte.

Con este propósito utiliza puertos para identificar sesiones de diferentes aplicaciones:

1 – 1023	Puertos bien conocidos
1 – 255	Puertos públicos
256 – 1023	Asignados a empresas
> 1023	Definidos por el usuario Puertos de origen

El número de puerto oscila entre 1 y 65.535.

Windowing: Técnica que controla la cantidad de información enviada por vez de extremo a extremo expresada en cantidad de bytes.

Protocolos que operan en esta capa: TCP y UDP.

Capa de Red - 3

Proporciona direccionamiento jerárquico y selección de la mejor ruta.

Routing de IP, ICMP, BootP, ARP, RARP considerando el direccionamiento lógico.

Para posibilitar la determinación de la ruta, el servicio de routing suministra:

- Inicialización y mantenimiento de tablas de enrutamiento
- Procesos y protocolos de actualizaciones de enrutamiento.
- Especificaciones de direcciones y dominios de enrutamiento
- Asignación y control de métricas de ruteo.

Protocolos que operan en esta capa: IP, IPX, Apple Talk, RIP, IGRP

Capa de Enlace de Datos - 2

Fragmenta utilizando Ethernet, Ethernet II, 802.5 (token ring), 802.3, 802.2 (802.3 con dsap y sap en los campos de control lógico).

Media Access Control: MAC: 48 bits, 3 bytes vendor + 3 bytes serial number

CDP, (Cisco Discovery Protocol)

Dial on Demand

Bridges / Switches

Direcciones de Capa de Enlace

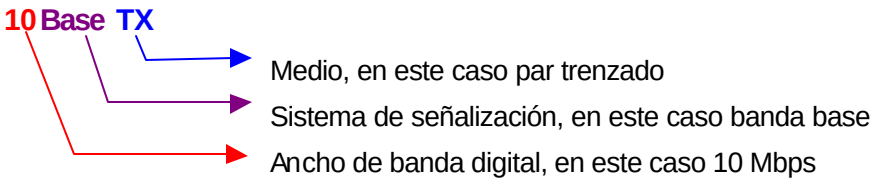
SAP y LLC son utilizados para definir las capas superiors. Provee control de flujo.

Se divide en dos subcapas: LLC y MAC. La subcapa LLC es responsable de la estructuración del frame, el direccionamiento y las funciones de control de error. La subcapa MAC es responsable del acceso al medio.

Capa Física - 1

Cables y conectores: v.24, v.35, x.21, g.703, hssi, etc

Repetidores / Hubs



Estándar	Sub Capa MAC	Medio Físico	Distancia Máxima	Observaciones
1Base 5	802.3	Cable coaxial	500 m	
10Base 2	802.3	Cable coaxial de 50 ohms (thin coaxial) RG-58	185 m	Soporta hasta 30 terminales conectadas. Conectores AUI. Topología en bus serial.
10Base 5	802.3	Cable coaxial de 50 ohms (tick coaxial)	500 m	Soporta hasta 208 usuarios. Conectores AUI. Utilizando repetidores, 2.500 m. máximo y 1024 usuarios.
10BaseF	802.3	Denominación genérica para referirse a tecnologías Ethernet de 10 Mbps sobre cables de fibra óptica.		
10BaseFB	802.3	Fibra óptica	2.000 m	Provee cableado de backbone con señalización sincrónica.
10BaseFL	802.3	Fibra óptica	1.000 m con FOIRL 2.000 m. Solo	Dado que es interoperable con el estándar FOIRL, ha sido diseñado para reemplazar esta tecnología.
10BaseFP	802.3	Fibra óptica	500 m.	Permite estableces terminales en una topología de estrella sin el uso de repetidores.
10BaseT	802.3	UTP cat. 3, 4 ó 5	100 m	Conectores RJ-45. Topología en estrella. Utiliza 2 pares de cables de un cable de par trenzado.
10Broad36	802.3	Cable coaxial	3.600 m	Servicio de 10 Mbps de banda ancha.
100BaseX	802.3	Denominación genérica para referirse a tecnologías Fast Ethernet de 100 Mbps sobre diferentes medios físicos.		

100BaseFX	802.3	Dos hilos de fibra óptica multimodo de 62.5/125 micrones	400 m	Conectores ST o SC. Topología punto a punto.
100BaseFX	802.3u	Fibra óptica monomodo	10.000 m	
100BaseT	802.3	Cable UTP		Utiliza la misma frecuencia de transmisión que 10BaseT, enviando mayor cantidad de información en cada pulso.
100BaseT2	802.3u	Cable UTP cat. 3, 4 ó 5	100 m	
100BaseT4	802.3u	Cable UTP cat. 3, 5 ó 5	100 m	Utiliza los 4 pares de cables.
100BaseTX	802.3u	Cable UTP cat. 5, 6 ó 7 ó STP	100 m	Fast-Ethernet. Utiliza 2 pares de cables.
100VG-AnyLAN	802.12	Cable UTP cat. 3, u o 5		Primer tecnología LAN, desarrollada por HP, que brindó 100 Mb. No es compatible con las técnicas de señalización Ethernet. Utiliza los 4 pares de cables.
1000BaseT	802.3ab	UTP cat. 5	100 m	
1000BaseCX	802.3z	Par trenzado de cobre blindado	25 m	
1000BaseSX	802.3z	Fibra óptima multimodo de 62.5 y 50 micrones	260 m	
1000BaseLX	802.3z	Fibra óptica monomodo de 9 micrones	3.000 a 10.000 m	
ARCnet		Coaxial		Bus LAN de token de 2.5 Mb desarrollado por Datapoint Corporation

CAPA MODELO OSI		PROTOCOLO
7	Aplicación	http – telnet – SNMP
6	Presentación	JPG – MP3
5	Sesión	NFS – Linux
4	Transporte	TCP – UDP
3	Red	IP – ARP – RIP
2	Enlace de Datos	Ethernet – PPP – HDLC
1	Física	

Norma para Cableado Estructurado EIA/TIA 568

Establece el estándar para cableado estructurado en edificios comerciales.

Data de 1991, y fue revisada en 1995, incorporando las variantes A y B.

Norma de cableado 568-A

Pin #	Par #	Función	Color del Cable
1	3	Transmite +	Blanco / Verde
2	3	Transmite -	Verde / Blanco
3	2	Recibe +	Blanco / Naranja
4	1	Telefonía	Azul / Blanco
5	1	Telefonía	Blanco / Azul
6	2	Recibe -	Naranja / Blanco
7	4	Respaldo	Blanco / Marrón
8	4	Respaldo	Marrón / Blanco

Norma de cableado 568-B

Pin #	Par #	Función	Color del Cable
1	2	Transmite +	Blanco / Naranja
2	2	Transmite -	Naranja / Blanco
3	3	Recibe +	Blanco / Verde
4	1	Telefonía	Azul / Blanco
5	1	Telefonía	Blanco / Azul
6	3	Recibe -	Verde / Blanco
7	4	Respaldo	Blanco / Marrón
8	4	Respaldo	Marrón / Blanco

Cable derecho

Igual pinado en ambos extremos. Se utiliza en:

- ✓ Router a hub o switch
- ✓ Servidor a hub o switch
- ✓ Estación de trabajo a hub o switch

Cable cruzado o crossover

Cruza el par 1-2 en un extremo con el 3-6 en el otro; en el 3-6 del primer extremo, con el 1-2 del otro. Se utiliza en:

- ✓ Uplinks entre switches
- ✓ Hubs a switches
- ✓ Hub a hub
- ✓ Puerto de un router a otro puerto de un router
- ✓ Conectar dos terminales directamente.

Cable consola o rollover

El pinado en ambos extremos es i nverso: 1-2-3-4-5-6-7-8 en un extremo, 8-7-6-5-4-3-2-1 en el otro.
Se utiliza en:

- ✓ Conectarse al Puerto consola de un dispositivo.

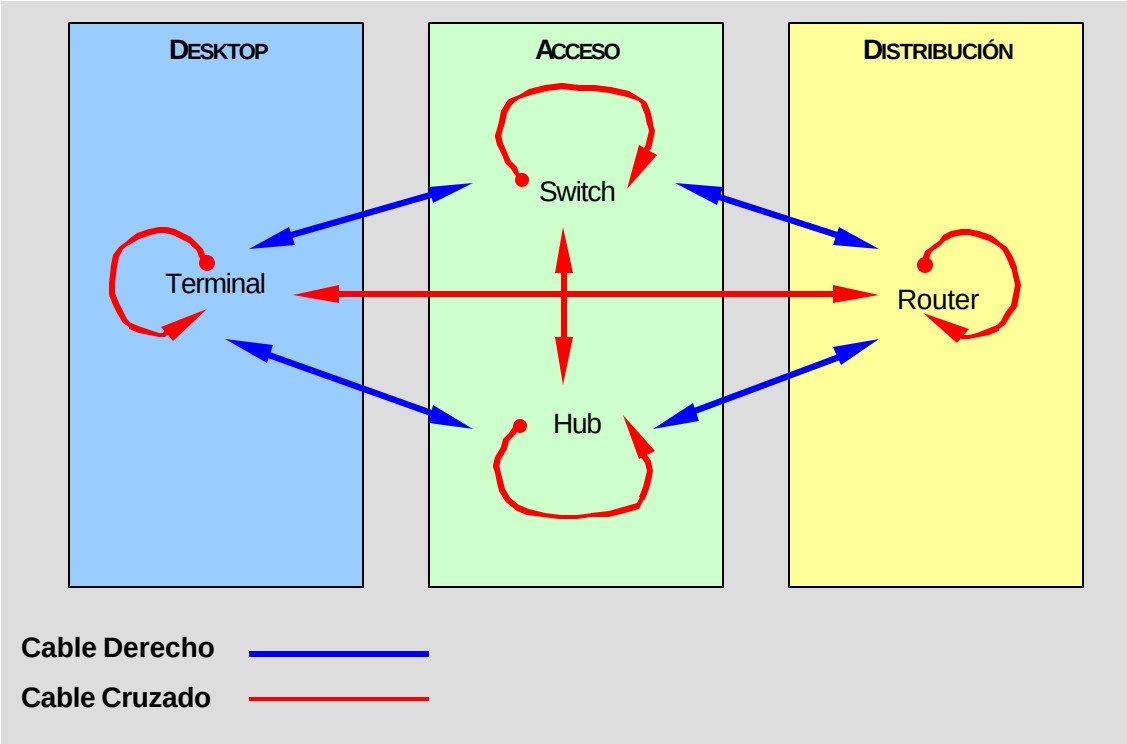
Criterio de conexión

Dispositivo terminal con dispositivo de acceso (hub o switch): cable derecho

Dispositivos de acceso entre sí: cable cruzado

Dispositivo de acceso con router: cable derecho

CONEXIÓN		TIPO DE CABLE
Terminal a	terminal	cable cruzado
	hub / switch	cable derecho
	router	cable cruzado
Hub a	hub	cable cruzado
	switch	cable cruzado
	router	cable derecho
Switch a	hub	cable cruzado
	switch	cable cruzado
	router	cable derecho
	consola	cable rollover
Router a	router	cable cruzado
	switch	cable derecho
	hub	cable derecho
	terminal	cable cruzado
	consola	cable rollover



Modelo TCP/IP

DoD	TCP/IP	OSI	Protocolos
Procesos de Aplicación	Procesos de Aplicación	7- Aplicación 6- Presentación 5- Sesión	Telnet, FTP, LPD, SNMP, TFTP, SMTP, NFS, X WINDOW
Host to Host	Host to Host	4- Transporte	TCP, UDP
Internet	Internet	3- Red	ICMP, BOOTP, ARP, RARP, IP
	Acceso a Red	2- Enlace de datos 1- Física	Ethernet, Fast Ethernet, Token Ring, FDDI

DoD – Modelo desarrollado por el Departamente de Defensa de los Estados Unidos en la década de 1970.

TCP/IP – Suite de protocolos estándar finalmente implementados por la comunidad de ARPANet.

OSI – Modelo estándar desarrollado por la ISO y publicado en el año 1984 a partir de los modelos DecNet, SNA y TCP/IP.

Modelo SNA

Modelo propietario de IBM introducido en 1974 para entornos terminal / mainframe.

Describe un modelo de 7 capas NO compatibles con las capas del modelo OSI, en las que cada capa se construye sobre los servicios provistos por la capa previa.

Los dispositivos en un sistema SNA usualmente se conectan utilizando protocolo SDLC sobre líneas seriales.

CAPA MODELO SNA
Transacción Presentación
Flujo de Datos
Transmisión
Control de Ruta
Enlace de Datos Física

Direccionamiento:

Direccionamiento de Hardware es utilizado para transportar un paquete desde un dispositivo local hasta otro dispositivo local.

Direccionamiento Lógico es utilizado para transportar un paquete end to end a través de una internetwork.

Direccionamiento Multicast es un direcionamiento MAC utilizado para identificar un grupo de destinatarios y se indica colocando el primer bit transmitido de la dirección de destino en 1.

- **Unicast –** de uno a uno en una red
- **Multicast –** de uno a un grupo en una red
- **Broadcast –** de uno a todos en una red

El enrutamiento utiliza Direcciones de Red.

El router toma un paquete de una capa de enlace de datos y lo envía a otra. Para dirigir un paquete, un router utiliza dos funciones básicas:

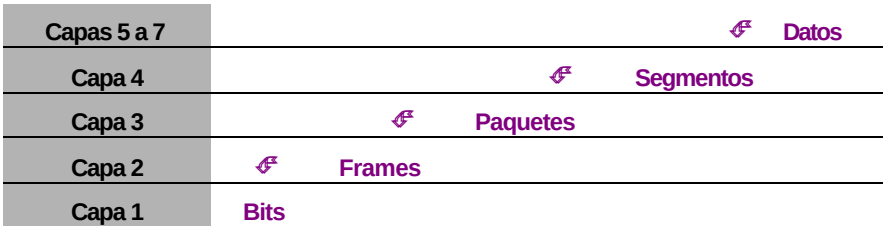
- Función de determinación de la ruta.
- Función de conmutación.

Direcciones	Dirección de Red	Dirección de Host
Dirección MAC		6 bytes -- 48 bits
Novell IPX	32 bits (hex)	48 bits (hex), usualmente es la dirección MAC de la NIC (total 32+48=80 bits)
Dirección IP	8 a 24 bits	24 a 8 bits (total 32 bits)
AppleTalk	16 bits (dec); refiere a una o una a muchas redes en el medio	8 bits agregados al número de red, usualmente asignados dinámicamente

Proceso de encapsulación

Los cinco pasos

1. Se convierte la información del usuario en **datos**.
2. Preparar los datos para el transporte end-to-end. Los datos son fragmentados en **Segmentos** y encapsulados con información de control para lograr una conexión confiable.
3. Agregar las direcciones de red en el encabezado de red. Los datos son colocados dentro de un **paquete** o **datagrama** especificando las direcciones lógicas de origen y destino.
4. Agregar las direcciones MAC en el encabezado de enlace de datos (deben ser colocados dentro de un **frame** o trama para permitir la transmisión a través de una interface).
5. Convertir a **bits** incluyendo algunas funciones de clocking para realizar la transmisión física.



Estructura del paquete

Encabezado de la Trama	Encabezado del Datagrama	Encabezado del Segmento	Datos	FCS

Frame Ethernet:

Preámbulo	Dirección de Destino	Dirección de Origen	Type	Datos	FCS

Longitud mínima del frame Ethernet = 64 bytes

Longitud máxima del frame Ethernet = 1518 bytes

Modelo OSI

Transporte	Segmentos TCP
Red	Paquetes IP / Datagramas
Enlade de Datos	Ethernet Frames / Tramas
Física	Bits

Términos clave:

Bits: La capa física toma los datos binarios de la capa de Enlace de Datos y convierte los 1's y 0's a una señal digital para enviarlos a través de la topología física.

Frames / Tramas: Alojan los paquetes o datagramas enviados desde la capa de Red para ser entregados a un dispositivo en la LAN. Incluye las direcciones físicas.

Paquetes: A veces llamados "datagramas", alojan los segmentos enviados por la capa de Transporte para ser enrutados a través de la red. Incluye las direcciones lógicas.

Segmentos: Se definen en la capa de Transporte. Se trata de la partición del flujo de datos que proviene de las capas superiors hacia el dispositivo de destino.

Modelo Cisco de Tres Capas:

1	**Núcleo - Principal**
2	**Distribución**
3	**Acceso**

Capa de Acceso:

En esta capa:

- ✓ Define dominios de colisión.
- ✓ Definición de VLANs.
- ✓ Conecta el grupo de trabajo a la Capa de Distribución.
- ✓ Dispositivos típicos: hub y switch.

Capa de Distribución:

Lo que se hace en esta capa:

- ✓ Implementación de herramientas tales como filtros, colas de espera y listas de acceso.
- ✓ Implementación de políticas de seguridad.
- ✓ Redistribución de tráfico utilizando protocolos de enrutamiento y rutas estáticas.
- ✓ Enrutamiento entre VLANs y grupos de trabajo.
- ✓ Definición de dominios de broadcast y multicast.
- ✓ Dispositivo típico: router.

Capa Núcleo:

Su principal función es brindar conmutación de tráfico rápida y eficiente. Una falla en el núcleo afecta a cada uno de los usuarios conectados, por lo tanto es crítica la tolerancia a fallos.

Lo que NO se debe hacer:

- ✓ Implementar recursos que incrementen la latencia.
- ✓ Brindar acceso a grupos de trabajos o usuarios finales.
- ✓ Expandir el núcleo. Cuando la red crece se debe privilegiar el aumento de potencia por sobre la expansión.

Lo que SI se debe hacer:

- ✓ Diseñar teniendo como objetivo la máxima confiabilidad.
- ✓ Diseñar buscando la máxima velocidad.
- ✓ Seleccionar protocolos de enrutamiento con bajos tiempos de convergencia.

2. TECNOLOGÍAS DE CONMUTACIÓN LAN

Funciones del switch

- ✓ Aprender direcciones MAC
- ✓ Reenviar / filtrar paquetes
- ✓ Evitar bucles

Diferencias entre switches y bridges

1. Los bridges se basan en software mientras los switches se basan en hardware (circuitos ASICs)
2. Los bridges sólo admiten una instancia STP por dispositivo, mientras los switches soportan varias.
3. Los bridges pueden tener solamente hasta 8 puertos, mientras que los switches pueden tener cientos.

Métodos de conmutación

1. Método de Corte
   1.1. Libre de Fragmentos
2. Almacenamiento y envío

Cut Through
Envío Rápido - Método de Corte

El switch LAN copia solamente la dirección MAC de destino en su buffer antes de proceder a conmutar al puerto de destino.
Tiene una latencia fija y baja ya que comienza a enviar el frame tan pronto como lee la dirección de destino y determina la interface de salida.
No implementa ningún método de detección de errores.

Fragment Free
Libre de Fragmentos

Es una variante del método de corte puro. El puerto del switch copia solamente los primeros 64 bytes del frame, de este modo filtra los residuos producto de colisiones y asegura procesar sólo paquetes que cumplen con el tamaño mínimo del estándar Ethernet.
Tiene una latencia fija y baja porque comienza el envío del frame luego de recibir los primeros 64 bytes.
Al esperar a recibir la "ventana de colisión" completa, minimiza la difusión de basura y residuos de colisión, por lo que se puede decir que implementa una forma de detección de errores.
Es la opción por defecto de los switches Catalyst 1900.

Store and Forward
Alamacenamiento y envío

Tiene una latencia variable ya que depende de la medida de cada paquete que es variable; y debe esperar a recibir la totalidad del frame antes de reenviarlo.
Copia el frame completo en el buffer y verifica el campo FCS.

Spanning Tree Protocol

Es un protocolo ca capa 2 para administración de enlaces que provee rutas redundantes a la vez que prevé bucles en la red, permitiendo que sólo exista una ruta activa entre dos estaciones.

Desarrollado originalmente por Digital Equipment Corporation, fue luego estandarizado por IEEE en la norma 802.1d

Para administrar esta redundancia, STP desarrolla un árbol que contiene a todos los switches en toda la extensión de la red. A partir de este "árbol" STP coloca algunos puertos en estado de espera (bloqueo): si la situación de algún puerto activo de la red cambiara, STP reconfiguraría la topología para restablecer el enlace activando el puerto que había bloqueado.

La operación de STP es transparente para las estaciones de trabajo.

Para compartir la información de switches y puertos, STP envía cada 2 segundos BPDU. Los paquetes BPDU se inundan por todos los puertos ya que se trata de paquetes en formato multicast.

Operación de STP

1. Elige un **switch raíz** (root bridge)
    a. Sólo hay un switch raíz en cada dominio de broadcast.
    b. Los puertos del switch raíz son denominados "puertos designados" (desginated ports).
    c. Los puertos designados están en estado de Forwarding.
    d. Proceso de elección:
        i. Todos los switch del dominio de broadcast inundan la red con BPDU conteniendo su ID como switch raiz.
        ii. Cada switch toma todos los BPDU recibidos y los compara para seleccionar cuál será su switch raiz.
        iii. Toma como base el ID del switch. El switch con menor ID será reconocido como switch raiz.
        iv. El ID es un valor de 8 bytes integrado por la prioridad STP (2 bytes) y la MAC del switch (6 bytes).
        v. En todos los dispositivos, la prioridad STP por defecto e s 32.768 (0x8000).
        vi. Consecuentemente, a igual prioridad utiliza la MAC del dispositivo para seleccionar el switch raiz. El que tiene la MAC más baja es designado root bridge.
2. Los demás switches se denominan **no-raíz** (nonroot bridge).
    a. Cada switch no-raíz tiene un solo puerto raiz en cada dominio de broadcast.
    b. Selecciona como **puerto raíz** (root port) al puerto de menor costo hacia el switch raíz y lo pone en estado de Forwarding.
        i. El costo STP es un valor acumulado basado en el ancho de banda del enlace.
        ii. Costos STP 802.1d original:

10 Gbps	1
1 Gbps	1
100 Mbps	10
10 Mbps	100

        iii. Costos STP versión 2:

10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

    c. Los puertos no-designados están en estado de blocking.

Estados de los Puertos STP

- ✓ **Bloqueado** (Blocking) – Es uno de los estados habituales de los puertos del switch. Todos los puertos están bloqueados por defecto para evitar los bucles. Permanece en este estado mientras el switch determine que hay una ruta mejor al switch raíz (menor costo).
  En este estado, el puerto recibe BPDUs, pero no recibe ni envía frames.
- ✓ **Escuchando** (Listening) – Es un estado transitorio del puerto. Atiende BPDUs para asegurarse de que no hay bucles antes de comenzar a enviar.
  Este estado se utiliza para indicar que el puerto está a punto de quedar listo para transmitir, pero aún no lo hace para garantizar que no se cree un bucle.
- ✓ **Aprendiendo** (Learning) – Es el siguiente estado transitorio del puerto. En este estado aprende direcciones MAC con las que construye sus tablas, pero no reenvía paquetes.
- ✓ **Enviando** (Forwarding) – En este estado el puerto envía y recibe todos los paquetes que ingresan.

Temporizadores STP

Para pasar del estado de Bloqueado al de Enviando, con los valores por defecto de los temporizadores (pueden ser ajustados por configuración) un puerto demanda **50 segundos**. Este es el tiempo considerado necesario para recopilar toda la información correcta sobre la topología de la res.

Retraso de retransmisión: tiempo que tarda un puerto en pasar del estado de escuchando al de aprendiendo; o de este al de enviando.

Temporizador	Función	Tiempo por Defecto
Tiempo de saludo	Lapso entre envío de BPDU	2 segundos
Duración Máxima Message age	Tiempo de almacenamiento de la información de un BPDU. Si transcurrido este tiempo no se recibe un nuevo BPDU con la misma información, el puerto pasa al estado de escuchando	20 segundos
Retraso de retransmisión Forward delay	Duración de los estados de escuchando y aprendiendo	15 segundos

Tiempo	Suceso	Intervalo
00 seg.	Se recibe el último BPDU	20 seg.
20 seg.	Se descarta la información correspondiente al último BPDU, y se inicia el proceso de recálculo del árbol. El puerto pasa al estado de Escuchando	15 seg.
35 seg.	Finaliza el período de escucha y el puerto comienza a aprender direcciones MAC y construir sus tablas. El puerto pasa al estado de Aprendiendo	15 seg.
50 seg.	Finaliza el período de aprendizaje y el puerto pasa al estado de Enviando.	

Anexo

Configuración por CLI del Catalyst 1900

Métodos de configuración del Catalyst 1900

- ✓ Interface web: VSM
- ✓ Menú
- ✓ CLI

Configuración de password

```
#enable password  level [1-15] [password]
```

level 1 - password de modo usuario

level 15 - password de modo enable

Cada password debe tener un mínimo de 4 caracteres y un máximo de 8

No es case sensitive.

```
#enable secret [password]
```

Verificación de la configuración

```
#show running-config
```

La configuración se almacena en la NVRAM, pero no puede ser revisada. No hay un comando show startup-config. Al hacer cambios en la running-config, estos automáticamente se almacenan en la NVRAM.

Configuración del nombre del dispositivo

```
#hostname [nombre]
```

Configuración de información IP

Show ip - Permite observar los valores de configuración IP del switch. Los valores por defecto son:

```
#show ip
ip address: 0.0.0.0
subnet mask: 0.0.0.0
default gateway: 0.0.0.0
management vlan: 1
domain nome:
name server 1: 0.0.0.0
name server 2: 0.0.0.0
http server: enabled
http port: 89
#ip address 172.16.10.16 255.255.255.0
#ip default-gateway 172.16.10.1
```

Configuración de interfaces

El Catalyst 1900 utiliza los comando *type slot/port* para identificar las interfaces. Aunque tiene un solo slot: 0.

Los puertos los numera de 1 a 24, el puerto AUI es 25, el puerto A es 26 y el B es 27.

```
#interface Ethernet 0/1
#interface fastEthernet 0/26
#show interface Ethernet 0/1
#show interface fastEthernet 0/26
```

Configuración de un puerto como full dúplex

```
#interface fastEthernet 0/26
#duplex full
```

Opciones de las funciones duplex:

`auto`	Modo de autonegociación. Estado por defecto para los puertos 100BaseTX.
`full`	Fuerza el modo full dúplex.
`full-flow-control`	Implementa control de flujo en puertos 100BaseTx evitando el desbordamiento de los buffers.
`half`	Fuerza a trabajar en modo half dúplex. Estado por defecto para los puertos 10BaseTX.

Verificación de conectividad IP

```
#ping 172.16.10.10
#telnet 172.16.10.10
```
¡¡¡El commando telnet no está disponible en el Catalyst 1900!!!

Borrar la configuración

```
#delete nvram
#delete vtp
```

Administración de las tablas de direcciones MAC

```
#show mac-address-table
#clear mac-address-table
```

`#mac-address-table aging-time` - Configura el tiempo de permanencia de una entrada dinámica en la tabla de direcciones MAC.

`#mac-address-table permanent [MAC] [interface]` - Relaciona de modo permanente una dirección MAC con una interface.

`#mac-address-table restricted static [MAC de destino] [Puerto destino] [Puerto origen]` - Configura una ruta fija para el tráfico originado en un puerto.

```
#interface Ethernet 0/2
```

`#port secure max-mac-count [1-132]` - Limita la cantidad de direcciones MAC que pueden asociarse a un puerto. El valor por defecto es 132.

```
#show version
#show port system
```

```
#switching-mode [fragment-free / store-and-forward]
```

Configuración de VLANs

```
#vlan [#] name [nombre]
#show vlan
#show vlan [# vlan]
#interface 0/4
#vlan-membership [static] [# vlan]
```
- Este comando se ejecuta en el modo de configuración de la interface correspondiente.

```
#show vlan-membership
```

Configuración de puertos troncales

```
#interface 0/26
#trunk on
#no trunk-vlan [#]
#show trunk [A/B]
#show trunk [A/B] allowed-vlans
```

Configuración de VTP

```
#vtp server
#vtp domain [nombre de dominio]
#vtp password [password]
#show vtp
```

Restauración o actualización del Cisco IOS

```
#copy tftp://[dirección del servidor tftp]/[nombre del archivo]
opcode
```

En el Catalyst 1900 no se puede hacer copia de seguridad del Cisco IOS.

Copia y restauración del archivo de configuración

```
#copy nvram tftp://[dirección del servidor tftp]/[nombre del archivo]
#copy tftp://[dirección del servidor tftp]/[nombre del archivo] nvram
```

3. VLANS

Son agrupaciones lógicas de puertos.

Cada VLAN constituyen un dominio de broadcast diferente.

Nota: Los switches Catalyst 1900 se presentan en dos versiones.
Catalyst 1900 estándar – Esta versión permite agrupar puertos en varios dominios de broadcast diferentes a los que denomina Bridge Groups. Estos switches no permiten habilitar puertos o enlaces troncales.
Catalyst 1900 enterprise – La versión Enterprise permite trabajar tanto con VLANs como con Bridge Groups, aunque no con ambos a la vez. Si está activada la versión VLAN permite configurar puertos troncales.

Beneficios:

- Reduce los costos de administración
- Controla el broadcast
- Mejora la seguridad de la red
- Mejora las prestaciones de los hubs ya instalados

Modos de pertenencia a la VLAN:

Estático - La asignación del puerto a una VLAN es realizada por el administrador.

Dinámico - Requiere de un VLAN Membership Policy Server (VMPS): según las direcciones MAC de las terminales, cada puerto es asignado a una VLAN.
El VMPS puede ser tanto otro switch (Catalyst 5000 por ejemplo, o un servidor externo).
Un puerto dinámico sólo puede pertenecer a una VLAN en un momento dado.
Puede haber varios hosts activos simultáneamente conectados a un puerto del switch, pero todos deberán pertenecer a la misma VLAN.

Al utilizar VLANs hay tres tipos de puerto o enlaces:

- Puertos de acceso: pertenecen a una única VLAN.
- Puerto sobrepuesto: pertenecen a varias VLANs simultáneamente. Esta opción sólo está disponible en los switches Catalyst 1900 estándar, la versión enterprise no soporta puertos sobrepuestos.
- Puerto troncal: permiten el transporte de varias VLANs a través de varios switches manteniendo sus identidades.
  Esta opción sólo está disponible en los switches Catalyst 1900 enterprise, no en la versión estándar.
  Para esto se utilizan básicamente dos protocolos:
  - ISL – Propietario de Cisco. Este es el protocolo implementado en los Catalyst 1900.
  - 802.1q - estándar IEEE.

Métodos de identificación VLANs

1. **ISL** (Inter-Switch Link) - Propietario de Cisco. Sólo funciona sobre enlaces Fast Ethernet o Gigabit Ethernet.
   Funciona tanto en interfaces de switches como de routers y servidores.

2. **IEEE 802.1q** - Estándart. Inserta un campo dentro del frame para identificar la VLAN.
3. **LAN Emulation** (LANE) - Utilizado sobre ATM.
4. **802.10** (FDDI) - Propietario de Cisco. Utilizado sobre FDDI. Utiliza un campo SAID en el encabezado del frame para identificar la VLAN.

ISL

Proporciona baja latencia y aprovechamiento del ancho de banda.

Se implementa sobre enlaces Fast-ethernet tanto half como full-dúplex.

Sólo funciona sobre switches. Es una tecnología no intrusiva en las terminales, las mismas nunca reciben tráfico ISL.

Se puede implementar entre switches, con routers y con servidores equipados con placas de red ISL.

Utiliza un proceso de marcación exterior. Sin tocar el frame original le agrega un encabezado exterior: agrega un encabezado de 26 bytes y un campo FCS de 4 bytes. El frame resultante puede llegar a tener un tamaño máximo de 1522 bytes (el máximo tolerado en segmentos ethernet es 1518).

Trunking

Son enlaces de 100Mbps o superiores que conectan punto a punto dos s witches, un switch con un router o con un servidor.

Transportan el tráfico de hasta 1005 VLANs.

Al habilitar un puerto troncal, por defecto transporta todas las VLANs configuradas en el switch.

VLAN Trunk Protocol (VTP)

Protocolo propietario de Cisco.

La información VTP circula a través de los enlaces troncales.

Beneficios que provee:

- ✓ Configuración consistente de las VLANs a través de todos los switches en la red.
- ✓ Permite el transporte de VLANs a través de redes mixtas.
- ✓ Reportes dinámicos .
- ✓ Agregado de VLANs plug and play.

Modos VTP

- **Servidor** - Comparte la información con los demás dispositivos VTP que integran el mismo dominio VTP. Es el modo en el que se crean VLANs y se realizan cambios. Toda modificación en el switch servidor es transmitida a todo el dominio. Es el estado por defecto de todo switch Cat 1900.
- **Cliente** - envía y recibe información VTP, pero no puede introducir ningún cambio.
- **Transparente** - Envía y recibe información de VTP, pero no la incluye en su base de datos. No participa del dominio VTP.

VTP Prunning

Permite restringir el broadcast que se envía a cada enlace troncal, preservando el ancho de banda. VTP prunning está deshabilitado por defecto en todos los switches.
En los Cat 1900 no se puede habilitar VTP prunning para la VLAN 1 pues es la VLAN de managment.

4. PROTOCOLO IP

Clases

Es definida por la posición del primer cero contando desde la izquierda en el primer octeto.

A partir de la clase (la posición del primer cero desde la izquierda), se establece cuántos bits u octetos utiliza para definir el número de red, y cuántos quedan para definir el número de host.

Clase A

Primer octeto: **0**0000001 a **0**1111111 **1.0.0.0 a 127.0.0.0**

127 - dirección de loop back

Direcciones reservadas: 10.0.0.0 a 10.255.255.255

Esquema: R.H.H.H

Clase B

Primer octeto: 1**0**000000 a 1**0**111111 **128.0.0.0 a 191.255.0.0**

Direcciones reservadas: 172.16.0.0 a 172.31.255.255

Esquema: R.R.H.H

Clase C

Primer octeto: 11**0**00000 a 11**0**11111 **192.0.0.0 a 223.255.255.0**

Direcciones reservadas: 192.168.0.0 a 192.168.255.255

Esquema: R.R.R.H

Clase D

Primer octeto: 111**0**0000 a 111**0**1111 **224.0.0.0 a 239.255.255.255**

Direcciones de Multicast o Multidifusión

Clase E

Primer octeto: 1111**0**000 a 1111**0**111 **240.0.0.0 a 247.255.255.255**

Direcciones de Investigación

Protocolos

ARP

Permite resolver o mapear direcciones IP a direcciones MAC.

RARP

Permite resolver o mapear direcciones a partir de una dirección MAC conocida a una IP desconocida.

Tengo la IP + Busco la MAC = ARP
Tengo la MAC + Busco la IP = RARP

Inverse ARP - ARP Inverso

Puede ser utilizado para que LMI pueda resolver una dirección IP a partir de un número DLCI. Se lo utiliza para resolver la dirección IP del próximo salto para una conección expecífica.

TCP

Fracciona y reensambla archivos.

Utiliza números de secuencia y windowing

Envía acknowledgements

Provee control y corrección de errores.

ICMP

Este protocolo informa en caso de que los dispositivos no puedan encontrar el próximo salto para direccionar los paquetes.

5. ENRUTAMIENTO IP

Para poder enrutar un paquete, el router debe conocer como mínimo:

- Dirección de destino.
- Router vecino a partir del cual puede aprender sobre las redes remotas.
- Rutas posibles a todas las redes remotas.
- La mejor ruta a cada red remota.
- Cómo mantener y verificar la información de enrutamiento.

El router aprende acerca de las redes remotas:

- ✓ De los routers vecinos.
- ✓ De un administrador.

Con esta información el router construye las tablas de enrutamiento. La información de las tablas puede constituirse de dos maneras:

- Dinámicamente – Protocolos de enrutamiento dinámico. Las actualizaciones se desencadenan de modo automático al generarse un cambio.
- Estáticamente – Rutas estáticas definidas por el Administrador. Las modificaciones necesarias al realizarse un cambio son responsabilidad del Administrador.

Rutas Estáticas

Proceso mediante el cual el Administrador agrega manualmente una ruta en la tabla de enrutamiento de cada router.

Ventajas	Desventajas
✓ No genera carga en la CPU del router.	✓ El Administrador debe tener una comprensión amplia de la internet y cómo cada router está conectado.
✓ No utiliza ancho de banda en los enlaces entre los routers.	✓ Si una red se agrega a la internet, el Administrador debe agregar la ruta hacia ella en todos los routers.
✓ Son más seguras.	✓ En redes grandes, la actualización de rutas puede convertirse en un trabajo full-time.

Configuración de una ruta estática

```
ip route [red destino] [máscara] [próximo salto] [distancia administrativa]
```

Red de destino– Dirección de red de la red o subred hacia la cual se quiere introducir una entrada en la tabla de enrutamiento.

Máscara – Máscara de subred a utilizar con la dirección de red de destino.

Próximo salto – Dirección de red del puerto del router vecino hacia el que se debe enviar el paquete. También se puede utilizar en su lugar la interface de salida en el propio router; esta opción solo es aplicable en enlaces WAN y no está disponible sobre puertos LAN, p.e. Ethernet.

Distancia Administrativa – Determina la confiabilidad de la fuente de origen de la información de enturamiento. En el caso de las rutas estáticas, por defecto su valor es 1 (a mayor confiabilidad, menor distancia administrativa).

Distancia Administrativa

Calificación referida a la calidad o confiabilidad de la fuente de la información de enrutamiento.

0 la mejor ruta

255 ruta que nunca se utilizará

Fuente	Valor
Red directamente conectada	**0**
Ruta estática (por defefecto)	**1**
Protocolo EIGRP	**90**
Protocolo IGRP	**100**
Protocolo OSPF	**110**
Protocolo RIP	**120**

Ruta por Defecto

Ruta utilizada para direccionar paquetes que tienen como destino una dirección perteneciente a una red para la cual no hay ninguna ruta en la tabla de enrutamiento.

Se implementan rutas por defecto en redes “stub”, es decir, redes que tienen una única ruta de entrada y salida a la internetwork.

Configuración de una ruta por defecto

```
ip route 0.0.0.0 0.0.0.0 [próximo salto]
```

Si se utiliza una ruta por defecto debe utilizar el comando `ip classless`, ya que las redes no remotas figurarán en la tabla de enrutamiento y tienen una máscara de subred diferente. En las versiones 12.x del IOS, está activo por defecto.

Enrutamiento Dinámico

Procedimiento que utiliza protocolos de enrutamiento paa encontrar y actualizar las tablas de enrutamiento.

Protocolos de Enrutamiento

Un protocolo de enrutamiento define el conjunto de reglas utilizadas por un router cuando este se comunica con los routers vecinos.

Básicamente hay dos tipos de protocolo de enrutamiento:

- ✓ Protocolos de Enrutamiento Interior
  Protocolos que administran rutas que conectan distintas redes o subredes de un único sistema autónomo.

  RIP

  IGRP

  Enhanced IGRP

  OSPF

  IS-IS

- ✓ Protocolos de Enrutamiento Exterior
  Protocolos que administran rutas que conectan diferentes sistemas autónomos.

  BGP

  EGPs

Sistema Autónomo

Conjunto de redes o routers bajo una administración común.

Protocolos con un AS

OSPF

EIGRP

IGRP

Comparación entre Enrutamiento de Vector Distancia y de Estado de Enlace

Vector Distancia	Estado de Enlace
Visualiza la red desde la perspectiva de los vecinos.	Buscan una vision común de la topología de la red íntegra.
Incrementa las métricas a través de las actualizaciones: convergencia lenta.	Cada dispositivo calcula la ruta más corta a los otros routers.
Realiza actualizaciones periódicas.	Los eventos activan la actualización: convergencia más rápida.
Transmite copia de la tabla de enrutamiento a los routers vecinos.	Transmite actualizaciones del estado de los enlaces a los otros routers.
RIP - utiliza solo el número de saltos como métrica. IGRP – su métrica considera: ancho de banda, delay, confiabilidad, carga, MTU. (por defecto sólo los dos primeros)	OSPF

Vector Distancia: Aprende la mejor ruta a la red de destino basándose en la acumulación de las métricas de cada vecino.

Estado de Enlace: Aprende la topología exacta de la red entera. Mantiene una compleja información de la topología. Es utilizado para crear usna imagen común de la red entera. Utiliza notificaciones del "vecindario".

RIP

Métrica: número de saltos

Métrica máxima: 15 saltos – 16 saltos = inalcanzable

Distancia Administrativa: 120

- Período de actualización: 30 segundos

- Período de invalidación de ruta: 90 segundos

- Período de renovación de rutas: 240 segundos

Propagación por broadcast

Protocolo de enrutamiento classful --- Todos los puertos de la red deben tener la misma máscara de subred.

Solo cuenta “saltos” (routers que debe atravesar en la ruta hasta el destino) para determinar la mejor ruta. Si encuentra más de un enlace a la misma red de destino con la misma métrica, automáticamente realiza balanceo de carga. RIP puede realizar balanceo de carga en hasta 6 enlaces de igual métrica.

La limitación de este protocolo es cuando se cuenta con enlaces de igual métrica en saltos pero diferente ancho de banda. El protocolo balanceará tráfico por igual entre ambos enlaces, tendiendo a provocar la congestión del enlace de menor ancho de banda (pinhole congestion).

Rip versión 2

Propagación por multicast

Protocolo de enrutamiento classless --- Los puertos pueden tener diferente máscara de subred.

Configuración de RIP

```
Router(config)# router rip
Router(config-router)# network X.X.X.X
Router(config-router)# passive-interface s0
```
impide la publicación de actualizaciones a través de la interface especificada.

```
Router# show ip protocol
```
verifica la configuración del protocolo, incluidos los temporizadores.

IGRP

Protocolo propietario de Cisco

Métrica compuesta: ancho de banda, delay, confiabilidad, carga MTU

Métrica por defecto: ancho de banda y delay

Cantidad de salto máxima: 255 saltos– 100 saltos por defecto

Distancia Administrativa: 100

- Período de actualización: 90 segundos

- Período de invalidación de rutas: 3 veces el período de actualización.

- Período de espera: 3 veces el período de actualización más 10 segundos.

- Período de renovación de rutas: 7 veces el período de actualización.

Protocolo de enrutamiento classful --- Todos los puertos de la red deben tener la misma máscara de subred.

Al tener una métrica combinada y soportar mayor cantidad de saltos, supera varias de las limitaciones de RIP y permite aprovechar el ancho de banda como métrica.

Permite balancear carga en hasta 6 enlaces de igual o diferente métrica.

Su configuración requiere que se defina un número de sSistema Autónomo

Configuración de IGRP

```
Router(config)# router IGRP [AS]
Router(config-router)# network X.X.X.X
Router(config-router)# variance [1-128]
```
controla el balanceo de carga entre la ruta de mejor métrica y la de peor métrica aceptable.

`Router(config-router)# traffic-share balanced`	Distribuye la carga de modo inversamente proporcional a la métrica de los enlaces.
`Router(config-router)# traffic-share min`	Se balancea tráfico utilizando primera las rutas que tienen menor métrica.
`Router# show ip protocol`	verifica la configuración del protocolo, incluidos los temporizadores.

Conceptos relacionados

Fragmentación:

Proceso que tiene lugar en routers ubicados entre origen y destino por el que los datagramas son particionados a la medida conveniente para ser transportados por los frames de una red particular.

Convergencia:

Tiempo en el que un conjunto de routers alcanza una visión consistente de la topología de la red.

Durante el procedimiento de convergencia, los dispositivos no reenvían tráfico.

Bucles:

Falta de consistencia de la red que genera una ruta en la que los paquetes nunca alcanzan su destino, ya que recorren repetidamente una serie constante de nodos de la red.

Resolución de bucles de enrutamiento

Máximo número de saltos
Maximum Hop Count

Al enviar un paquetea través de una ruta cada router reduce el valor del campo TTL en al menos una unidad cada vez. De este modo, cuando el campo TTL alcanza el valor 0 es descartado. Este procedimiento permite descartar un paquete que no alcanza su ruta de destino y que de otro modo circularía indefinidamente dentro de la red.

Para prevenir que esta cuenta tienda al infinito, los protocolos de vector distancia definen infinito como un número entero. Este número se refiere a una métrica de enrutamiento como un número de saltos.

Esta técnica no evita el bucle, sino la propagación al infinito de los paquetes.

Número máximo de saltos RIP = 15

Número máximo de saltos IGRP= 255. Por defecto 100.

Horizonte Dividido
Split Horizon

Nunca resulta útil volver a enviar información acerca de una ruta de destino en la misma dirección de donde ha venido la actualización original.

Permite prevenir los bucles de enrutamiento y acelerar la convergencia.

Envenenamiento de Ruta
Poison Reverse

Es una variante del horizonte dividido. Consiste en crear una entrada en la tabla de enrutamiento en la que se guarda la información nueva recibida esperando que el resto de la red converja en la misma información. En esa entrada, la red de destino es marcada como inalcanzable.

De este modo se evita que el router pueda aceptar información incoherente. Funciona en combinación con los temporizadores.

Temporizadores

Holddowns

Se utilizan para prevenir mensajes de actualización regulares tendientes al restablecimiento de una ruta que pueda haber quedado inutilizable.

También permiten prevenir que los cambios se hagan con excesiva rapidez, permitiendo que una ruta caída vuelva a ser operativa dentro de un lapso de tiempo, sin que haya habido cambios.

- El temporizador de espera se activa cuando el router recibe la primera actualización indicando que una red que estaba activa ahora es inaccesible.
- Si se recibe una nueva actualiza ción con una métrica mejor, el temporizador se remueve y se ingresan los datos.
- Si la actualización que se recibe tiene una métrica peor, el temporizador sigue contando.

6. CONFIGURACIÓN Y ADMINISTRACIÓN DEL CISCO IOS

Cisco router IOS

El Cisco IOS es el kernel de los router y la mayoría de los switches Cisco.

Funciones básicas:

- Protocolos de red
- Direccionar tráfico entre dispositivos a alta velocidad.
- Agregar seguridad al control de acceso y detener el uso no autorizado de la red.
- Proveer escalabilidad para facilitar el crecimiento y escalabilidad de la red.
- Brindar confiabilidad en la conexión a los recursos de red.

Conexión al router

1. **Puerto Consola**
   - **a.** Conexión física: cable consola con conector RJ-45.
   - **b.** Requiere la utilización de un programa de emulación de terminal (p.e. Hyperterminal)
     - 9600 baudios
     - 8 bits de datos
     - Paridad ninguna
     - bit de parada 2
     - Control de flujo ninguno
   - **c.** Por defecto no requiere password.
2. **Puerto Auxiliar**
   - **a.** Conexión física: cable consola con conector RJ-45.
   - **b.** Se puede utilizar también para configuración directa (no sólo por módem). Requiere la utilización de un programa de emulación de terminal (p.e. Hyperterminal)
     - 9600 baudios
     - 8 bits de datos
     - Paridad ninguna
     - bit de parada 2
     - Control de flujo hardware
   - **c.** Por defecto no requiere password.
3. **Terminal Virtual**
   - **a.** Conexión física: se accede desde una terminal conectada a la red en cualquier punto de la misma.
   - **b.** Requiere la utilización del programa de emulación de terminales bobas Telnet

c. Por defecto requiere password, aunque esta no está configurada. Si no se configura password el router no permitirá el acceso por terminal virtual.

Modos:

	Modo Setup
`rommon>`	ROM Monitor Mode - Modo monitor de ROM
`Router>`	EXEC Mode – Modo usuario
`Router#`	Privileged EXEC Mode - Modo privilegiado
`Router (config)#`	Modo configuración global
`Router (config-mode)#`	Otros modos específicos de configuración: interface subinterface line router

Modo setup

Proceso step-by-step asistido de configuración de un router.

Se activa:

- Automáticamente durante el proceso de inicialización cuando el router no puede encontrar un archivo de configuración válido en la NVRAM.
- Desde el modo de configuración global:

```
Router (config)#setup
```

Presenta dos opciones:

- Basic Managment – Sólo permite realizar una configuración básica para asegurar conectividad al router.
- Extended Setup – Permite además configurar algunos parámetros globales y las interfaces.

Para abortar el desarrollo del modo setup se utiliza la combinación `Ctrl+C`

Al terminar el proceso, el sistema muestra la nueva configuración y requiere la confirmación para grabarla y utilizarla.

Modo EXEC:

Tiene dos niveles: modo **usuario** y modo **privilegiado.**

El modo usuario permite verificar el estado del router.

El modo privilegiado es el que permite acceder a los modos de configuración del router.

Para acceder al modo privilegiado se debe tipear ***enable***

Para salir del modo usuario, tipear **exit** en el prompt.

Modo de configuración global

Se accede utilizando el comando `configure.`

`Configure terminal`	Ingresa al modo de configuración global
`Configure network`	Copia a la RAM un archivo de configuración guardado en un servidor TFTP

`Configure memory`
Copia a la RAM un archivo de configuración guardado en el NVRAM.

Para salir del modo configuración tipear `exit` o `Ctrl + Z`

Passwords de acceso

1. Password de acceso a modo usuario. Se configuran diferentes password de acceso de acuerdo al modo de conexión.
   - Password de acceso por consola.
   - Password de acceso por puerto auxiliar.
   - Password de acceso por terminal virtual. Si no está configurada, no se podrá acceder al router por telnet.
2. Password de acceso a modo privilegiado.
   - Enable password – utilizada por el Cisco IOS 10.3 y anteriores.
   - Enable secret – utilizada por Cisco IOS 11.0 y siguientes.

Comando Help

Para enlistar todos los comandos disponibles en un determinado modo: ***?***

Para enlistar todos los comandos asociados que coomienzan con una secuencia de letras: ***cl?***

Para enlistar todos los subcomandos asociados a un comando: ***clock ?***

Para ver los parámetros asociados a un comando y sus subcomandos: ***clock set ?***

La tecla **TAB** completa los comandos por el operador.

Comandos de Edición

Ctrl	**+A**	Desplazarse al comienzo de la línea de comando
	+E	**[end]** Desplazarse al final de la línea de comando
	+B	**[back]** Desplazarse un carácter hacia atrás
	+F	**[forward]** Desplazarse un carácter hacia adelante
	+P / ↑	**[previous]** Hace aparecer el último comando
	+N / ↓	Hace asparecer nuevamente el comando más reciente
	+R	**[repeat] Repite el último comando**
	+D	**[delete]** Borra un carácter
	+K	Borra todo a la derecha del cursor
	+X	Borra todo a la izquierda del cursor
	+W	Borra una palabra
	+U	Borra una línea
Esc	**+B**	**[back]** Desplazarse una palabra hacia atrás
	+F	**[forward]** Desplazarse una palabra hacia delante
Retroceso		Borra un carácter a la izquierda del cursor
Tab		Completa un comando introducido parcialmente

>show history	Muestra buffer de comandos
>terminal history	Establece el tamaño del buffer de comandos
>no terminal editing	Inhabilita las funciones de edición avanzada
>terminal editing	Habilita las funciones de edición avanzada

Comandos show:

`show running-config:` Muestra los parámetros de configuración activos.

`show startup-config:` Muestra el archivo de configuración guardado.

`show ip route:` Muestra las entradas de la tabla de enrutamiento.

`show flash:` Muestra:

Memoria FLASH total del router
Memoria FLASH disponible
Nombre de la imagen del archivo del sistema.

Comandos varios:

`bandwidth 64`

Configura el parámetro ancho de banda (en Kb) que utilizan los protocolos de enrutamiento en el cálculo de la métrica. No tiene relación real con el ancho de banda del enlace.

`banner motd`

Permite insertar un mensaje para mostrar cuando se accede al router.

`copy tftp running-config`

Copia un archivo de configuración guardado en un servidor tftp a la RAM del router.

`copy tftp startup-config`

Copia un archivo de configuración guardado en un servidor tftp directamente a la NVRAM del router.

`copy startup-config running-config`

Copia la configuración almacenada en la NVRAM a la RAM del router.

`clock rate 64000`

Configura el temporizador (en bps) en el extremo DCE de un enlace serial.

`debug ipx routing activity`

Permite monitorear las actualizaciones IPX RIP enviadas y recibidas en un router.

`dialer list`

Permita crear un filtro de "tráfico interesante" para activar un enlace bajo demanda.

`interface ethernet 0.1`

Indica la primer subinterface sobre la interface Ethernet 0
El número de subinterface puede variar entre 1 y 4.292.967.295

`line console 0`

Comando para ingresar al modo de configuración del puerto consola.

`login`	Habilita la posibilidad de logearse introduciendo una password.
`password [xxxxxxxx]`	Configura la password de acceso.
`line vty 0 4`	Comando para ingresar al modo de configuración de las terminals virtuales (sesiones telnet).
`terminal monitor`	Permite derivar las salidas de los comando debug de la terminal de consola a las terminales virtuales.

7. ADMINISTRACIÓN DE UNA RED CISCO

Componentes de un router Cisco

Bootstrap	Se encuentra almacenado en el microcódigo de la ROM. Es responsable de que el router se inicialice y luego cargue el IOS.
POST	Se encuentra almacenado en el microcódigo de la ROM. Se utiliza para revisar las funcionalidades básicas del hardware del router y determinar las interfaces presentes.
monitor de ROM	Almacenado en el microcógido de la ROM. Se utilizar para realizar revisiones básicas y en las tareas de diagnóstico y resolución de fallos.
Mini-IOS	También denominado RXBOOT o bootloader. Es una versión reducida del IOS almacenada en la ROM que puede ser utilizado durante el arranque del dispositivo. Permite realizar varias operaciones de mantenimiento.
ROM **RAM**	Se utiliza para arrancar y mantener el router. En ella están almacenados el bootstrap, el POST, el monitor de ROM, y en algunos dispositivos el mini-IOS. Utilizada para almacenar paquetes, tablas de enrutamiento, software y datos que permiten al router cumplir sus tareas. La running-config (configuración dinámica) se almacena en la RAM, y el IOS también puede correr desde la RAM en algunos dispositivos. Esta memoria se vacía por completo al apagar o rebootear el dispositivo.
Memoria flash	Utilizada por el router para almacenar el Cisco IOS. No se borra cuando el router es apagado o rebooteado ya que es una memoria EEPROM.
NVRAM	En ella se almacena la configuración del dispositivo. Tampoco se borra cuando el dispositivo es apagado o rebooteado.
Registro de configuración	Controla algunas funciones durante el arranque del router. Sus valores pueden visualizarse con el comando show versión y típicamene es 0x2102.

Secuencia de Inicio

✓ Ejecuta el POST	
✓ Carga del Bootstrap	ROM
✓ Lectura del Registro de Configuración	NVRAM
✓ Carga del Cisco IOS	FLASH TFTP ROM

- ✓ Carga del Archivo de Configuración NVRAM
  TFTP

Contenido de las memorias

FLASH	Imagen del Cisco IOS
RAM	Running-config, tabla de enrutamiento, buffers de paquetes, etc.
ROM	Bootstrap, Imagen básica del Cisco IOS
NVRAM	Startup-config

Registro de Configuración

Registro de 16 bits guardado en la NVRAM.

0x2100 - Arranca en modo monitor ROM: indica que la carga del sistema operativo se realizará manualmente

0x2101 - Indica al router que deberé leer automáticamente el sistema operativo desde la ROM

0x2102 - Indica al router que debe examinar los commandos boot system en la NVRAM.

0x2142 - Indica que el router debe examinar los comandos bootsystems, pero ignorar la configuración almacenada en la NVRAM, forzando el modo setup. Es el registro utilizado en la secuencia de recuperación de password.

Procedimiento para recuperación de password

- Rebootear el dispositivo
- Interrumpir la secuencia de arranque
- Cambiar el registro de configuración a 0x2142
- Rebootear el router
- Ingresar en el modo privilegiado
- Copiar la configuración de la NVRAM a la RAM
- Cambiar la password de acceso a modo privilegiado
- Volver el registro de configuración a su valor original
- Rebootear el router

Procedimiento para efectuar una copia de resguardo y restaurar la imagen del IOS

1. Verificar la memoria flash

   `show flash`

2. Hacer una copia de resguardo del IOS

   `ping [ip del servidor tftp]`

   `copy flash tftp`

3. Restaurar o actualiza r la imagen del IOS

   `copy tftp flash`

4. Reinicio automático del router

Procedimiento para efectuar una copia de resguardo y restaurar el archivo de configuración

1. Verificar la configuración actual

   `show running-config`

2. Verificar la configuración almacenada en la NVRAM

   `show startup-config`

3. Copiar la configuración actual a la NVRAM

   `copy running-config startup-config`

4. Copiar la configuración actual a un servidor tftp

   `copy running-config tftp`

5. Restaurar la configuración desde un servidor tftp

   `copy tftp running-config`

   `copy tftp startup-config`

CDP Cisco Discovery Protocol:

Protocolo propietario de Cisco que permite recoger información sobre los dispositivos vecinos.

Por defecto todas las interfaces son CDP activas.

Parámetros CDP

CDP timer - período de tiempo entre transmisiones de paquetes CDP a todos los puertos activos.

CDP holdtime - período de tiempo que el dispositivo mantiene los paquetes recibidos.

`show cdp`

`cdp timer 90`

`cdp holdtime 180`

`no cdp run` - desactiva totalmente cdp en el router

`no cdp enable` - desactiva cdp en una interface

Verificación de información CDP

⇨ `show cdp neighborg`

ID de los dispositivos
interface local
holdtime
capacidad
plataforma
ID del puerto

⇨ `show cdp neighborg detail`

Hostname del colindante
IP del colindante
Versión del Cisco IOS
+ la información que muestra el comando anterior

- `show cdp entry *`

  Muestra la misma información

- `show cdp traffic`

- `show cdp interface`

Comandos relacionados con el acceso vía telnet:

`telnet [IP]`

`Ctrl+shift+6 luego x`	alterna entre sesiones telnet simultáneas.
`show sessions`	muestra conexiones con dispositivos remotos.
`show ussers`	muestra conexiones remotas al router.
`exit / disconnect`	cierra una sesión telnet propia.
`clear line #`	cierra una conexión telnet al propio dispositivo.

8. CONFIGURACIÓN DE NOVELL IPX

Stack de protocolos IPX

Aplicación, Presentación, Sesión	→	RIP IPX, SAP, NCP, NLSP, etc…
Transporte	→	SPX
Red	→	IPX
Enlace de Datos	→	ODL
Física	→	cualquiera

Tipos de Frame

Interface	Tipo de encapsulación Novell	Cisco Keyword
Ethernet	Ethernet 802.3 [1]	**novell-ether** (def.)
	Ethernet 802.2 [2]	sap
	Ethernet II	arpa
	Ethernet SNAP	snap
Token Ring	Token Ring	sap (def.)
	Token Ring_SNAP	**snap**
FDDI	FDDI SNAP	**snap** (def.)
	FDDI 802.2	sap
	FDDI RAW	novell-fddi
Serie	DIC	**Hdlc (def)**

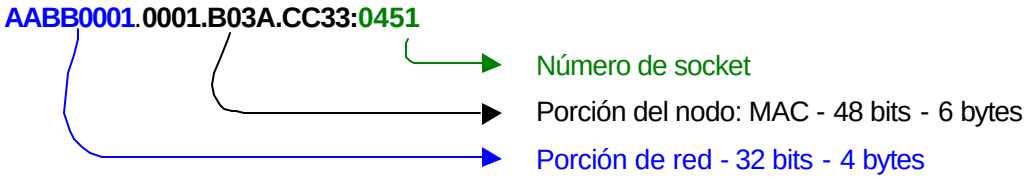
[1] Encapculación Novell por defecto en Novell NetWare 2 a 3.11

[2] Encapsulación Novell por defecto en Novell NetWare 3.12 y 4.x

Direccionamiento IPX

Jerárquico y dividido en porción de red y de nodo.

Esquema de direccionamiento de 80 bits (10 bytes), expresados en hexadecimales.



Atención: en cada porción, los ceros a la izquierda pueden ser omitidos.

Estructura cliente-servidor Novell Netware

GNS request (Get Nearest Server) - Broadcast - Requerimiento de determinado servicio por parte de un cliente Novell.

GNS reply - Respuesta del servidor Novell indicando la ubicación del servicio requerido.

Tabla SAP - Tabla mantenida por servidores y routers conteniendo la información de todos los servicios de red disponibles.
La tabla SAP de los routers contiene l a información referida a los servicios brindados por servidores instalados en otras redes, y responde con esta información las solicitudes GNS.

SAP (Service Advertising Protocol) - Broadcast - Protocolo que utilizan los servidores para ofrecer sus servicios. Tiempo de actualización 60 segundos.

RIP (Routing Information Protocol) - Broadcast - Información de enrutamiento intercambiada entre los servidores Novell. Tiempo de actualización: 60 segundos.
Métrica: ticks (1/18 segundo) y hops.

Activación de IPX en el router Cisco

Activación de enrutamiento IPX

Protocolo de vector distancia : RIP IPX

```
ipx routing
```

```
ipx maximum path [1 - 64]
```

IPX RIP envía actualizaciones cada 60 segundos

Métrica de Novel RIP: utiliza ticks (1/18 segundo) y saltos

Protocolo de estado de enlace:

NLSP Novell Protocolo de Enrutamiento de Estado de Enlace (Novell Link State Protocol):
Interactúa con RIP y SAP para facilitar la negociación y asegurar la compatibilidad con redes RIP que no necesitan enrutamiento por estado de enlace.

Habilitación de IPX en una interface

```
ipx network [#] encapsulation [tipo]
```

```
ipx network [#] encapsulation [tipo] secondary
```

Verificación y monitoreo de IPX

`show ipx route` muestra el contenido de las tables de enrutamiento ipx.

`show ipx servers`	muestra el contenido de las tables de servidores ipx.
`show ipx traffic`	muestra información acerca del número y tipo de paquetes ipx recibidos y transmitidos por el router.
`show ipx interface`	muestra el estado y estadísticas de tráfico de las interfaces ipx.
`show protocols`	
`debug ipx routing activity`	
`debug ipx sap activity`	
`debug ipx routing events`	
`ping ipx [ipx address]`	

9. ADMINISTRACIÓN DEL TRÁFICO UTILIZANDO ACL

Reglas de funcionamiento de ACL

- Cada paquete que ingresa en la interface es comparado con cada línea de la lista secuencialmente.
- La comparación se sigue realizando hasta tanto se encuentre una coincidencia. Una vez que el paquete cumple la condición de una línea, se ejecuta la acción indicada y no se sigue comparando.
- Hay un deny all implícito al final de cada lista de acceso.
- Tener en cuenta que al activar listas de acceso el router automáticamente conmuta de fast switching a process switching.
  - Fast Switching – Feature de los routers Cisco que utiliza un cache del router para conmutar rápidamente los paquetes hacia el puerto de salida sin necesidad de seleccionar la ruta para cada paquete que tiene una misma dirección de destino.
  - Process Switching – Operación que realiza una evaluación completa de la ruta por paquete. Implica la transmisión completa del frame al CPU del router donde será re-encapsulado para ser entregado a través de la interface de destino. El router realiza la selección de la ruta para cada paquete. Es la operación que requiere una utilización más intensiva de los recursos del router.

Tipos de listas para IP e IPX

- **Listas de acceso estándar** - Listas IP: utilizan únicamente direcciones IP de origen. Listas IPX: utilizan direcciones IPX de origen y destino.
- **Listas de acceso extendidas** - Listas IP: verifican direcciones de origen y destino, protocolo de capa 3 y puerto de capa 4. Listas IPX: igual (en capa 4, el número de socket).
- **Listas de acceso nombradas –** Listas de acceso IP que verifican direcciones de origen y destino, procolos de capa 3 y puertos de capa 4, identificadas con una cadena de caracteres alfanuméricos. A diferencia de las listas de acceso numeradas, se configuran en un submodo propio y son editables.
- **Filtros IPX SAP** - Se utilizan para controlar el tráfico de paquetes SAP
- **Lista de acceso entrante –** Controlan el tráfico que ingresa al router a través del puerto en el que está aplicada, y antes de que sea conmutado a la interface de salida.
- **Lista de acceso saliente –** Controlan el tráfico saliente del router a través del puerto en que está aplicada, una vez que ya ha sido conmutado.

Número de lista de accesso:

1-99	IP estándar
100-199	IP extendida
200-299	Protocol type code
300-399	DECnet
400-499	XNS estándar
500-599	XNS extendida

600-699	AppleTalk
700-799	48 bit MAC address estándar
800-899	IPX estándar
900-999	IPX extendida
1000-1099	IPX SAP
1100-1199	48 bit MAC address extendida
1200-1299	IPX summary address

Números de puerto

Echo	= 7	
FTP	= 21	TCP
Telnet	= 23	TCP
SMTP	= 25	TCP
DNS	= 53	UDP
DHCP	= 67	UDP
TFTP	= 69	UDP
HTTP	= 80	TCP
POP3	= 110	
SNMP	= 161	
IRC	= 194	

Configuración de las listas

Listas de acceso IP estándar

```
Router(config)#access-list [1-99] [permit/demy] [IP origen]
Router(config-if)#ip access-group [1-99] [in/out]
```

Listas de acceso IP extendida

```
Router(config)#access-list [100-199] [permit/demy] [protocolo][IP
               origen] [IP destino] [tipo servicio]
Router(config-if)#ip access-group [100-199] [in/out]
```

Listas de acceso IP nombradas

```
Router (config)#ip access-list [standard/extended] [nombre]
```

Para configurar una lista de acceso nombrada estándar:

```
Router (config-std-nacl)# [permit/demy] [IP origen]
```

Para configurar una lista de acceso nombrada extendida:

```
Router (config-ext-nacl)# [permit/demy] [protocolo][IP origen] [IP
              destino] [tipo servicio]
```

Listas de acceso IPX estándar

```
Router(config)#access-list [800-899] [permit/demy] [red IPX origen]
               [red IPX destino]
Router(config-if)#ipx access-group [800-899] [in/out]
```

Listas de acceso IPX extendida

```
Router(config)#access-list [900-999] [permit/demy] [protocolo][red
               IPX origen] [red IPX destino] [socket]

Router(config-if)#ip access-group [900-999] [in/out]
```

Filtros IPX SAP

```
Router(config)#access-list [1000-1099] [permit/demy] [red IPX origen]
                [servicio]

Router(config-if)#ipx [input/output]-sap-filter
```

Aplicar filtros a las terminales virtuales

```
Router(config)#access-list 10 permit 172.16.10.3

Router(config)#line vty 0 4

Router(config-line)#access-class 10 in
```

Comandos especiales

`xxx.xxx.xxx.xxx 0.0.0.0`	= host xxx.xxx.xxx.xxx
`0.0.0.0 255.255.255.255`	= any
`-1`	= any IPX network

Para insertar comentarios en una lista de acceso:

= `remark` en lugar de la opción permit/deny

Monitoreo de las listas

`show access-list [#]`	muestra el contenido de todas las ACL o una en particular
`show ip access-list`	muestra solamente la configuración de ACL IP
`show ipx access-list`	muestra solamente la configuración de ACL IPX
`show ip interface`	muestra los puertos que tienen aplicadas ACL IP
`show ipx interface`	muestra los puertos que tienen aplicadas ACL IPX
`show running-config`	muestra tanto las listas de acceso configurada, como la aplicación a cada interface

Tips de aplicación

- Organice su lista de acceso de modo que los criterios más específicos estén al comienzo de la misma.
- Sólo se puede asignar una lista de acceso por interface.
- No se puede remover una única línea de una lista de acceso numerada (no son editables).
- Cada vez que agrega una línea a la lista de acceso, esta se ubicará a continuación de las líneas existentes.
- Toda lista debe incluir al menos un comando permit.
- Las listas no filtran el tráfico originado en el router.
- Las listas de acceso estándar deben colocarse lo más cerca posible del destino del tráfico.

- Las listas de acceso extendidas deben colocarse lo más cerca posible del origen del tráfico que será denegado.

10. PROTOCOLOS WAN

Premisas en el Equipamiento del Usuario

Punto de Demarcación - Es el lugar en el que el CPE se conecta con el loop local del proveedor. Marca el último punto de responsabilidad del proveedor de servicios.

Loop local – Conecta el punto de demarcación con el switch del proveedor de servicio más próximo.

CO - Central Office – Oficina de telefonía local a la cual todos los loops locales de un área están conectados y en la cual se conmuta el circuito del suscriptor.

CPE – Customer Premises Equipment – Dispositivo ubicado en la locación del suscriptor de servicios, al que se conecta el loop del proveedor de servicio.

DTE y DCE – La capa física WAN describe la interface entre el Data Terminal Equipment (**DTE**) y el Data Circuit terminating Equipment (**DCE**). Típicamente el DCE es el Service Provider, y el DTE es dispositivo adjunto a la red.

Tipos de conexión WAN

- Líneas Dedicadas

  Línea de comunicación WAN preestablecida desde el CPE local hasta el CPE remoto a través de una nube DCE.

  Brinda servidios full-time, sin requerir procedimientos de inicialización antes de iniciar la transmisión de datos.

  Utiliza líneas seriales sincrónicas de hasta 45 Mbps.

- Redes de Circuito Conmutado

  Sus servicios pueden ser activados bajo demanda. La transferencia de datos no se puede realizar hasta tanto no esté establecida la conexión extremo a extremo.

  Es utilizada cuando se requieren tranferencia de bajo ancho de banda.

- Redes de Paquetes Conmutados

  Tecnología que permite compartir el ancho de banda entre diferentes usuarios tomando como base el concepto de transmisión por ráfagas. Ofrece tasas de transmisión que van desde 56 Kbps hasta 2.048 Mbps.

Protocolos WAN:

HDLC	High-level Data Link Control (en su versión propietaria, es el default de Cisco para enlaces seriales)
SDLC	Synchronous Data Link Control
LAPB	Link Access Procedure, Balanced
X.25	
Slip	
PPP	Point to Point Protocol
Frame Relay	

HDLC
High Level Data Link Control:

Protocolo estándar, derivado de SDLC y desarrollado por ISO, que ha sido implementado de diferentes formas por cada fabricante.

Especifica un formato de encapsulación de frame para enlaces de datos sincrónicos, orientado a la conexión.

Utilizado para trabajar sobre líneas punto a punto dedicadas.

HDLC propietario de Cisco

Encapsulación por defecto en los enlaces seriales de dispositivos Cisco.

Soporta enlaces punto a punto sobre líneas sincrónicas.

No proporciona autenticación u otros servicios adicionales.

El campo Propietario es el que le permite transportar múltiples protocolos de capa 3.

Flag	Dirección	Control	Propietario	Datos	FCS	Flag

PPP

Protocolo de encapsulación de capa 2 que puede ser utilizado tanto sobre enlaces sincrónicos como asincrónicos.

Su propósito básico es transportar paquetes de capa 3 a través de enlaces de datos punto a punto.

Componentes Principales

- **EIA/TIA 232 C** – Estándar de capa física para comunicaciones seriales.
- **HDLC** – Método de encapsulación estándar de datagramas sobre enlaces seriales. Lo utiliza para la transferencia de datos.
- **LCP** – Método para estableces, configurar, mantener y terminar enlaces punto a punto.
- **NCP** – Método para establecer y configurar diferentes protocolos de capa de red (IP, IPX, Apple Talk, etc). De este modo permite el uso simultáneo de múltiples protocolos de capa 3. Este no es un protocolo de capa 3.

Etapas de establecimiento de una sesión PPP

1. Fase de establecimiento de la conexión
   Se envían paquetes LCP para configurar y probar el enlace. Utilizan el campo configuración para configurar opciones, si no hay opciones en el campo se utilizan las opciones por defecto.
2. Fase de autenticación (opcional)
   Se ejecuta si se seleccionó PAP o CHAP como procedimientos de autenticación.
3. Fase de protocolo de red
   Se envían paquetes NCP.
4. Fase de cierre de la sesión

Opciones de configuración de LCP

- Autenticación
  - PAP
    Envía password en texto plano.
    Sólo autentica el establecimiento de la sesión.
  - CHAP

Autentica en el establecimiento de la sesión y periódicamente durante la sesión envía un valor de desafío que si no es respondido correctamente cancela la sesión.

- Compresión
  - Stacker
  - Predictor
- Detección de errores
  - Quality
  - Magic Number
- Multilink

Comandos de configuración

```
Router#config terminal
Router(config)#interface serial0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication [chap/pap]
```

Comandos para verificar encapsulación

```
Router#show interface serial0
Router#show running-config
```

Frame Relay

Provee servicios de conmutación de paquetes orientados a la conexión a través de circuitos virtuales, sin detección de errores.

Surge a partir de los trabajos conjuntos del denominado Grupo de los Cuatro: Cisco Systems, Strata Com, Northern Telecom, y la Digital Equipment Corporation. A partir de este desarrollo luego tuvo lugar el estándar de la IETF.

Sus circuitos virtuales son conexiones lógicas entre dos dispositivios DTE a través de una red de paquetes conmutados. Ambos DTEs se identifican por un DLCI.

El servicio de circuitos virtuales asegura una ruta completa hacia la red de destino antes de enviar la primer trama.

Utiliza tanto

- PVC – Permanent Virtual Circuits
- SVC – Switched Virtual Circuits

Dos formas de encapsulación Frame-Relay:

Cisco (por defecto)	`encapsulation frame-relay`
IETF RFC 1490	`encapsulation frame-relay ietf`

DLCI – Data Link Connection Identifiers

Identificador del circuito Frame Relay, que permite diferencias entre diferentes circuitos virtuales en la red.

Es asignado por el proveedor de servicio, a partir de 16.

Se pueden asociar varios DLCI a una única interface, cuando se trata de una interface frame-relay multipoint.

```
frame-relay interface-dlci [16-1007]
```

Cada dirección IP debe ser mapeada a un DLCI. Este mapeo puede ser:

- Dinámico: utilizando el protocolo IARP
- Manual: utilizando el comando map

```
frame-relay map ip [x.x.x.x] [dlci]
```

El DLCI puede tener significancia tanto local como global.

LMI – Local Management Interface:

Método de señalización entre el dispositivo CPE y el switch Frame Relay, responsable de mantener y administrar el enlace entre ambos dispositivos. Desarrollado por el Grupo de los Cuatro en 1990.

Provee información acerca del keeptalive verificando el flujo de datos, multicast, direcciónamiento multicast y estado del circuito virtual.

Actualiza el estatus del circuito a tres diferentes estados:

Activo – Los routers pueden intercambiar información.

Inactivo – La interface del router local está operativa, pero el router remoto no e stá trabajando.

Deleted – No se está recibiendo información LMI desde el switch.

Tipos de LMI:

- Cisco – Propietario, por defecto en los dispositivos Cisco

```
frame-relay lmi-type cisco
```

- ANSI – estándar T1.617

```
frame-relay lmi-type ansi
```

- ITU-T (q933a) – estándar de ITU-T

```
frame-relay lmi-type q933a
```

A partir del Cisco IOS 11.2 la configuración del tipo de LMI es autosentiva.

Subinterfaces sobre el enlace serial:

Permite definir varios circuitos virtuales sobre una misma interface física tratándolos como si se tratara de diferentes interfaces.

Tipos:

- Punto a punto - Circuito que conecta un router con otro. Requiere su propia red o subred.

```
Interface serial 0.16 multipoint
```

- Multipunto - Interface que se constituye en centro de una estrella de circuitos virtuales. Utiliza una única red o subred para todas las interfaces conectadas.

```
Interface serial 0.16 point-to-point
```

Control de congestión:

Frame Relay permite implementar mecanismos simples de notificación de saturación. No constituyen un control de flujo explícito.

- **DE Discard Eligibility -** Bit en el encabezado FR que identifica el tráfico "excedente" respecto del CIR. Cuando la interface Frame Relay detecta tráfico excedente en el enlace coloca el bit DE en on. De este modo los switches de la red Frame Relay –en caso de congestión de los enlaces - descartan estos paquetes en primer lugar.
- **FECN Forward-Explicit Congestion Notification -** Controlado por un bit incluido en el campo de direcciones del encabezado de la trama Frame Relay. Si la red está

saturada los switches fijan el bit FECN en 1, de este modo notifican al dispositivo destino que la ruta está congestionada.

- **BECN Backward-Explicit Congestion Notification -** Los switches fijan el valor de este bit en 1 en las tramas que viajan en sentido contrario de las tramas con FECN en 1, notificando así al dispositivo de origen, de modo que disminuya la tasa de envío de paquetes.

CIR - Committed Information Rate

Especifica la cantidad máxima de datos ingresados en la red Frame Relay cuya transmisión se garantiza. Si la cantidad de información excede el CIR, su acarreo no está garantido.

Monitoreo de Frame Relay

```
show frame-relay lmi
show frame-relay pvc
show interface
show frame-relay map
clear frame-relay inarp
debug frame-relay lmi
```

ISDN - Integrated Service Digital Network

RDSI - Red Digital de Servicios Integrados

Es un conjunto de protocolos de comunicación propuestos por compañías telefónicas, diseñados para suministrar múltiples servicios sobre una misma red de comunidaciones.

Componentes ISDN

Network Termination:

- **NT1 -** Implementa especificaciones y conectores propias del dispositivo de usuario de una red ISDN. Se conecta con una interface de 4 pares hacia la red del usuario, y de 2 pares con el loop de conexión local.
- **NT2:** Equipo del proveedor como un switch o PBX que permite la conexión de varios dispositivos ISDN.

Terminal Equipment (dos tipos básicos)

- **TE1 -** Terminal especializada ISDN. Se conecta directamente a la red ISDN con un par trenzado de 4 pares.
- **TE2 -** Terminal no ISDN. Se conecta a la red ISDN a través de un TA.
- **TA Terminal Adaptor -** puede ser tanto un dispositivo separado como estar dentro del TE2. Convierte el cableado tradicional en el propio de ISDN para poder conectarse a un NT1.

Interfaces ISDN

R: Entre un dispositivo no-ISDN (TE2) y un TA.

S: Interface de conexión a un NT2.

T: Interface de conexión a un NT1.

U: Entre un dispositivo NT1 y el equipamiento de la red de transporte.

Código de los protocolos ISDN:

E: Regulan el uso de ISDN sobre líneas telefónicas existentes.

I: Regulan conceptos, terminos y servicios

Q: Cubren aspectos de conmutación, señalización y configuración de llamadas

Tipos de switch ISDN:

AT&T BRI switch	`isdn switch-type basic-sess`
Nortel DMS-100 BRI	`isdn switch-type basic-dms100`
National ISDN-1	`isdn switch-type basic-ni1`
AT&T 4ESS (ISDN-PRI)	`isdn switch-type primary-4sess`
AT&T 5ESS (ISDN-PRI)	`isdn switch-type primary-5sess`
Nortel DMS-100 (ISDN-PRI)	`isdn switch-type primary-dms100`

ISDN BRI Basic Rate Interface 2B+1D

2 canales B de 64 Kbps - transportan datos

1 canal D de 16 Kbps - transporta información de control y señalización. Utiliza encapsulación LAPD en la capa 2

Ancho de banda total: 144 Kbps

Requiere la implementación de 1 SPID (Service Profile Identifier) por cada canal B.

ISDN PRI Primary Rate Interface 23B+1D / 30B+1D

Estados Unidos y Japón

23 canales B de 64 Kbps

1 canal D de 64 Kbps

Ancho de banda total: 1.544 Mbps

Europa y Australia

30 canales B de 64 Kbps

1 canal D de 64 Kbps

Ancho de banda total: 2.084 Mbps

Servicio	Composición	Ancho de Banda
BRI	2B+D	144 Kbps
PRI T1	23B+D	1.544 Mbps
PRI E1	30B+D	2.084 Mbps

Protocolos de encapsulación de capa 2

PPP

HDLC

LAPD

Configuración de una interface ISDN/BRI en un Cisco 2500

```
isdn switch-type basic-ne1
```

```
interface bri0
encapsulation ppp
isdn spid1 086506610100 8650661
isdn spid2 086506620100 8650662
```

Comandos adicionales para configurar DDR

```
dialer-list [#] protocol [ip/ipx] permit
dialer-list [#] list [# access-list]
dialer-group [#]
dialer-string 8650662
dialer idle-timeout [xx segundos]
dialer load-threshold 2 either
hold-queue [# paquetes] in
isdn disconnect interface bri0
```

Monitores de tráfico ISDN

```
show dialer
show isdn active
show isdn status
debug isdn q921
debug isdn q931
debug dialer
```

Velocidades de conexión

Tecnología	Velocidad de transmisión	Distancia límite
Módem convencional	56 Kbps de downstream y hasta 33.6 Kbps de upstream	No tiene
ISDN	A partir de 128 Kbps simétricos	18.000 pies
E1	Enlace punto a punto dedicado de 2,048 Mbps, compuesto por 32 canales de 64 Kbps: 30 canales de voz, 1 canal de control y 1 canal de sincronización	6.000 pies
T1		
E2	Enlace punto a punto dedicado de 8,848 Mbps. Equivale a 4 E1.	
T2		
E3	Enlace punto a punto dedicado de 34,368 Mbps. Equivale a 16 E1.	
T3		
E4	Enlace punto a punto dedicado de 139,26 Mbps. Equivale a 4 E3.	
E5	Enlace punto a punto dedicado de 565,148 Mbps.	

	Equivale a 4 E4.	
Cable módem	Hasta 30 Mbps de downstream y 10 Mbps de upstream	30 millas
DSL	Tecnología de transmisión de datos sobre pares de cobre de líneas telefónicas existentes. Con tasas de transmisión simétricas o asimétricas de entre 16 Kbps y 52 Mbps	
ADSL	1,5 a 8 Mbps de downstream y hasta 1,544 Mbps de upstream	18.000 pies
SDSL	1,544 a 2,048 Mbps simétricos	10.000 pies
HDSL	1,544 a 2,048 Mbps simétricos sobre 3 líneas telefónicas	12.000 pies
VDSL	13 a 52 Mpbs de downstream y 1,5 a 2,3 Mbps de upstream	4.500 pies
RADSL	Servicio ADSL que verifica la longitud y cualidad de la línea antes de establecer la conexión, y ajusta la velocidad de la línea en consecuencia.	

11. ANEXO 1: COMANDOS IOS PARA MONITOREO

A. Comandos de monitoreo del router

show sessions / show users

Permiten visualizar:

- ✓ show sessions: las sesiones telnet abiertas desde mi router hacia otros dispositivos.
- ✓ show users: las sesiones telnet abiertas en mi router desde otros dispositivos.

```
Router>show sessions
Conn Host               Address            Byte  Idle Conn Name
* 1  172.16.20.2        172.16.20.2        0     1    172.16.20.2
```

```
Router>show users
  Line     User      Host(s)                Idle Location
* 0 con 0           172.16.20.2            00:07:52
```

show flash

Permite visualizar el contenido de la memoria flash. Como aquí se aloja la imagen del Cisco IOS, permite conocer la información pertinente al archivo del Cisco IOS: tamaño (length) expresado en bytes, y nombre (name/status).

Adicionalmente informa la cantidad total de memora flash disponible (este dato se requiere al intentar una actualización de IOS, junto con la cantidad de memoria RAM).

Utilice este comando siempre que se requiera conocer el tamaño y nombre de la imagen del Cisco IOS almacenado en la RAM del router.

Se ejecuta tanto en modo usuario como privilegiado.

```
Router>show flash
System flash directory:
File  Length   Name/status
  1   10218508  /c2500-js-l_120-8.bin
[10218572 bytes used, 6558644 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```

Anotaciones

```
System flash directory:
File  Length   Name/status
  1   10218508  /c2500-js-l_120-8.bin
```

- ✓ File: indica el número de la imagen del IOS. Si no se especifica lo contrario, el router levantara la imagen cuyo número de "file" es menor.
- ✓ Length: tamaño del archivo en bytes
- ✓ Name/status: nombre y estado del archivo. El estado aparece en el caso en que el archivo haya sido re-escrito [recopied], ya que mantiene el archivo original y lo marca como [invalidated]. Esta marca también aparece cuando se ha hecho una copia defectuosa de una imagen. En este caso el nombre de la imagen (c2500-js-

l_120-8.bin) indica que se trata de una imagen versión 12.0 para un router Cisco 2500

`[10218572 bytes **used**, 6558644 **available**, 16777216 **total**]`

- ✓ Este dispositivo en particular, cuenta con 16 MB de memoria Flash.
- ✓ La imagen actual del IOS ocupa un total de 10 MB.
- ✓ La segundas cifra, indica el total de memoria flash aún disponible (en bytes).

`**16384**K bytes of processor board System flash (Read ONLY)`

- ✓ Tamaño total de la memoria flash expresado en KB
- ✓ Read Only indica que se trata de la partición en la que está alojada la imagen del IOS actualmente en ejecución.

show version

Permite visual izar información correspondiente a las versiones de hardware y software disponibles en el dispositivo.

Este comando indica la versión de la imagen del Cisco IOS residente en la ROM, la versión del Bootstrap, el tiempo de encendido del dispositivo y la forma en que fue inicializado. Particularmente, indica los valores de configuración del registro de configuración. Buena parte de esta información es mostrada en la consola durante el proceso de arranque del dispositivo.

Este es el único comando que le permite conocer los valores actuales del registro de configuración. Aquí también puede visualizarse el valor que se ha dado al registro de configuración luego de cambiarlo y antes de reiniciar el equipo. En este caso muestra el valor actual y entre paréntesis el valor que adoptará al inicializarse la próxima vez.

Se ejecuta tanto en modo usuario como privilegiado.

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(8), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 29-Nov-99 14:52 by kpma
Image text-base: 0x03051C3C, data-base: 0x00001000
ROM: System Bootstrap, Version 11.0(10c)XB1, PLATFORM SPECIFIC RELEASE
SOFTWARE
(fc1)
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c)XB1,
PLATFORM
SPECIFIC RELEASE SOFTWARE (fc1)

Router uptime is 2 hours, 26 minutes
System restarted by reload
System image file is "flash:/c2500-js-l_120-8.bin"

cisco 2500 (68030) processor (revision M) with 6144K/2048K bytes of memory.
Processor board ID 17048803, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Ethernet/IEEE 802.3 interface(s)
```

```
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102
```

Anotaciones:

```
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Versio n 12.0(8), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 29-Nov-99 14:52 by kpma
Image text-base: 0x03051C3C, data-base: 0x00001000
```

- ✓ Información referida a la versión de Cisco IOS residente en la ROM del router.

```
ROM: System Bootstrap, Version 11.0(10c)XB1, PLATFORM SPECIFIC RELEASE
SOFTWARE
(fc1)
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c)XB1,
PLATFORM
SPECIFIC RELEASE SOFTWARE (fc1)
```

- ✓ Información referida a la versión del programa de bootstrap.

```
Router uptime is 2 hours, 26 minutes
System restarted by reload
```

- ✓ Tiempo transcurrido desde la puesta en funcionamiento del dispositivo
- ✓ Procedimiento por el cual se inició el dispositivo.

```
System image file is "flash:/c2500-js-l_120-8.bin"
```

- ✓ Nombre de la imagen del IOS almacenada en la memoria flash.

```
cisco 2500 (68030) processor (revision M) with 6144K/2048K bytes of memory.
Processor board ID 17048803, with hardware revision 00000000
```

- ✓ Información del hardware del equipo.

```
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
```

- ✓ Información sobre interfaces con que cuenta el dispositivo.

```
32K bytes of non-volatile configuration memory.
```

- ✓ Cantidad de memoria NVRAM expresada en KBytes.

```
16384K bytes of processor board System flash (Read ONLY)
```

- ✓ Cantidad de memoria flash expresada en KBytes.

```
Configuration register is 0x2102
```

- ✓ Valor del registro de configuración.

- ✓ Si el registro de configuración hubiera sido cambiado, el nuevo valor aparecería entre paréntesis.

B. Comandos de monitoreo de cdp

CDP es un protocolo de capa 2 que permite recoletacr información de dispositivos colindantes. Se encuentra activido por defecto en todos los dispositivos Cisco. Es un protocolo propietario de Cisco.

Este conjunto de comandos, junto a show interface y show controllers, nos permiten hacer un relevamiento de la topología en la que estamos trabajando.

Todos los subcomandos correspondientes a show cdp se ejecutan en modo privilegiado.

show cdp

Show CDP muestra loa información global de configuración de CDP, incluyendo los timers.

Este comando se ejecuta en modo privilegiado.

```
Router#show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
```

```
Router#show cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  <cr>
```

Anotaciones:

```
Global CDP information:
        Sending CDP packets every 60 seconds
```

- ✓ Tiempo envío de paquetes de actualización de CDP

```
        Sending a holdtime value of 180 seconds
```

- ✓ Valor de holdtime.

show cp traffic

Muestra las estadísticas de tráfico CDP.

```
Router#show cdp traffic
CDP counters :
        Packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
```

Anotaciones:

```
CDP counters :
        Packets output: 0, Input: 0
```

- ✓ Conta dores de paquetes CDP recibidos y enviados.

```
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
```

```
No memory: 0, Invalid packet: 0, Fragmented: 0
```

- ✓ Estadística del tráfico CDP

show cdp neighbors

Permite visualizar la información correspondiente a los dispositivos colindantes recogida utilizando cdp.

Utilice este comando siempre que requiera verificar la conectividad de capa 2, e identificar la conexión con los dispositivos vecinos.

Se ejecuta en modo privilegiado.

```
Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch,s H - Host, I - IGMP, r - Repeater
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Sistemas         Eth 0             238        S           1900      1
Casa_Central     Ser 0             138        R           2621      Ser 0/0
Server_Farm      Ser 1             138        R           2500      Ser 0
```

Anotaciones:

Información que brinda:

- ✓ Hostname de cada uno de los dispositivos colindantes.
- ✓ Interface local a través de la cual nos conectamos al colindante.
- ✓ Holdtime.
- ✓ Capacidad del dispositivo vecino: routing, switiching, etc.
- ✓ Plataforma o modelo del dispositivo colindante.
- ✓ Puerto del dispositivo colindante al cual estamos conectados.

show cdp neighbors detail

Proporciona información detallada acerca del hardware, software y configuración de protocolos de enrutamiento de cada uno de los dispositivos colindantes.

Este comando nos permite hacer un relevamiento de la estructura y estado de nuestra red a partir de un dispositivo en particular.

```
Router#show cdp neighbors detail
-------------------------
Device ID: Sistemas
Entry address(es):
  IP address: 172.16.30.2
Platform: 1900,  Capabilities: Switch
Interface: Ethernet0,  Port ID (outgoing port): 1
Holdtime : 166 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C1900 Software (C1900-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE
(fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 19-Aug-99 17:29 by kpma:
```

```
advertisement version: 1
-------------------------
Device ID: Casa_Central
Entry address(es):
  IP address: 172.16.10.1
Platform: 2621,  Capabilities: Router
Interface: Serial0,  Port ID (outgoing port): Ser 0/0
Holdtime : 166 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 28-Apr-99 17:29 by kpma:


advertisement version: 1
-------------------------
Device ID: Server_Farm
Entry address(es):
  IP address: 172.16.20.2
Platform: 2500,  Capabilities: Router
Interface: Serial1,  Port ID (outgoing port): Ser 0
Holdtime : 166 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2500 Software (C2500-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE
(fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 03-May-99 17:29 by kpma:


advertisement version: 1
```

Anotaciones:

Device ID: Server_Farm

- ✓ Hostname del dispositivo vecino. También podemos conocerlo utilizando show cdp neighbors.

Entry address(es):
IP address: 172.16.20.2

- ✓ Información de configuración de capa 3 del dispositivo identificado previamente. Me permite conocer la dirección del puerto vecino.

Platform: 2500, **Capabilities**: Router

- ✓ Información referida a plataforma y capacidad del dispositivo colindante. Esta información también se accede a través de show cdp neighbors.

Interface: Serial1, **Port ID (outgoing port)**: Ser 0

- ✓ Interface local a través de la cual nos conectamos al dispositivo colindante.
- ✓ ID del puerto del dispositivo colindante al cual estamos conectados.

Holdtime : 166 sec

- ✓ Tiempo de espera.

```
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2500 Software (C2500-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE
(fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 03-May-99 17:29 by kpma:

advertisement version: 1
```

- ✓ Información correspondiente a la versión del sistema operativo que corre en el dispositivo vecino.

show cdp entry

Brinda información detallada acerc a del hardware, software y configuración de protocolos de enrutamiento de cada uno de los dispositivos colindantes, permitiendo especificar el nombre del dispositivo del que queremos recibir información. Si se utiliza un asterisco en lugar del nombre, se obtiene la misma información que con show cdp neighbors detail.

También se ejecuta en modo privilegiado..

Este comando tiene dos opciones adicionales: protocol y versión, que nos permiten ver la información sobre los protocolos de direccionamiento habilitados en el dispositivo colindante y la versión de software actualmente ejecutándose.

En cuanto a la descripción de la salida general, es igual a la de show cdp neighbors detail.

```
Router#show cdp entry Sistemas
-------------------------
Device ID: Sistemas
Entry address(es):
  IP address: 172.16.30.2
Platform: 1900,  Capabilities: Switch
Interface: Ethernet0,  Port ID (outgoing port): 1
Holdtime : 166 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C1900 Software (C1900-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE
(fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 19-Aug-99 17:29 by kpma:


advertisement version: 1
```

C. Comandos de monitoreo de interfaces

show protocols

Este comando permite revisar la información correspondiente a configuración de protocolos enrutados actualmente activos en mi router. y el estado de cada una de las interfaces.

Es un excelente recurso para tener una visión general del estado de todas las interfaces del dispositivo.

Si tengo configuradas direcciones IPX o Apple Talk, podría revisarlas también con este comando.

Se ejecuta solo modo usuario como privilegiado.

No brinda información sobre protocolos de enrutamiento.

.

```
Router#show protocols
Global values:
  Internet Protocol routing is enabledss
Ethernet0 is up, line protocol is up
  Internet address is 172.16.30.1/24
Serial0 is up, line protocol is up
  Internet address is 172.16.10.2/24
Serial1 is up, line protocol is up
  Internet address is 172.16.20.1/24
```

Anotaciones:

```
Global values:
Internet Protocol routing is enabled
```

- ✓ Se encuentra habilitado el enrutamiento por IP. Corresponde al comando ip routing.

Ethernet0 is up, line protocol is up

- ✓ Informa sobre el estado de una interface en particular. Es la misma línea de información que muestra el comando show interface. La primera referencia es la conectividad física (capa 1), la segunda a la conectividad de capa de enlace de datos.

Internet address is 172.16.30.1/24

- ✓ Configuración de direccionamiento de capa 3. En este caso nos indica la dirección IP del puerto y la máscara de subred.

show interface

Comando que permite revisar el estado, configuración y estadística de todos o cada uno de los puertos del dispositivo.

Se ejecuta solo en modo privilegiado.

Si no se especifica un puerto brinda la información de todos los puertos del dispositivo. La información brindada es diferente según la configuración de cada puerto.

```
Router#show interface serial0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Description:
  Internet address is 172.16.10.2
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
```

```
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   0 packets output, 0 bytes, 0 underruns
   0 output errors, 0 collisions, 17 interface resets
   0 output buffer failures, 0 output buffers swapped out
   0 carrier transitions
   DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
```

Posibles resultados de show interface

- `Serial0 is` **`down`**`, line protocol is` **`down`**
  Posible fallo de capa física.
- `Serial0 is` **`administratively down`**`, line protocol is` **`down`**
  Interface desabilitada por el Administrador.
- `Serial0 is` **`up`**`, line protocol is` **`down`**
  Posible fallo en la capa de enlace de datos: diferente encapsulación.
- `Serial0 is` **`up`**`, line protocol is` **`up`**
  Interface operativa a nivel de capa 1 y 2.

Anotaciones:

`Serial0 is up, line protocol is up`

- ✓ Indica el estado de ls interface al nivel de capa 1 y 2.

```
Hardware is HD64570
Description:
Internet address is 172.16.10.2
```

- ✓ Dirección IP configurada en el puerto. Si quisiera ver una dirección de IPX, debería especificar esto en el comando: show ipx interface serial 0.

`MTU` `1500 bytes,` **`BW`** `1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255`

- ✓ MTU: tamaño máximo de los paquetes transmitidos por el puerto, expresado en bytes.
- ✓ BW: Ancho de banda digital asignado al puerto.

`Encapsulation` `HDLC, loopback not set, keepalive set (10 sec)`

- ✓ Encapsulación del frame activida. En este caso muestra la encapsulación por defecto para enlaces seriales Cisco.

```
Last input never, output never, output hang never
Last clearing of "show interface" counters never
```

- ✓ Tiempo en segundos desde que se pusieron los contadores en cero.

`Queueing strategy``: fifo`

- ✓ Estrategia para el despacho de paquetes en la cola de este puerto. FIFO: First In First Out.

```
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 17 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

- ✓ Contadores de paquetes del puerto.

```
DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
```

```
Router#show controllers serial 0
HD unit 0, idb = 0x1076CC, driver structure at 0x10CB58
buffer size 1524  HD unit 0, V.35 DCE cable
cpb = 0x61, eda = 0x4940, cda = 0x4800
RX ring with 16 entries at 0x614800
00 bd_ptr=0x4800 pak=0x10FBEC ds=0x61ECC8 status=00 pak_size=0
01 bd_ptr=0x4814 pak=0x10F9E8 ds=0x61E60C status=00 pak_size=0
02 bd_ptr=0x4828 pak=0x10F7E4 ds=0x61DF50 status=00 pak_size=0
03 bd_ptr=0x483C pak=0x10F5E0 ds=0x61D894 status=00 pak_size=0
04 bd_ptr=0x4850 pak=0x10F3DC ds=0x61D1D8 status=00 pak_size=0
05 bd_ptr=0x4864 pak=0x10F1D8 ds=0x61CB1C status=00 pak_size=0
06 bd_ptr=0x4878 pak=0x10EFD4 ds=0x61C460 status=00 pak_size=0
07 bd_ptr=0x488C pak=0x10EDD0 ds=0x61BDA4 status=00 pak_size=0
08 bd_ptr=0x48A0 pak=0x10EBCC ds=0x61B6E8 status=00 pak_size=0
09 bd_ptr=0x48B4 pak=0x10E9C8 ds=0x61B02C status=00 pak_size=0
10 bd_ptr=0x48C8 pak=0x10E7C4 ds=0x61A970 status=00 pak_size=0
11 bd_ptr=0x48DC pak=0x10E5C0 ds=0x61A2B4 status=00 pak_size=0
12 bd_ptr=0x48F0 pak=0x10E3BC ds=0x619BF8 status=00 pak_size=0
13 bd_ptr=0x4904 pak=0x10E1B8 ds=0x61953C status=00 pak_size=0
14 bd_ptr=0x4918 pak=0x10DFB4 ds=0x618E80 status=00 pak_size=0
15 bd_ptr=0x492C pak=0x10DDB0 ds=0x6187C4 status=00 pak_size=0
16 bd_ptr=0x4940 pak=0x10DBAC ds=0x618108 status=00 pak_size=0
cpb = 0x61, eda = 0x5000, cda = 0x5000
TX ring with 1 entries at 0x615000
00 bd_ptr=0x5000 pak=0x000000 ds=0x000000 status=80 pak_size=0
01 bd_ptr=0x5014 pak=0x000000 ds=0x000000 status=80 pak_size=0
0 missed datagrams, 0 overruns
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
0 residual bit errors
```

D. Comandos de monitoreo de enrutamiento

show ip protocol

Este comando permite revisar la información correspondiente a configuración de los protocolos de enrutamiento IP activos en el router

También permite revisar los timers utilizados por cada protocolo.

```
Router#show ip protocol
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
```

```
Redistributing: rip
Default version control: send version 1, receive any version
  Interface        Send  Recv   Key-chain
  Ethernet0        1     1 2
  Serial1          1     1 2
Routing for Networks:
  172.16.0.0
Routing Information Sources:
  Gateway         Distance      Last Update
  172.16.20.2          120      00:00:21
Distance: (default is 120)
```

Anotaciones:

Routing Protocol is "rip"

- ✓ La información que sigue corresponde a la configuración del protocolo RIP.

Sending updates every 30 seconds, **next due in** 12 seconds

- ✓ Período de actualización: 30 segundos.
- ✓ Próxima actualización a enviar en....

Invalid after 180 seconds, **hold down** 180, **flushed after** 240

- ✓ Período de invalidación de ruta: 180 segundos
- ✓ Período de espera: 180 segundos.
- ✓ Período de renovación de rutas: 240 segundos.

```
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Redistributing: rip
Default version control: send version 1, receive any version
  Interface        Send  Recv   Key-chain
  Ethernet0        1     1 2
  Serial1          1     1 2
```

- ✓ Tabla de control de versiones de RIP. Permite visualizar que versión (1 ó 2) está habilitada para recibir y enviar cada interface

Routing for Networks:
172.16.0.0

- ✓ Red a partir de la cual está "aprendiendo" rutas. Son las redes declaradas con el comando "network".

Routing Information Sources:

```
  Gateway         Distance      Last Update
  172.16.20.2          120      00:00:21
  172.16.40.1          120      00:00:23
```

- ✓ Información sobre el router vecino del cual está aprendiendo rutas.
- ✓ Especifica la distancia administrativa y el tiempo transcurrido desde la última actualización recibida desde ese router vecino.

Distance: (default is 120)

- ✓ Distancia administrativa declarada para este protocolo.

show ip route

Este comando permite visualizar las rutas elegidas en el router y toda la información pertinente.

Tenga en cuenta que puede haber diversos protocolos activos en el dispositivo (los puede revisar utilizando el comando show ip protocolos), pero en la tabla de enrutamiento sólo se mostrará la mejor ruta, es decir, la de menor distancia administrativa.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
default
       U - per-user static route, o - ODR

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 5 subnets
R        172.16.40.0 [120/1] via 172.16.20.2. 00:00:18. Serial1
C        172.16.30.0 is directly connected. Ethernet0
C        172.16.20.0 is directly connected. Serial1
R        172.16.10.0 [120/1] via 172.16.10.1. 00:00:18. Serial0
R        172.16.1.0 [120/1] via 172.16.10.1. 00:00:18. Serial0
```

Debug ip rip

Envía las acutalizaciones de enrutamiento recibidas y enviadas a la sesión de consola del router.

```
Router#debug ip rip
RIP protocol debugging is on
Router#
00:12:07: RIP: sending v1 update to 255.255.255.255 via Serial0
(172.16.10.2) -
suppressing null update
00:16:51:      subnet  172.16.10.0, metric 2
00:16:35: RIP: received v1 update from 172.16.10.1 on Serial0
00:16:35:      172.16.10.0 in 1 hops
00:12:07: RIP: sending v1 update to 255.255.255.255 via Serial1
(172.16.20.1) -
suppressing null update
00:16:51:      subnet  172.16.20.0, metric 2
00:16:35: RIP: received v1 update from 172.16.20.2 on Serial1
00:16:35:      172.16.20.0 in 1 hops
00:12:07: RIP: sending v1 update to 255.255.255.255 via Ethernet0
(172.16.30.1) -
suppressing null update
```

E. Comandos de monitoreo de listas de acceso IP

```
Router#show ip access-list
Standard IP access list 10
   deny host 172.16.40.3
   permit any
```

```
Router#show ip interface
Ethernet0 is up, line protocol is up
  Internet address is 172.16.30.1
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  Web Cache Redirect is disabled
  BGP Policy Mapping is disabled
Serial0 is up, line protocol is up
  Internet address is 172.16.10.2
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 10
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
```

```
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  Web Cache Redirect is disabled
  BGP Policy Mapping is disabled
```

```
Router#show running-config
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
!
ip subnet-zero
Standard IP access list 10
   deny host 172.16.40.3
   permit any
!
interface Ethernet0
 ip address 172.16.30.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 ip address 172.16.10.2 255.255.255.0
 no ip directed-broadcast
 clock rate 64000
 no ip mroute-cache
 ip access-group 10 in
!
interface Serial1
 ip address 172.16.20.1 255.255.255.0
 no ip directed-broadcast
 clock rate 64000
 no ip mroute-cache
access list 10 deny host 172.16.40.3
access list 10 permit any
!
!
router rip
network 172.16.0.0
!
!
no ip classless
!
!
!
line con 0
line aux 0
line vty 0 4
!
end
```