



Ing. Marco Leonel Ari Zurita

# CCNA ROUTING & SWITCHING APUNTES

Versión 01



**Ingeniero Electrónico Marco Leonel Ari Zurtita**

**Celular:** +591 72570395

**RNI:** 35095

**Correo:** [marco.leonel.ari@gmail.com](mailto:marco.leonel.ari@gmail.com)

[leonel\\_marco@hotmail.com](mailto:leonel_marco@hotmail.com)

Facebook: <http://facebook.com/LeonelMarcoAri>

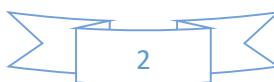
<https://www.facebook.com/LeoTICisco>

Youtube: [https://www.youtube.com/channel/UCuGgVoTkcckFcu\\_0GGhjmCw](https://www.youtube.com/channel/UCuGgVoTkcckFcu_0GGhjmCw)

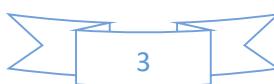


## Contenido

CCNA – SWITCHING AND ROUTING .....	7
1.1. Conceptos básicos de la comunicación de red .....	7
1.1.1. Red.....	7
1.1.2. Componentes de una red.....	7
1.1.3. Protocolo .....	7
1.2. Modos de transmisión.....	7
1.2. Tipos de dispositivos .....	7
1.2.1. El Hub .....	8
1.2.2. Switch.....	8
1.2.3. Modos de envío de un switch .....	8
1.2.4. Firewall de nueva generación NGF.....	9
1.2.5. Access point.....	9
1.3. Composición de la red.....	11
1.4. Tipo de direccionamiento MAC (Media Access Control).- .....	12
1.4.1. Redes SOHO small office home office.....	12
1.4.2. Servicios en Sitio o en la nube.....	12
1.5. Interfaces de router .....	12
1.5.1. Interface Ethernet .....	12
1.6. Estructura Ethernet (Trama Ethernet) .....	13
1.7. Dirección MAC (Media Access Control).....	14
1.8 Tipos de redes .....	14
1.9. Comparación entre los protocolos de WAN y LAN.- .....	14
1.10 Capas del modelo TCP/IP y el modelo OSI .....	15
1.10.1 Protocolo de internet .....	15
1.10.2 Proceso de encapsulación.....	17
1.10.3 Comparación entre el modelo TCP/IP con el modelo OSI.- .....	18
1.10.4. Capa 4 de trasporte.....	19
1.11. Sesión de confianza (3 way handshake).....	20
1.11.1 Servidor .....	21
1.12 Protocolos .....	21
1.12.1 DNS (Sistema de nombres de dominio) .....	21
1.12.2 HTTP .....	22
1.12.3 HTTPS .....	22
1.13 Cable UTP .....	22



1.14 Fibra óptica.....	23
1.14.1. Técnicas de multiplexacion en sistemas ópticos.....	24
1.15 Funcionalidades de enrutamiento .....	24
1.15.1 Operaciones de enrutamiento .....	24
1.15.2 Tabla de enrutamiento.....	24
1.16. Ruta dinámica.....	26
1.16.1. Distancia vector.....	27
1.16.2. Estado de enlace (link-state routing protocol).....	28
1.17. Classless CIDR (Classless Inter-Domain Routing) y classfull.-.....	29
1.17.1. VLSM (Variable Length Subnet Mask) .....	30
1.18. ARP (Address Resolution Protocol) .....	32
1.19 Puerta de enlace (Gateway).....	32
1.20. Seguridad.....	32
1.20.2 ACL (Access Control List) listas de acceso .....	33
1.20.3. Listas de acceso estándar .....	34
1.20.4. Listas de acceso extendidas .....	35
1.20.5. Radius y tacacs .....	36
1.21. Servicios IP.....	37
1.22. DHCP (Dynamic Host Configuration Protocol) .....	37
1.22.1. DHCP con Relay agent (agente de trasmisión).....	38
1.23. NAT (Network Address Translation).....	39
1.23.1. NAT estática .....	39
1.23.2. NAT dinámica .....	40
1.23.3. PAT (Port Address Translation) .....	41
1.24. Calidad de servicio QoS .....	43
1.24.1. MQC Modular QoS Command Line Interface.....	44
2.1. Diseño de una red LAN.....	45
2.1.1. Topología Spine and Leaf .....	45
2.2. VLAN (virtual área network).....	46
2.2.1. Creación de VLAN .....	46
2.2.2. Trunk (Troncal) .....	47
2.2.3. Vlan nativa.....	48
2.3. Redundancia física en una LAN .....	49
2.4. Enrutamiento entre VLAN .....	50
2.4.1. Por cada VLAN del switch una interface en el router .....	50



2.4.2. Router on stick .....	50
2.4.3. SVI (Switch Vlan interface) .....	51
2.5. IOS CISCO.....	52
2.5.1. Parámetros de seguridad que nos ofrece cisco .....	52
2.5.2. Protocolo NTP (Network Time Protocol).....	58
2.5.3. Mensajes de interrupción (syslog) .....	58
2.6. La administración de dispositivo cisco .....	58
2.6.1. Configuración de registro.....	60
2.6.2. Servidor TFTP (Trivial file transfer Protocol) .....	60
2.6.3. Nomenclatura de una imagen IOS. ....	60
2.6.4. Password recovery (recuperar contraseña) .....	61
2.9. Licencia.....	63
3.1. Introducción a IPv6.....	64
3.1.1. Soluciones planteadas por IPv4.....	65
3.1.2. Problemas con IPv4.....	65
3.1.3. Beneficios de IPv6 .....	65
3.1.4. Tipos de direccionamiento en IP v6 .....	65
3.2. Cabecera de IPv6 y IPv4 .....	68
3.3. ICMP v6 (internet control message protocol versión 6) .....	69
3.4. Direcciones Multicast de nodo solicitado .....	69
3.5. Multicast mapeo sobre Ethernet .....	70
3.6. Ejemplo de red en ipv6.....	70
<b>4.1. Vlan DE VOZ .....</b>	<b>71</b>
4.2. Troncal.....	71
4.2.1. Protocolo dinámico troncal (DTP) .....	72
4.2.2. VTP (Vlan trunking protocol) .....	73
4.3. Redundancia física en una LAN .....	74
4.3.1. Spanning Tree Protocol STP IEEE 802.1d.....	74
4.3.2. Designar el Root Bridge .....	76
4.3.3. Estados de STP.....	77
4.3.4. Tipos de Spaning Tree Protocol (STP) .....	77
4.3.5. PortFast y la protección BPDU (Bridge Protocol Data Units) .....	79
4.3.6. Redundancia en switch con Etherchannel .....	80
4.4. Redundancia a nivel de capa 3 FHRP (First Hop Redundancy Protocol) .....	82
4.4.1. HSRP (Hot Standby Router Protocol) .....	82

4.4.2. VRRP (Virtual Router Redundancy Protocol) .....	84
4.4.3. GLBP (Gateway Load Balancing Protocol).....	84
5.1. Protocolo de enrutamiento dinámico (distancia vector avanzado o híbrido) EIGRP.....	85
5.1.1. Balanceo de carga en EIGRP.....	88
5.1.2. Autenticación en EIGRP .....	89
5.1.3. Puerto pasivo en EIGRP .....	90
5.1.4. EIGRP en IPv6 .....	91
6.1. Protocolo de Enrutamiento OSPF (open short phat firts).....	91
6.1.1. Areas OSPF .....	91
6.1.2. Paquete Hello .....	92
6.1.3. Métrica de OSPF .....	92
6.1.4. Configuración de OSPF .....	93
6.1.5. El router id.....	93
6.1.6. Estados de ospf.-.....	93
6.1.7. Tipos de paquetes de OSPF.-.....	94
6.1.8. Creación de adyacencia.....	94
6.1.9. LSA link state advertise .....	94
6.1.9. Balanceo de carga .....	94
6.1.11. OSPF sumarizado.....	96
6.1.12. Configuración áreas.....	97
7.1. Configuración de una red Wireless .....	98
7.1.1. Arquitectura Split-MAC centralizada.....	98
7.1.2. Arquitectura autónoma.....	104
8.1. REDES WAN .....	106
8.2. Dispositivos WAN .....	107
7.3. VPN administrado por el proveedor MPLS .....	107
8.4. WAN privada .....	108
8.4.1. PPP punto a punto.....	108
8.4.2. Establecer la sesión en PPP.-.....	108
8.4.3. Comparación HDLC y PPP .....	110
8.5. Redes VPN (Virtual Private Network).-.....	111
8.5.1. VPN Sitio a Sitio .....	111
8.5.2. VPN acceso remoto .....	111
8.5.3. Sitio a Sitio IPsec.....	112
8.5.4. Sitio a Sitio Túnel GRE .....	114

9.1. Administración de Routers y switch.....	115
9.1.1. CDP (Cisco Discovery Protocol) .....	115
9.1.2. SNMP (Simple network managment protocol) .....	115
8.1.3. Protocolo de capa 7 Syslog.....	116
9.1.4. NETFLOW.....	117
8.1.5. SPAN, RSPAN, ERSPAN (Switch) .....	117
9.1.6. Stackwise .....	118
10.1. BGP (Boreder Gatwey Protocol).-	119
10.1.1. Tablas de BGP.-.....	119
11.1 Software defined network SDN.....	121
11.1.1. Overlay y Underlay y Fabric.....	121

## CCNA – SWITCHING AND ROUTING

### 1.1. Conceptos básicos de la comunicación de red

La estructura de una red se basa en tres cosas:

- Fuente de mensaje
- Canal
- Destino

#### 1.1.1. Red

Es la unión entre dispositivos a través de un medio que es capaz de llevar información.

- **Segmentación.**- capa de transporte, es el proceso en el cual el **mensaje se divide en bloques**.
- **Multiplexación.**- capa de transporte, se trata de **intercalar mensajes a través de un medio** (fibra óptica, cobre, medio inalámbrico) que tienen distintos orígenes. Lo que permite que múltiples usuarios se puedan interconectar.
- **Demultiplexación.**- capa de transporte, una vez que el mensaje llega a su destino, **los datos se ordenan**.
- **Re ensamblaje.**- capa de transporte, los **mensajes ordenados se reconstruyen**.

#### 1.1.2. Componentes de una red

Se dividen en componentes de hardware (pc, routers, switch) y software (protocolos que permiten la interconectividad de los elementos, HTTP, POP, DNS).

#### 1.1.3. Protocolo

Es un conjunto de reglas que gobiernan la comunicación en red, los protocolos son independiente de la tecnología.

- Proporcionan el formato del mensaje.
- El protocolo es el proceso en el cual los dispositivos comparten información de las rutas hacia otras redes.
- Determinan como y cuando existen errores de sistemas, inicio y termino de transferencia de datos.

### 1.2. Modos de transmisión

- **Simplex:** Llamada también unidireccional es aquella que ocurre en una sola dirección. **El receptor no puede responder al transmisor.** Se lo utiliza en la radiodifusión (Broadcast) de TV y radio.
- **Half dúplex.**- Permite transmitir en ambas direcciones. Sin embargo, **la transmisión puede ocurrir solamente en una dirección a la vez.** Tanto transmisor y receptor comparten una sola frecuencia. Un ejemplo es el radio de banda civil donde el operador puede transmitir o recibir, no pero puede realizar ambas funciones simultáneamente por el mismo canal. Cuando el operador ha completado la transmisión, la otra parte debe ser avisada para que puede empezar a transmitir.
- **Full dúplex.**- **transmisor y el receptor se comunican simultáneamente** utilizando el mismo canal, pero usando dos frecuencias.

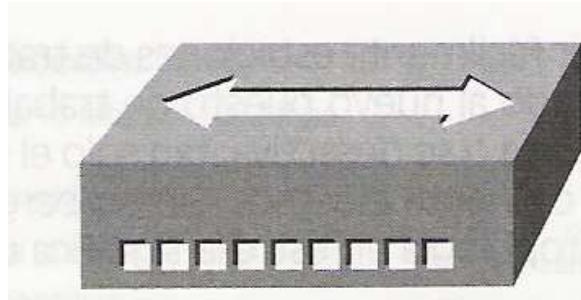
### 1.2. Tipos de dispositivos

- **Dispositivos finales.**- Le dan acceso directo al usuario a la red (pc, teléfono inteligente, impresora, servidor, cámara IP etc.)

- **Dispositivos intermedios.**- Proveen conectividad y se aseguran que los flujos de datos corren a través de la red. Tienen la responsabilidad de decidir el camino por donde se envía los datos (Switch, Routes, Fireware, Access point).

### 1.2.1. El Hub

Es un dispositivo intermedio que trabaja en capa 1, extiende el segmento LAN, la topología de su bus es **Half dúplex** (transmite y recibe pero no simultáneamente) (10 base-T, 10Mbps banda base UTP) lo que implica un canal único, donde pueden producirse colisiones de datos (**Genera colisiones de red**), su función principal es de distribuir y extender nuestro segmento de red, **el ancho de banda es repartido entre los host**. Es menos seguro que un switch debido a que genera duplicidad de datos.



### 1.2.2. Switch

Trabaja en capa 2 y permite transmisión **full dúplex** (envía y recibe simultáneamente) dentro de un dominio de Broadcast (solo una red), tiene **dominio de colisión por puerto** (a diferencia del Hub, que solo tiene un dominio de colisión para todos sus puertos) y solo maneja un dominio de Broadcast (solo maneja una red). Al trabajar en full dúplex no necesita CSMA/CD (CSMA/CD permite la detección de colisiones en Half duplex). **El switch envía, filtra e inunda de tramas basados en la dirección Mac** (Anota el puerto y luego la Mac).

Cuando la trama llega al switch, este compara en base a la dirección Mac el destino. Si se determina el destino está en su lista, la trama se envía dentro de la misma red al host sin enviar a los demás “filtra” (*Unicast*), si el switch no encuentra el destino en su lista inunda (envía a todos menos así mismo). Cada vez que se anota una nueva dirección Mac el switch inunda (Broadcast). Una dirección Mac se almacenada por defecto 300 segundos (5min). Ofrece ancho de banda dedicado por puerto (no divide como el HUB). Además este dispositivo ofrecen ancho de banda dedicado (no reparte el ancho de banda).

Nota.- El Switch tiene tecnología ASIC (chip CMOS) que le permite enviar de datos internos rápidos.

**El HUB genera colisiones de red**  
**El switch genera dominios de colisión**  
**El router genera dominios de Broadcast**

### 1.2.3. Modos de envío de un switch

- **Cut and through** (corte): **solo ve el destino, envía la trama antes de recibirla en su totalidad verifica la dirección de destino.** Su uso es mejor en la capa core pues es primordial la velocidad y no existe tanto error. Duplica los primeros 6 bytes antes de tomar la decisión
- **Store and forward** (Almacena y envía): **Revisa toda la trama, el switch almacena la trama completa en los bufer verifica si el código de redundancia cíclica CRC es correcto, busca la**

dirección de destino la cual determina la interfaz de salida y envía la trama. Se usa más en la capa de acceso donde se encuentra la mayoría de problemas de red y los usuarios.

- **Fragment-free** (libre de fragmentos): **hibrido** almacena los primeros 64 bytes de la trama antes de realizar el envío puesto que es ahí donde ocurren los errores y colisiones.

Se tiene los siguientes dispositivos

- Catalyst 2960: 24/48 puertos, usados en acceso, puertos Gigaethernet, usb, consola, slots para SFP
- Catalyst 3560: Capa 3
- Catalyst 3750: 24/48 puertos, permite stack que es el apilamiento, para redundancia.
- Catalyst 4500/6500: 11 tarjetas de 48/96 puertos.

#### 1.2.4. Firewall de nueva generación NGF

Monitorea el tráfico, filtra el tráfico, todo el tráfico que se protege debe pasar a través de él. Decide que permitir o bloquear utilizando reglas. Existen dos tipos ASA y Fire Power.

**IPS (intrusión Prevention system):** examina el tráfico para determinar patrones de ataque según una base de firmas de ataques conocidos puede ser un dispositivo separado o dentro del Firewall. Usa Deep Packet Inspection.

Tipos de firewall:

- Packet Filter Firewall: basado en la inspección IP, puerto o protocolo, header. **Usa ACLs**, es State Less, opera en capa 3 y 4.
- Stateful Firewall: los más comunes, revisa conexiones (SPI State Packet Inspection), analiza basado en la tabla de estados, maneja zonas de seguridad y trabaja hasta nivel de capa 7.
- Next Generation Firewall: es stateful, tiene visibilidad y control de aplicaciones, IPS, AMP(Advanced Malware Protection), posee filtro url, VPN (Virtual Private Network).

#### 1.2.5. Access point

Dispositivo que interconecta host de forma inalámbrica, Wireless LAN WLAN. Basado el protocolo 802.11 (g 54Mbps, n 600Mbps, ac 1.3Gbps). Opera en dos bandas 2.4Ghz y 5Ghz (bandas libres). Usa el SSID (Service Set Identifier) es el indicador de paquetes de servicio, donde nos conectamos para usar wifi.

Estandar	Frecuencia	Velocidad Maxima	Compatibilidad	Estado actual
802.11b	2.4 GHz	11 Mbps	802.11g	Obsoleto
802.11a	5 GHz	54 Mbps	802.11n (5 GHz )	Obsoleto
802.11g	2.4GHz	54 Mbps	802.11b (11 Mbps)	Actual
802.11n	2.4 GHz o 5 GHz	300 Mbps	802.11g (a 54 Mbps) 802.11b (a 11 Mbps) 802.11n (a 54 Mbps a 5 GHz)	Actual

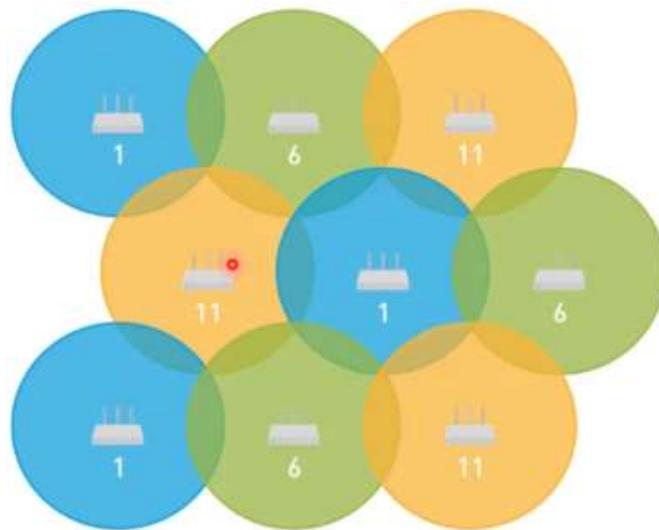


Existen de dos tipos por su administracion:

- Autonomos: administrado individualmente
- Lightweight: administración centralizada mediante WLC (wireless LAN Controller), usado para redes empresariales.

#### *1.2.5.1. Frecuencias 2.4 Ghz*

Se divide en 14 frecuencia 11 utilizables, para evitar que se overlapping (no se solapan) se recomienda el uso de 1, 6, 11.



#### *1.2.5.2. Frecuencias 5 Ghz*

Se tiene 24 canales non overlapping

##### **5 GHz (802.11a/n/ac)**



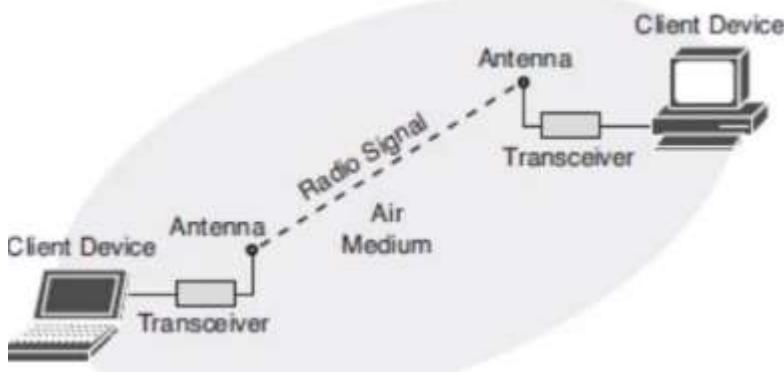
#### *1.2.5.3. SSID Service Set Identifier*

Identifica la red inalámbrica, consta de 32 caracteres ASCII



#### 1.2.5.4. Radio frecuencia

El sistema se compone de un cliente dispositivo, transmisor, medio (aire).



La señal de radio son las ondas a ser transmitidas que viajan a través del aire, dependerán de la Amplitud, Frecuencia, longitud y fase. Estas ondas se convierten a 1 y 0 siendo encapsulados.

#### 1.2.5.5. Tipos de encriptación

Cifrado	Nivel
Abiertas	Riesgoso. Sin contraseña
WEP	Riesgoso. viejo estándar de encriptación WEP.
WPA-PSK (TKIP)	Riesgo Medio. Estándar de cifrado WPA o WPA1. clave precompartida (PSK)
WPA-PSK (AES)	Riesgo Medio. Protocolo de cifrado inalámbrico WPA con el cifrado Advanced Encryption Standard (AES)
WPA2-PSK (TKIP)	Riesgo Medio. Estándar WPA2 con cifrado TKIP
WPA2-PSK (AES)	Seguro. Advanced Encryption Standard (AES)
WPAWPA2-PSK (TKIP / AES)	Permite WPA y WPA2 con TKIP y AES.

Solo se usan abiertas (ciertas implementaciones) y WPA2-PSK AES. El WPAWPA2 se usa como compatibilidad con dispositivos como impresoras o algunos teléfonos inalámbricos.

### 1.3. Composición de la red

A nivel físico los medios pueden ser, cobre (coaxial, UTP), F.O (no tiene límite). Medios inalámbricos wifi, 3g, 4g, bluetooth. Interconexiones (tarjeta de red). El cobre tiene límite físico de transmisión de ancho de

banda el cual puede ser 100Mbps, 1Gbps, 10Gbps **el cable UTP se puede emplear hasta una distancia de 100 m.** Fibra óptica, no tiene problemas de inducción eléctrica, no tiene límites de transmisión de ancho de banda (el ancho de banda depende de los dispositivos).

#### 1.4. Tipo de direccionamiento MAC (Media Access Control).-

- Broadcast: de uno a todos, un host envía un paquete a todos los host de esa red
- Multicast: de uno a un grupo, origen 10.1.1.1 destino 224.0.0.0
- Unicast: uno a uno, comunicación de una dirección de origen a una de destino.

#### 1.4.1. Redes SOHO small office home office

Redes pequeñas cableadas o inalámbricas de 1 a 10 usuarios, que necesitan conectarse a un sitio central generalmente usando internet mediante una VPN

#### 1.4.2. Servicios en Sitio o en la nube

- En sitio: todos nuestros servidores correo, web, base de datos estarán dentro de mi red, en mi centro de datos
- En la nube: varios servicios o servidores estarán en la nube, es público porque cualquier empresa puede adquirir sus servicios, Amazon Web Services, Google Cloud, Microsoft Azure
  - Pública: Amazon, google cloud, Microsoft Azure.
  - Privada: hosting (tener servidores dentro de un RACK privado), Colocation (comprar servidores físicos a Amazon)

### 1.5. Interfaces de router

Se refiere a la comunicación con una LAN. El router tiene puertos de administración como consola, usb, auxiliar y administración (única que soporta TCP/IP). El puerto de administración “management” se le coloca una IP solo para administración remota que puede estar en otra red y de esta manera aumentar la seguridad, a diferencia de lo que se hace comúnmente que es asignarle una IP que pertenece a la red, en la vlan 1 mediante el puerto consola e ingresar por telnet o SSH.

```
Conf #Interface management 0/0
Conf-if #ip address 192.168.1.254 255.255.255.0
Conf-if # no shutdown
```

#### 1.5.1. Interface Ethernet

Nace con Ethernet 10Mbps posteriormente Fastethernet 100Mbps y Gigaethernet 1Gbps (nomenclatura: interface Fastethernet slot / número de interfaz).

- **Interface Serial:** Generalmente van conectados a redes WAN, asincrónicas o sincrónicas (Interface serial modulo /slot / número de interface).
- **Interfaces Loopback:** Es una interface lógica o virtual, utilizada para verificación de conectividad.

Por defecto las interfaces en el router a diferencia del switch están caídas (Shutdown) se deben levantar a través de comando.

Levantar la interfaz

```
router (conf-if) # no shutdown
```

En caso de querer hacer caer las interface se utiliza el comando.

**router (conf-if) # shutdown**

Para ver el resumen de las interfaces se utiliza el comando

**router # show ip interface brief**

Detalles específicos del puerto

**router # show protocols fastethernet 0/0**

Detalles del protocolo de enrutamiento que se está utilizando (solo capa 3)

**router # show ip protocols**

## 1.6. Estructura Ethernet (Trama Ethernet)

Los campos principales de la trama de Ethernet son los siguientes:

IEEE 802.3						
7 Preámbulo	1 Delimitador de inicio de trama	6 Dirección de destino	6 Dirección de origen	2 Longitud	46 a 1500 y datos de 802.2	4 Secuencia de verificación de trama

Nota: 802.3 primer protocolo de redes basadas en Ethernet.

- Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD) 1 byte en total **8 bytes**: **se utilizan para la sincronización entre los dispositivos emisores y receptores**. Estos ocho primeros bytes de la trama se utilizan para captar la atención de los nodos receptores. Básicamente, los primeros bytes le indican al receptor que se prepare para recibir una trama nueva.
- Campo Dirección MAC de destino: este campo de **6 bytes es el identificador del destinatario** previsto. La Capa 2 utiliza esta dirección para ayudar a los dispositivos a **determinar si la trama viene dirigida a ellos**. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.
- Campo Dirección MAC de origen: este campo **de 6 bytes identifica la NIC** (tarjeta de red) o la interfaz que origina la trama.
- Campo Longitud/tipo: **Define la longitud exacta del campo de datos de la trama**, propósito del campo es describir qué protocolo de capa superior está presente.
- Campo Datos: este campo (**de 46 a 1500 bytes**) **contiene los datos encapsulados** de una capa superior, que es una PDU de capa 3 genérica o, más comúnmente, un paquete IPv4.
- Campo Secuencia de verificación de trama (FCS): este campo de **4 bytes se utiliza para detectar errores en una trama**. Utiliza una comprobación de redundancia cíclica (CRC).

Nota: MUT (Unidad de transmisión máxima) 46 a 1500 Byte Datos. La trama Ethernet solo detecta errores no los corrige (capa 2).

### 1.7. Dirección MAC (Media Access Control)

Es un identificador de 48 bits (6 bloques hexadecimales (12 dígitos hexadecimales)) que corresponde de forma única a una tarjeta o dispositivo de red. La MAC se almacena por 300 segundos en la CAM (Content Address Memory). La tabla se llena identificando la MAC de origen de la trama e identificando el puerto por el cual llegó de tal manera que la MAC de destino se compare con las MAC almacenadas. Si la MAC de destino no está en la tabla entonces se manda a todos los puertos para que uno responda.

- Se conoce también como dirección física, y es única para cada dispositivo.
- Se separa en dos partes, la primera de 24 bits (IEEE) y la segunda de 24 bits (fabricante).

Ver la tabla de direcciones MAC

**# show mac address-table"**

Para limpiar la tabla de direcciones Mac

**# clear mac address-table dynamic**

Muestra el Puerto al cual está conectado el host

**#show mac address-table address 6ca8.4987.295f**

Muestra las direcciones mac asociadas a una ip (recomendado capa 3)

**#show ip arp**

Nos ayuda a ver una descripción de los puertos.

**#show interface status**

### 1.8 Tipos de redes

- LAN (*Local Area Network*): Abarcan un área reducida (hogar, universidad, edificio), pero soportan anchos de banda bastante grandes Ethernet 10Mbps, FastEthernet 100Mbps GigaEthernet 1Gbps.
- MAN(*Metropolitan Area Network*) es una red de alta velocidad (**banda ancha**) que da cobertura en un área geográfica extensa, proporcionando capacidad de integración de múltiples servicios mediante la transmisión de datos
- WAN(*Redes de área amplia, Wide area network*).- Interconectan LANs remotas, por medio de la interconexión de rúters (Internet)

Nota.- Se denomina nube, al ISP (proveedor de servicio de internet, Internet Service Provider).

### 1.9. Comparación entre los protocolos de WAN y LAN.-

**WAN**

PPP (Protocolo punto a punto)

**LAN**

Ethernet

### Frame Relay

HDLC (High-Level Data Link Control) Capa 2, proporciona recuperación de errores en caso de pérdida de paquetes de datos, fallos de secuencia y otros, por lo que ofrece una comunicación confiable entre el transmisor y el receptor.

### Metro Ethernet

MPLS (Multiprotocol Label Switching) capa 2 y 3, unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP

CSMA/CD capa 2, evita y detecta colisiones de datos

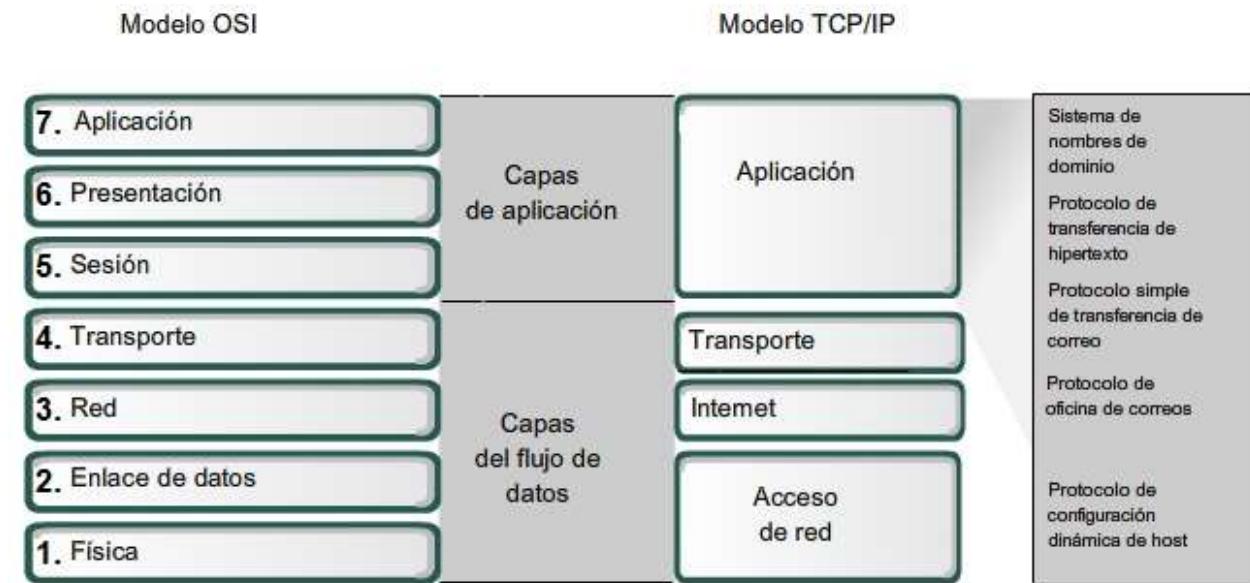
STP (Spanning Tree Protocol) capa 2 El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles. STP es transparente a las estaciones de usuario

VTP (VLAN Trunk Protocol) reduce la administración en una red de switch. Al configurar una VLAN nueva en un servidor VTP, se distribuye la VLAN a través de todos los switches del dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes

802.1Q permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas Trunking

## 1.10 Capas del modelo TCP/IP y el modelo OSI

La ventaja de usar un modelo en capas es que el cambio en una de ellas no afecta a los demás, son independientes, permite interconexión entre distintos fabricantes.



### 1.10.1 Protocolo de internet

Nos permite llevar información de un sitio a otro, es **protocolo no orientado a conexión** (no hace verificación, solo le interesa entregar el paquete), opera en la capa de internet o en la capa 3 Red del modelo OSI, independiente de amenazas, protocolo rápido (sección de confianza rápida), se divide en 2 partes red y host, **no tiene recuperación de datos**, dos versiones de 32 bits IPv4 y 128 bits IPv6.

### *1.10.1.1 Direcciones IPv4*

Se divide en dos porciones porción de red y porción de host, es de 32 bits o 4 octetos, la dirección de red y Broadcast (solo son referenciales). Network id, identifica a que red pertenece el host (asignado por router). Host id, identificador único del host.

Cabecera de ipv4, tipo de servicio (define la prioridad de cada paquete), tiempo de vida que le toma al paquete llegar a su destino disminuye su valor dependiendo del número de saltos (TTL 255), protocolo identifica la conectividad en capa 4 (UDP puerto17 /TCP puerto 6).

**Formato de la Cabecera IP (Versión 4)**

0-3	4-7	8-15	16-18	19-31				
Versión	Tamaño Cabecera	Tipo de Servicio		Longitud Total				
Identificador		Flags		Posición de Fragmento				
Time To Live	Protocolo		Suma de Control de Cabecera					
Dirección IP de Origen								
Dirección IP de Destino								
Opciones			Relleno					

Nota.- la cabecera IP pesa 20 Bytes.

Las direcciones IPv4 se han separado en 5 clases:

- Clase A.- 1 a 126
- Clase B.- 128 a 191
- Clase C.- 192 a 223
- Clase D (reservado para multicast).- 224 a 239 nos sirve para especificar un grupo
- Clase E (reservado para aplicaciones dinámicas).-240 a 255

### *1.10.1.2. Direcciones privadas*

No están registradas, no son válidas en el espacio de internet, son usadas en espacios locales, LAN.

- Clase A: 10.0.0.0 a 10.255.255.255
- Clase B: 172.16.0.0 a 172.31.255.255
- Clase c: 192.168.0.0 a 192.168.255.255

### *1.10.1.3. Direcciones públicas*

Están registradas en internet, son válidas al alcance público de internet.

- Clase A: 1.0.0.0 a 9.255.255.255 y 11.0.0.0 a 126.255.255.255
- Clase B: 128.0.0.0 a 172.15.255.255 y 172.32.0.0 a 191.255.255.255
- Clase c: 192.0.0.0 a 192.167.255.255 y 192.169.0.0 a 223.255.255.255

Nota: direcciones 127.0.0.0 a 127.255.255.254 son loopback, es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. Nos indica si tcp/ip está instalado correctamente. **APIPA** (Automatic private IP address) 169.254.0.0/16 no es ruteable se asignada cuando no se encuentra el DHCP.

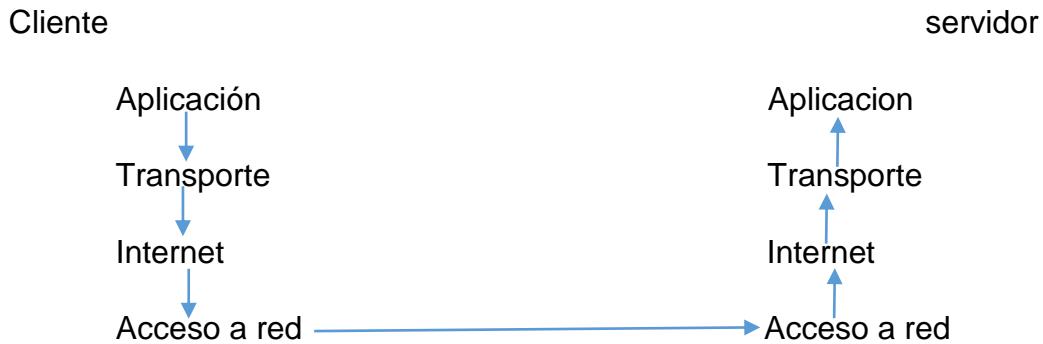
Dirección de red = (IP host) AND (máscara)

Dirección de broadcast = Máscara invertida + Dirección de red

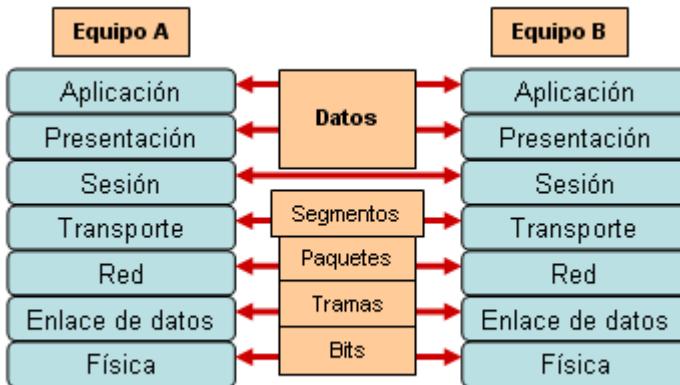
La dirección de red y Broadcast solo son referenciales ejemplo si hacemos en nuestro computador ping a 127.0.0.0 o 127.255.255.255 nos dará error porque son direcciones de red y Broadcast

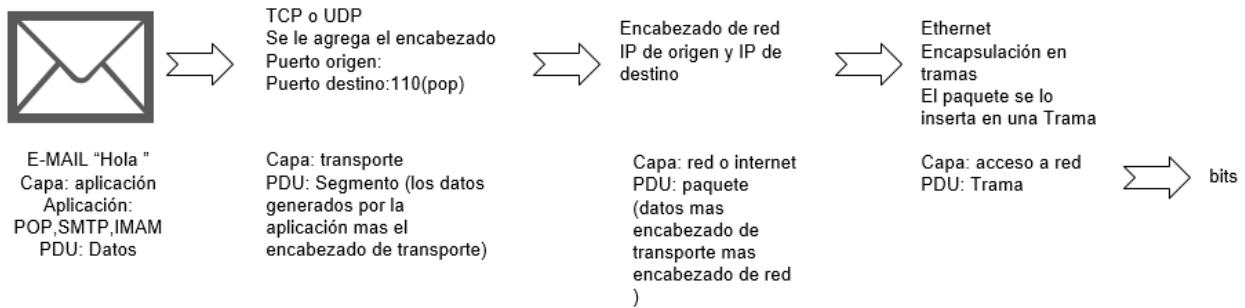
### 1.10.2 Proceso de encapsulación

Cliente genera datos los cuales se encapsulan (se le agrega información de las capas hacia abajo desde la capa de aplicación hasta acceso a red modelo (TCP/IP).

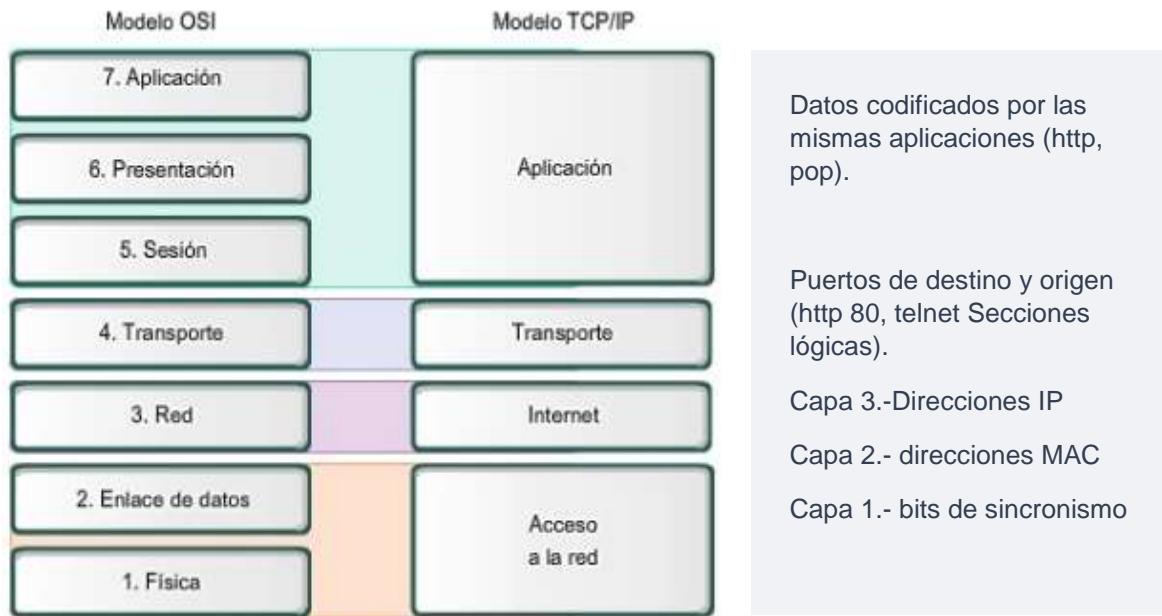


PDU son las unidades de los datos del protocolo, la encapsulación sigue el siguiente proceso.





### 1.10.3 Comparación entre el modelo TCP/IP con el modelo OSI.-



Nota.- cada capa tiene su propia señalización. La comunicación se realiza capa a capa.

- **Capa 7 de aplicación.**- provee los mecanismos para que las aplicaciones accedan a la red.
- **Capa 6 presentación.**- Se encarga de la codificación de datos ambos extremos comparten el mismo lenguaje.
- **Capa 5 Sesión.**- Inicia, mantiene y termina la sesión.
- **Capa 4 de transporte.**- se compone de dos protocolos: UDP y TCP. Encargado de la multiplexación (un puerto de destino varios puertos de origen), identificación de las aplicaciones a través del puerto, maneja segmentación (un dato que pesa por ejemplo 2Gb lo parte en segmentos para mandarlo por el ancho de banda limitado), realiza control de flujo (envía de manera confiable, TCP), es orientado a conexión, confiabilidad TCP (se asegura que todos los segmentos lleguen a destino). A UDP le interesa más la velocidad de entrega
- **Capa 3 de red.**- controla el funcionamiento de la subred, decidiendo qué ruta de acceso física deberían tomar los datos en función de las condiciones de la red, la prioridad de servicio y otros factores. Proporciona enrutamiento, control de tráfico de subred, fragmentación de trama (MTU), asignación de direcciones lógico-físicas.
- **Capa 2 enlace de datos.**- Específica cómo se organizan los datos cuando se transmiten en un medio particular. Esta capa define como son las tramas, las direcciones y las sumas de control de

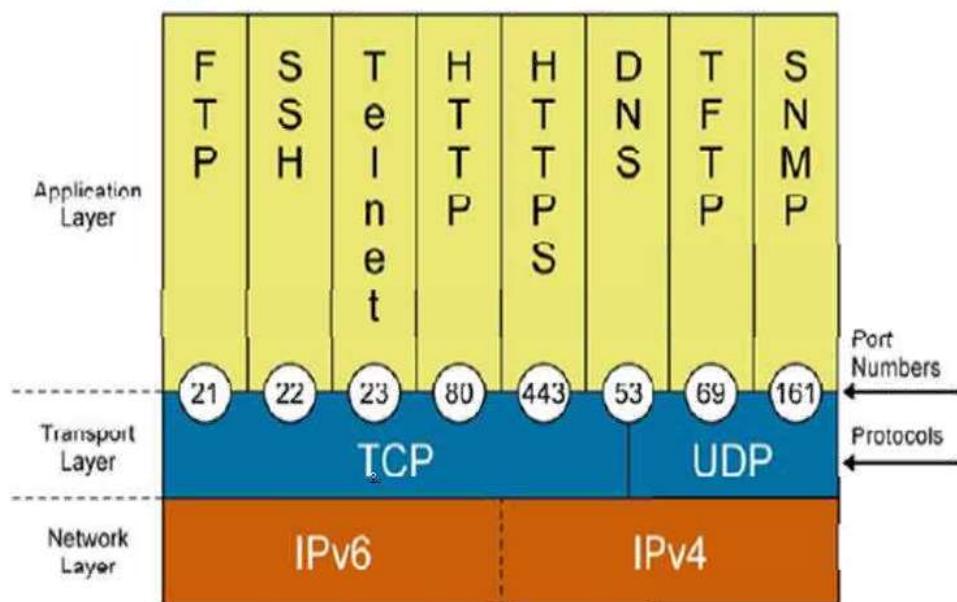
los paquetes Ethernet. Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. Para esto agrupa la información a transmitir en bloques, e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad.

- **Capa 1 física.**- Es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes, de la velocidad de transmisión. Se encarga de transformar un paquete de información binaria en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable), electromagnéticos (transmisión Wireless) o luminosos (transmisión óptica). Cuando actúa en modo recepción el trabajo es inverso, se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

#### 1.10.4. Capa 4 de transporte

##### 1.10.4.1. Puertos

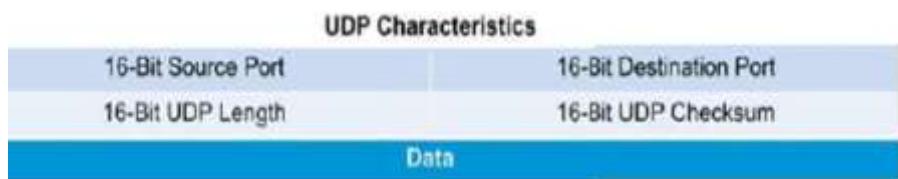
Son de 16 bits, 65535 números de puertos, de 0 a 1023 puerto conocidos, tienen sus aplicaciones definidas. Del 1024 al 49152 registrados por los fabricantes. 49159 a 65535 puertos dinámicos (los usa cualquiera).



- ICMP Puerto 8 UDP/TCP
- SMTP Simple mail transfer Protocol Puerto 25 tcp
- POP3 post office Protocol Puerto 110 tcp
- IMAP internet messages Access Protocol 143 tcp

##### 1.10.4.2. UDP User Datagram Protocol

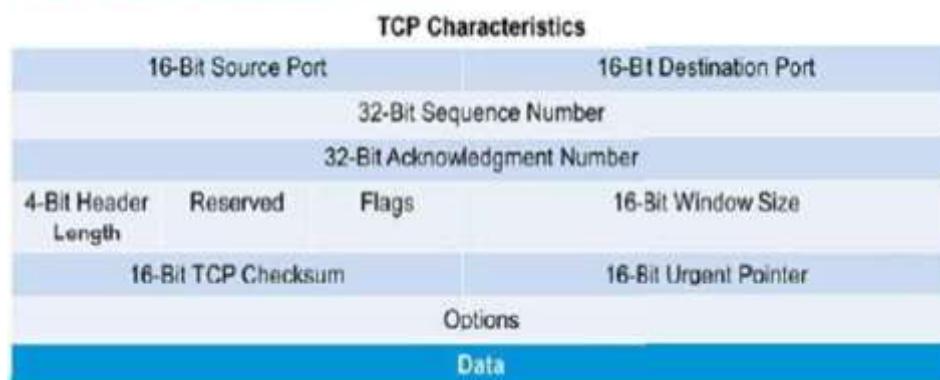
Protocolo rápido, usado en video y voz. No establece sesión de confianza, solo le interesa el destinatario. La segmentación es de tamaño irregular no es secuencial pero es veloz, el MTU (unidad de transmisión máxima es de 1500 byte)



#### 1.10.4.3. TCP Protocolo de control de transmisión

, usado en correo electrónico, descargas, impresiones, compartimiento de archivos. Tiene control de flujo, envía de manera confiable los segmentos, se define el tamaño de carga de envío mínimo 64 byte y máximo 1500 Byte, se contempla el tamaño, almacenamiento temporal BUFFER, y se evita el congestionamiento. TCP está orientado a conexión (establece una sesión entre origen y destino), se asegura que todos los segmentos lleguen a destino.

#### TCP Characteristics (Cont.)



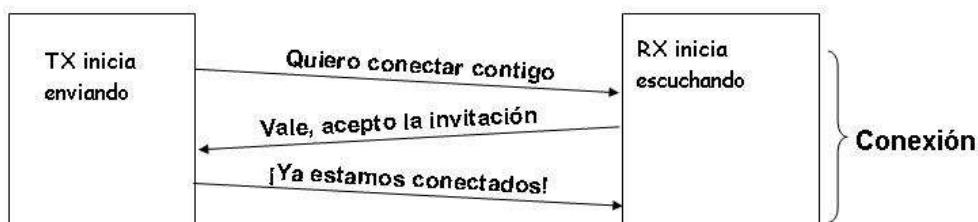
Segmentación es tamaño homogéneo y secuencial, el MTU (unidad de transmisión máxima es de 1500 byte)

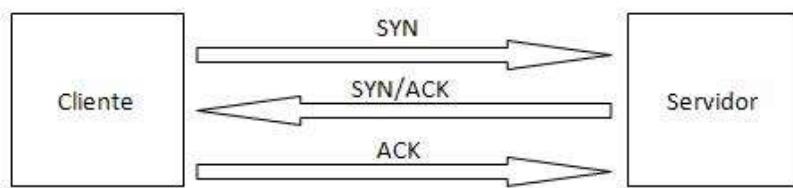
Nota: transmisiones mayores a 1500 hasta 1600 se llaman baby-gigants y superiores a 1600 se llaman transmisiones jumbo

#### 1.11. Sesión de confianza (3 way handshake)

Comunicación de tres vías: petición de conexión, confirmación de conexión y la recepción de la confirmación.

- SYN: es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales ISN
- ACK: acknowledgement, en español acuse de recibo.





### 1.11.1 Servidor

Es una máquina que tiene un servicio ejemplo telnet, DNS, DHCP. Los servidores gestionan múltiples conexiones simultáneas. Cada aplicación abre un puerto Ej. Telnet puerto 23, cuando un cliente quiere conectarse al servidor telnet se encapsula los datos, en la capa de transporte se le agrega un encabezado de transporte (datos, puerto destino: 23, puerto de origen: Random (1025-65535), IP de destino IP de origen) y si un segundo cliente que quiera conectarse con el servidor hace lo mismo pero cambia la IP y el puerto de origen, de esa manera el servidor puede manejar múltiples conexiones.

#### 1.11.1.1 Modelo cliente servidor (c/s)

Una maquina con el rol de servidor y otra con el rol de cliente, (Ej. Servidor http: puerto 80 “abierto” estará en estado de *listening* y es el cliente quien solicita la conexión).

#### 1.11.1.2 Modelo per-to-per (punto punto)

Simultáneamente una PC actúa como cliente-servidor (Ej. Cuando más de un PC ejecutan una aplicación, y una de ellos le solicita a otra datos).

## 1.12 Protocolos

### 1.12.1 DNS (Sistema de nombres de dominio)

Es un protocolo UDP utiliza el puerto 53, convierte un nombre de dominio a una dirección IP, mundialmente existen 13 servidores DNS.

DNS Hostname	IP Address
www.cisco.com	184.168.221.96
www.emc.com	184.86.149.199
www.microsoft.com	65.55.57.27
www.netapp.com	63.97.127.59
www.redhat.com	184.86.151.214
www.vmware.com	184.86.147.51
www.gmail.com	74.125.227.118
www.wikipedia.com	208.60.154.225
www.wunderground.com	38.102.136.104
www.thinkgeek.com	74.205.43.152

Nota: para determinar la dirección de IP de un sitio específico se puede usar el comando **nslookup** posteriormente introducir la dirección Ej. [www.google.com.bo](http://www.google.com.bo)

```
C:\Users\Goku>nslookup
Servidor predeterminado: ns1.acelerate.com
Address: 200.105.128.40

> www.google.com.bo
Servidor: ns1.acelerate.com
Address: 200.105.128.40

Respuesta no autoritativa:
Nombre: www.google.com.bo
Addresses: 2800:3f0:4003:c01::5e
64.233.190.94
```

servidor al que consultamos  
IP del DNS configurado en el host  
dirección que queremos averiguar  
ip del dominio que queremos resolver

### 1.12.2 HTTP

Protocolo (inseguro) TCP, utiliza el puerto 80 (*protocolo de transferencia de hipertexto*). Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Uno de los métodos más conocidos es GET donde el cliente envía datos al servidor solicitando una página, y POST existe un formulario ej. Password y nombre de usuario, posteriormente el servidor procesa los datos.

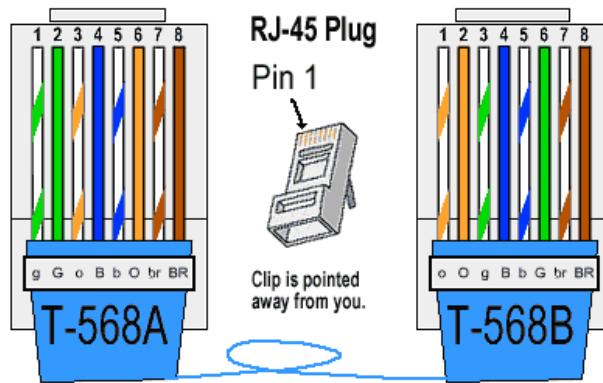
### 1.12.3 HTTPS

Se trata de una combinación de http más SSL puerto 443 TCP. Es un protocolo seguro cuyo texto será encriptado.

## 1.13 Cable UTP

Distancia máxima 100 m, sin que se deteriore el ancho de banda llega hasta categoría 7,

- Categoría 1.- telefonía
- Categoría 2.- transmisión de datos hasta 4Mbps
- Categoría 3.- (cable consola, plano) 10Mbps (10base T),
- Categoría 4.- Token ring, 16Mbps.
- Categoría 5.- cuatro pares trenzados (reduce los problemas de interferencia electromagnética EMI), transmisión de 100Mbps, conector RJ45.
- Categoría 5e.- Transmisión de 1Gbps (Mas utilizado hasta el momento)
- Categoría 6.- 10Gbps, puede llegar con dificultad.(se adiciona un aislante por cada par)
- Categoría 7.-10Gbps



**Cable directo:** T 568A – T568A o T 568B – T568B (más utilizado) Se lo utiliza cuando se conecta distintos equipos o de distinta capa (con la excepción de router-pc donde se conecta cable cruzado).

**Cable cruzado:** T 568A – T568B, Cuando se conecta equipos iguales o de la misma capa casi (ojo la mayoría usan MDI o MDIX).

Nota: Solo son funcionales los pares naranja y verde (cuatro pines)

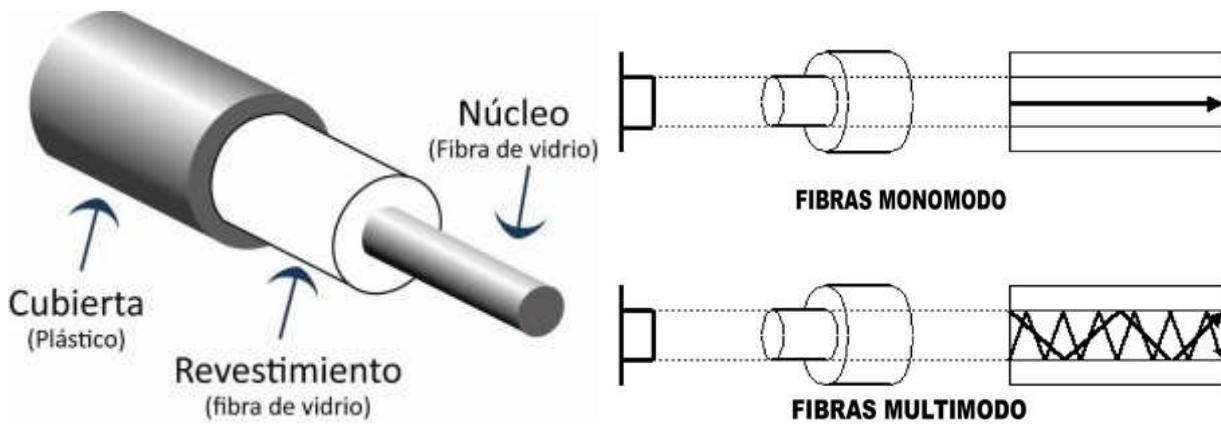
- MDI (Medium dependent interface): Si los cables están cruzados en un extremo se utiliza la tecnología MDI, para colocar como cable directo de manera lógica.
- MDIX (Medium dependent interface crossover): Sería el caso de los cables directos que gracias a esta tecnología (MDIX) los cruza en alguno de los extremos.
- NICs disponen MDI y routers y switchs MDIX

El cableado horizontal es el cableado que va desde las oficinas (en el mismo piso) hasta el data center o MDF. Vertical o backbone que es el cableado que conecta los data center entre pisos generalmente se usa F.O.



### 1.14 Fibra óptica

Son son afectados por el ruido eléctrico. Consiste en un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede provenir de un láser o un diodo led.



- **Multimodo MMF:** Núcleo de mayor diámetro, haz de luz puede tomar distintas direcciones, transmisión LED, distancias cortas.
- **Monomodo SMF.-** Núcleo delgado, solo una de luz en una dirección, transmisión LASER, alta velocidad largas distancias (Mayor costo).

Sus conectores usan GBIGs (Gigabit Interface Converter) y SFP (Small Form Factor Plugables) más usado, que son módulos que se insertan el switch



#### 1.14.1. Técnicas de multiplexación en sistemas ópticos

DWDM (multiplexación por longitud de onda densa): Puede multiplexar arriba de 256 canales en una sola fibra, soporta estándares de SDH (Synchronous Digital Hierarchy) y SONET (Synchronous Optical NETwork). Cada canal puede llevar 1 Gbps

#### 1.15 Funcionalidades de enrutamiento

Enrutamiento es el proceso de mover paquetes de datos de un origen a un destino, seleccionando la mejor ruta. El router es un dispositivo intermedio de red de capa 3, cumple los siguientes roles.

- construye dominios de Broadcast
- construye una tabla de enrutamiento.

El router determina el camino y envía el paquete. El router se divide de dos *partes*:

- **Data Plane** (procesamiento interno de conmutación)
- **Control Plane** (que envía hacia afuera, se encuentra la tabla de enrutamiento).

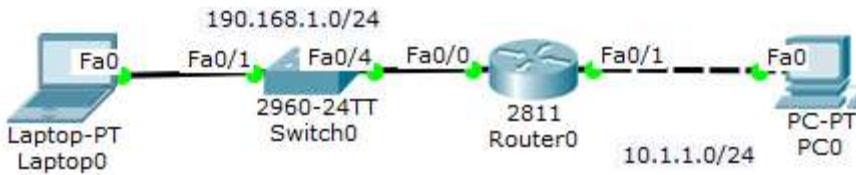
#### 1.15.1 Operaciones de enrutamiento

- Identifica el destino
- Identifica el origen
- Identificar las rutas
- Selecciona las rutas y las mantiene
- verifica la información de enrutamiento.

#### 1.15.2 Tabla de enrutamiento

##### 1.15.2.1 Ruta directamente conectada

Son los dispositivos que están conectados directamente al router. El router siempre conocerá las redes directamente conectadas cuya distancia administrativa es 0. La distancia administrativa define la prioridad cuanto menor sea, mayor será la prioridad.



```
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, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set
```

```
10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/1
C       192.168.1.0/24 is directly connected, FastEthernet0/0
```

#### 1.15.2.2. Ruta estática

Se define el camino o ruta de manera manual (altamente confiable), recomendables para redes pequeñas un ejemplo de enrutamiento estático es un teleférico. Las rutas estáticas no detectan cambios en la red, requiere de una actualización manual, son unidireccionales por ello se debe configurar en ambos extremos la ruta su distancia administrativa es 1.

```
Router 0 (conf)# ip route "dirección red destino" "máscara destino" "dirección ip next-hop o la interfaz de salida del router local" "distancia admi"
```

```
Router 0 (conf)# ip route 192.168.1.0 255.255.255.0 100.1.1.2 1
```

```
Router 0 (conf)# ip route 192.168.2.0 255.255.255.0 Fa 0/1 1
```

```
Gateway of last resort is not set

100.0.0.0/24 is subnetted, 3 subnets
C       100.1.1.0 is directly connected, FastEthernet0/1
C       100.1.2.0 is directly connected, Ethernet0/1/0
C       100.1.3.0 is directly connected, Ethernet0/3/0
S       192.168.1.0/24 [1/0] via 100.1.1.2
S       192.168.2.0/24 [1/0] via 100.1.2.2
S       192.168.3.0/24 [1/0] via 100.1.3.2
C       200.1.1.0/24 is directly connected, FastEthernet0/0
```

**Nota.-** se puede tener varios destinos con una sola salida pero no varias salidas para un mismo destino.

- Nos muestra la ip vecina #Show cdp neighbor
- Ver la tabla de enrutamiento #show ip route

#### 1.15.2.3. Ruta estática flotante

Son rutas estáticas que se utilizan para proporcionar una ruta de respaldo a una ruta estática o dinámica principal, en el caso de una falla del enlace. La ruta estática flotante se utiliza únicamente cuando la ruta

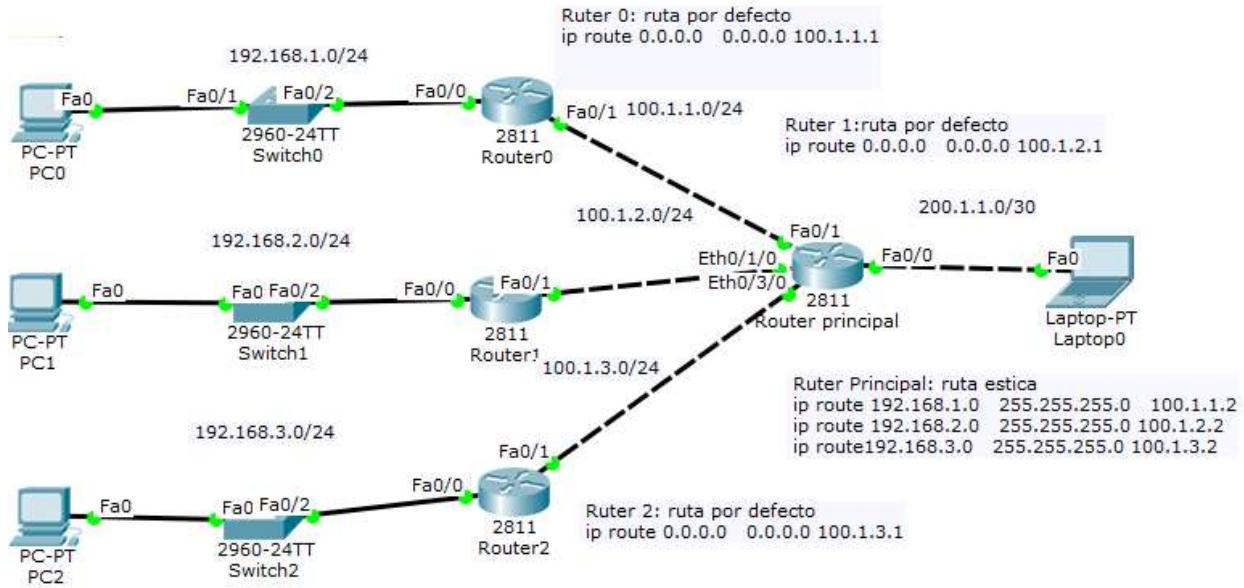
principal no está disponible. La ruta estática flotante se configura con una distancia administrativa mayor que la ruta principal.

#### 1.15.2.4. Ruta por defecto (ruta pre determinada)

Se define de manera manual pero el camino es dinámico, solo se le indica el destino cualquiera y la IP next-hop, no es muy confiable. Se usa comúnmente para configurar la salida a internet.

Router 0 (conf)# ip route 0.0.0.0 0.0.0.0 100.1.1.1 (puerta de ip vecina)

Router 0 (conf)# ip route 0.0.0.0 0.0.0.0 Fa 0/1 (interfaz local del router)



```
ROUTER_2#show ip route
```

```
Gateway of last resort is 100.1.2.1 to network 0.0.0.0
```

```
100.0.0.0/24 is subnetted, 1 subnets
C       100.1.2.0 is directly connected, FastEthernet0/1
C       192.168.2.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 100.1.2.1
```

#### 1.16. Ruta dinámica

Busca el mejor camino para llegar a destino de forma automática según su conveniencia. Se adecuan al cambio de redes, aprenden y mantienen de manera remota mediante de intercambios de enrutamiento periódicos, descubren nuevas redes y comparten sus tablas de enrutamiento. En resumen su función es:

- Descubrir redes remotas
- Mantener actualizado la información de enrutamiento
- Escoger la mejor ruta para llegar a destino logrando alta disponibilidad
- Me permite habilitar el mejor camino

Cada protocolo utiliza a su vez otros protocolos para su diseño, *Routed Protocol IP* (lleva paquetes en base al camino determinado) y *Routing Protocol* (determina el camino).

Existen de dos tipos de enrutamiento dinámico, distancia vector y estado de enlace.

### 1.16.1. Distancia vector

Informa a sus vecinos periódicamente de su estado, llevan carga de enrutamiento más que carga útil, puede generar bucles infinitos. RIP v2 (Routing Information Protocol) y EIGRP (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado), EIGRP se considera híbrido (distancia vector y estado de enlace) pero nació como distancia vector.

#### 1.16.1.1. RIP v2

Utiliza algoritmo de Bellman Ford (conteo de saltos), permite balanceo de carga por defecto 4 enlaces soportados, lamentablemente no utiliza parámetros como ancho de banda, usa como métrica el número de saltos ósea que escogerán el camino que tenga menores saltos. Admite hasta 15 saltos y actualizaciones cada 30 segundos, es multicast.

- **Permitir actualizaciones de unidifusión para RIP:** Debido a que RIP es normalmente un protocolo de difusión, para que las actualizaciones de enrutamiento RIP lleguen a redes que no son de difusión, debe configurar el software Cisco IOS para permitir este intercambio de información de enrutamiento. Para hacerlo, use el siguiente comando en el modo de configuración del enrutador:

Mando	Propósito
Router (config-router) # neighbor <i>ip-address</i>	Define un enrutador vecino con el que intercambiar información de enrutamiento.

- **Los temporizadores de Ripv2:**

- Update, por defecto 30s, son las actualizaciones periódicas que se envían.
- Invalid, 180 s, tiempo que se almacena en la tabla de enrutamiento.
- Flush, por defecto 240 s, tiempo para eliminar una ruta desde que se declara invalida.
- Holddown, 180s tiempo para prevenir los bucles.

```
Router# show ip protocols
```

```
Routing Protocol is "rip"
  Sending updates every 30 seconds next due in 21 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
```

Si se quiere cambiar estos parámetros

```
Router(config)# router rip
Router(config-router)# timers basic 30 180 180 240
```

Si se quiere que no envié sus actualizaciones pero si las reciba se debe poner el interface en pasivo

```
R-1(config)# router rip
R-1(config-router)# passive-interface fastEthernet 0/1
```

Se tiene dos problemas conteo al infinito (se copian información falsa de la cantidad de saltos cuando una red cae) y loops de enrutamiento (se genera información falsa). Una solución es:

- **Split Horizon** corta la comunicación de un sentido evitando actualizaciones en el bucle.
- **Route Poison** da de baja la red caída.

- **Poison Reverse** (envenena la ruta) una mezcla de los dos primeros indica que una ruta es infinita.
- **Hold Down Timer** espera 180 segundos a que se levante la red y luego la elimina de la tabla, en esos 180 segundos actúa el **Triger Update** intentando levantar la red (en 60s lo da de baja).

### 1.16.2. Estado de enlace (link-state routing protocol)

Requiere que todos los nodos estén informados en base una topología de red, OSPF (*Open Short Path First*) y IS-IS (*intermedia System Intermedia System*). Los protocolos de enrutamiento dinámico se basan en la métrica para elegir la mejor ruta, esta constante puede ser:

- Ancho de Banda que es la capacidad de envío de enlace.
- Delay (tiempo requerido para moverse de un origen a un destino, es inversamente proporcional al ancho de banda).
- Costo es inversamente proporcional al ancho de banda.
- Salto (hop count) el número de router a pasar para entregar los paquetes.

Nota.- con el comando siguiente se puede ver las redes vecinas: Show cdp neighbor.

### 1.16.2.1 Determinación del camino

El router puede usar diferentes protocolos de enrutamiento para determinar el camino, lo que le interesa es la Distancia Administrativa que es un valor numérico que indica la confiabilidad, cuanto menor es el valor mejor la confiabilidad.

C (ruta directamente conectada)= 0

S (ruta estática)= 1

EIGRP= 90

OSPF= 110

IS-IS= 115

RIP= 120

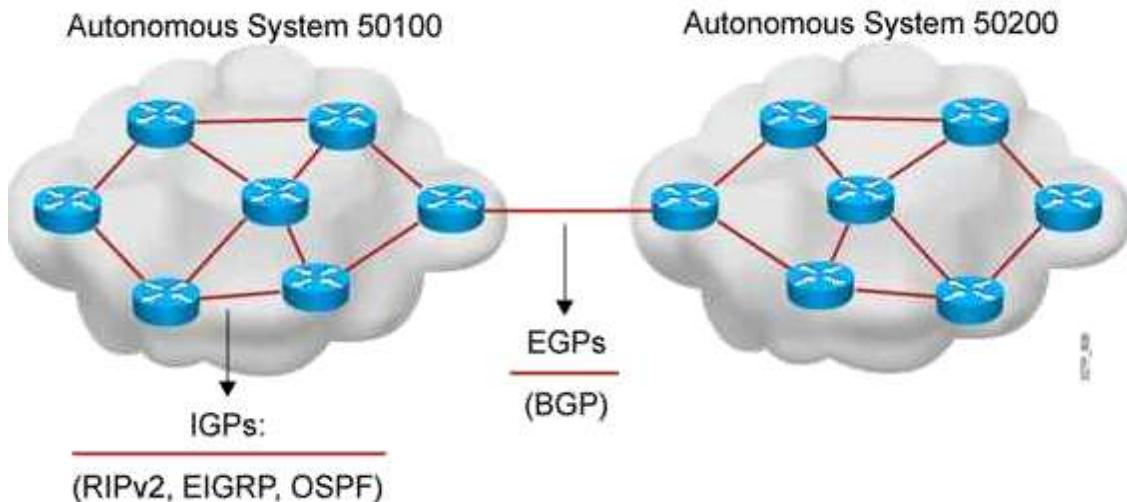
BGP= 200

*Nota: Se puede acceder a la tabla de enrutamiento mediante el comando “Show ip route”.*

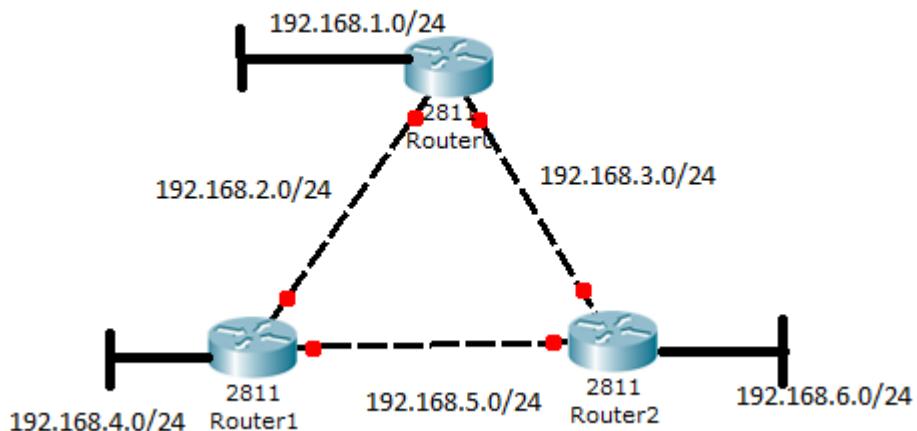
### 1.16.2.2. Grupos de enrutamiento

Existen dos tipos de protocolos:

- **Interior Routing Protocol o Interior Gateway protocol IGP:** RIPv2, EIGRP, OSPF están dentro del mismo sistema autónomo o sea que determinan el camino
- **Exterior Routed protocols o Exterior Gatewaey Protocol EGP:** BGP que comunica distintos sistemas autónomos. Un sistema autónomo es un sistema de redes bajo un dominio por ejemplo un dominio será la empresa axs y otro dominio Entel.

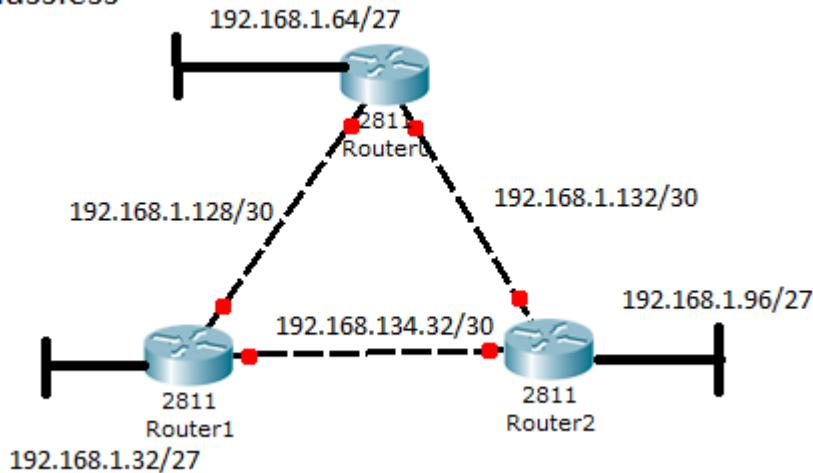


### 1.17. Classless CIDR (Classless Inter-Domain Routing) y classfull.-classfull



Son protocolos que no transmiten la máscara de subred en sus actualizaciones, la summarización ocurre en los límites de la red, las rutas que se intercambian entre redes diferentes se sumarizan al límite de la clase, entonces dentro de la red las rutas a las sub redes se intercambian sin la máscara de sub red, y a diferencia también de la classless todas las interfaces utilizan la misma máscara de sub red. “En este tipo de protocolos el router toma las decisiones basándose en las reglas del classfull aunque si existen en la tabla de routing una entrada a una ruta más específica a una red, esta será reenviada a esa red más específica”. Los protocolos que soporta el classfull son: RIP 1, EIGRP

## classless



Son los protocolos que incluyen la máscara de subred en sus actualizaciones, de modo que las interfaces de los dispositivos de una misma red pueden tener diferentes máscaras de subredes, es decir VLSM, tienen soporte para dominios sin utilizar clases, es decir CIDR, algunas rutas pueden ser sumarizadas dentro de los límites de una clase ya que esto se hace manualmente. Los protocolos que soporta el classless son: RIP 2, OSPF, EIGRP, IS-IS, BGP.

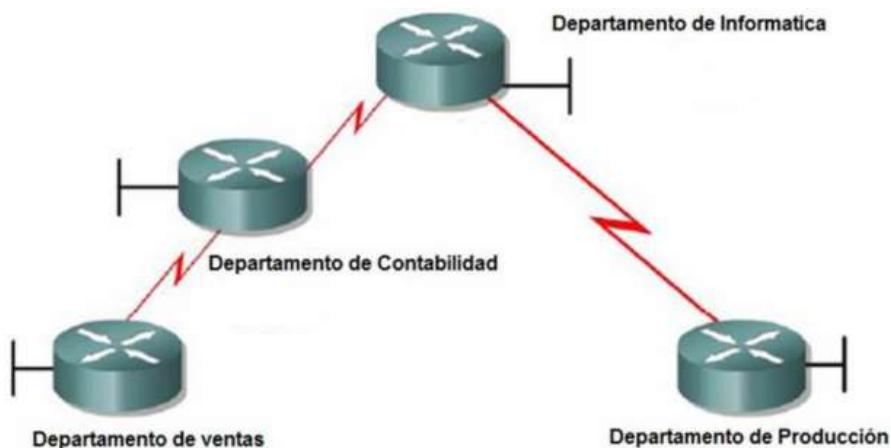
	Type	Convergence	Class	AD	Metric	Classless	Algorithm	Transport Type	Routing updates	propagate a default route
RIP v1	IGP	Slow	Distance Vector	120	Hop Count (max 15)	NO	Bellman-Ford	UDP/port520	every 30 seconds full table Broadcast 255.255.255.255	default-information originate
RIP v2	IGP	Slow	Distance Vector	120	Hop Count (max 15)	YES	Bellman-Ford	UDP/port520	every 30 seconds full table multicast address 224.0.0.9	default-information originate
OSPF	IGP	Fast	Link State	110	Cost	YES	Dijkstra (SPF) (OSPF)	IP protocol 89 (OSPF)	only when changes occurs multicast address 224.0.0.6	default-information originate
Integrated IS-IS	IGP	Fast	Link State	115	Cost	YES	Dijkstra (SPF)	Layer 2	only when changes occurs	default-information originate
EIGRP	IGP	Very Fast	Hybrid: (Advanced Distance Vector)	5 (summary) 90 (internal) 170 (external)	LOWEST BEST Composite (BW + DLY) Hopcount 100 (max 224)	YES	DUAL	IP protocol 88 (EIGRP)	multicast address 224.0.0.10 or unicast (RTP) only when change occurs	redistribute static
BGP	EGP	Average	Path Vector	20 (external) 200 (internal)	Path Attributes (Usually AS-Path)	YES	Best PATH	TCP/179	only when changes occurs (unicast updates)	default-information originate

### 1.17.1. VLSM (Variable Length Subnet Mask)

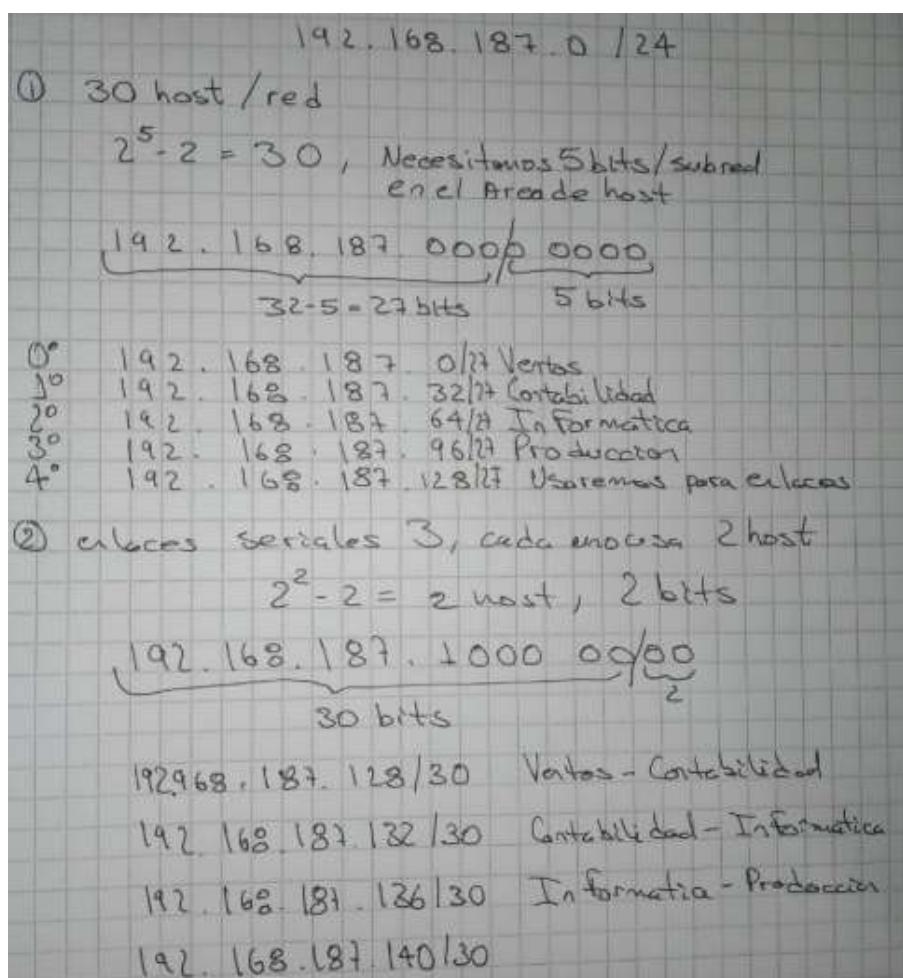
Máscara de longitud variable, sub dividir las redes reduce el tráfico de la red, optimiza el rendimiento, administración simplificado, facilidad de gestión. Lo que se debe responder en VLSM es:

- ¿Cuántas subredes se obtienen de la máscara?
- ¿Cuántos hosts válidos por subred?
- ¿Cuál es la dirección de Broadcast y red de esas subredes?

Ejemplo:



Se requiere subnetear la red 192.168.187.0 /24 para la red de una empresa.  
Departamento 30 direcciones utilizables (host).



#### 1.17.1.1. CIDR (classless interdomain Routing) RFC 1517

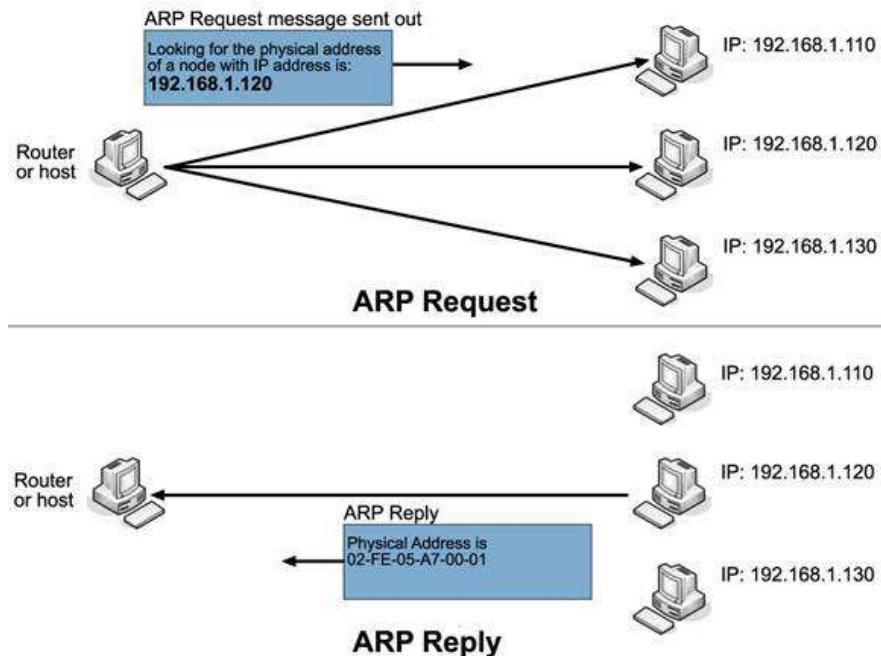
Permite un uso eficiente del espacio de direcciones IPv4, debido a la introducción del prefijo "/" que reduce el tamaño de las tablas de enrutamiento al no depender de la clase

### 1.18. ARP (Address Resolution Protocol)

Protocolo de capa 3 con funcionalidades en capa 2, nos permite resolver o traducir una dirección IP a una dirección MAC y la función *Caching* que nos permite localizar la dirección MAC de un dispositivo. En fin ARP verifica de dónde viene la dirección IP y donde está contenido la dirección MAC.

Lo primero que hace es mandar a todos un mensaje (*broadcast*) para verificar que dirección MAC le corresponde a la dirección IP, lo que se llama *ARP REQUEST* y el destinatario responde con un mensaje (*unicast*) indicando la dirección MAC que tiene *ARP REPLY*. El comando para verificar la tabla ARP en CMD de windows es: **arp -a**, si se desea ser más específico se usa: **arp -a -n dirección IP**

El comando para verificar la tabla ARP en el router es: **show ip arp**



Nota: El inverso de ARP es RARP (Reverse Address Resolution Protocol) que traduce las direcciones MAC a direcciones IP.

### 1.19 Puerta de enlace (Gateway)

Nos permite salir a redes externas a la local, generalmente esta siempre en el router. Un Gateway permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. Para ello realiza operaciones de traducción de direcciones IP (NAT: Network Address Translation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

### 1.20. Seguridad

Es el conjunto de políticas, procesos y herramientas de hardware y software que se encargan de proteger la privacidad la disponibilidad y la integridad de la información y los sistemas de una red. Se debe tener claro los siguientes conceptos:

- **Threats (amenazas):** intentos maliciosos que comprometen las políticas de seguridad

- **Malware:** software dañino que se instala.
  - Virus: código malicioso que se adjunta a archivos ejecutables que son programas legítimos, los virus requieren activación del usuario final.
  - Trojan: lleva a cabo operaciones maliciosas bajo la apariencia de una función deseada, explota los privilegios del usuario que lo ejecuta.
  - Worm: se replica explotando de forma independiente las vulnerabilidades en la red, son programas autónomos que atacan un sistema para explotar una vulnerabilidad conocida.
  - Ramsomware: niega el acceso y exige un rescate pagado
  - Phising: Correos fraudulentos que intentan que se divulgue información confidencial.
  - Rootkit: acceso privilegiado al hacker
  - Scareware: software de estafa de ingeniería social mediante percepción de amenaza
  - Spyware: recopila información de un usuario y envía a otra entidad (Key logger)
  - Adware: ventanas emergentes
- Hacker: usuario con conocimientos avanzados de informática que los usa para acceder a sistemas no autorizados o manipularlos
- Vulnerabilidad: una debilidad que se puede explotar, un bugs, o código erróneo.
- Exploit: usa la vulnerabilidad para acceder al sistema

#### **Tipos de ataques a la red:**

- Ataques de reconocimiento: Ping sweep, port scan
- Ataques de acceso: Password attack, port redirection, man-in-the-middle, spoofing, buffer overload
- Ataques de ingeniería social: phishing, span
- DoS (denegación de servicio):Ping of Death, Smurf, TCP SYN flood, DDoS

#### **Técnicas de mitigación:**

- Firewalls
- Parches de software
- Antivirus
- antimalware

**Elementos de un programa de seguridad:** Concientización del usuario de los riesgos y políticas de seguridad, capacitación periódica, control de acceso a equipos.

**Contraseñas:** al menos 8 caracteres mayúsculas minúsculas números caracteres especiales. Cambios periódicos cada 30 días

**Contraseñas multifactor:** login+SMS, login+APP, login+Token

**Certificados:** Documento electrónico firmado por una entidad certificadora que acredita la identidad del titular y asocia dicha entidad con un par de claves una pública y otra privada

#### **1.20.2 ACL (Access Control List) listas de acceso**

Son sentencias que clasifica filtran tráfico a través del router. Una lista de acceso nos permite identificar el tráfico, crear listas que permitan o nieguen el acceso, identifican tráfico en base a paquetes IP, opera en capa 3 y 4 (identificando puertos), son secuenciales de lo más específico a lo más general.

Wildcar (tarjeta de invitación) es un valor de 32 bits que compara los bits para filtrar los paquetes IP, un bit “0” es comparar y un bit “1” es ignorar, la wildcard resulta del inverso de la máscara de subred. Una wildcard **host** es comparar todos 0.0.0.0 y una wildcard **any** es ignorar todos 255.255.255.255

Nota: no se solapan (si se equivocan en una lo mejor es borrar toda la lista) y siempre se crea una ACL que lo deniega todo

Se siguen reglas importantes en las Wildcard deben ser semejante a una subred o el inverso de esa subred, segundo los el número de las wildcard debe ser 0, 1, 3, 7, 15, 63, 127, 255. Existen dos tipos de listas de acceso.

### 1.20.3. Listas de acceso estándar

Solo revisan tráfico de origen, filtran toda la suite de protocolos (TCP/IP), el número de lista van del 1 al 99 o 1300 al 1999, también pueden ser nombradas. Solo se permite una lista de acceso por interfaz (se recomiendan su uso cerca de destino).

```
Router (conf)# Access-list 1 permit 172.16.0.0 0.0.255.255//permite toda la clase B
Router (conf)# Access-list 1 permit host 172.16.1.20 //permite solo la IP 172.16.1.20
Router (conf)# Access-list 1 permit any // es equivalente a 0.0.0.0 255.255.255.255
```

Para aplicar las listas de acceso se debe asignar a una interface para ello se tiene:

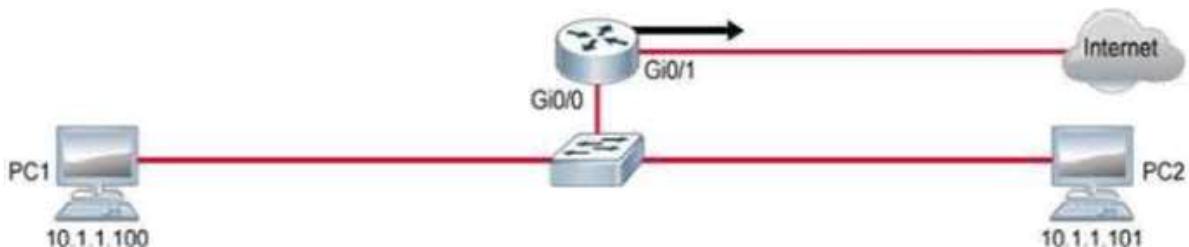
- **Listas de acceso outbound:** Tráfico que ha sido analizado para permitir su salida del router.

```
Router(config-if)# ip access-group 1 out
```

- **Listas de acceso inbound:** tráfico que va a ser analizado antes de su entrada al router.

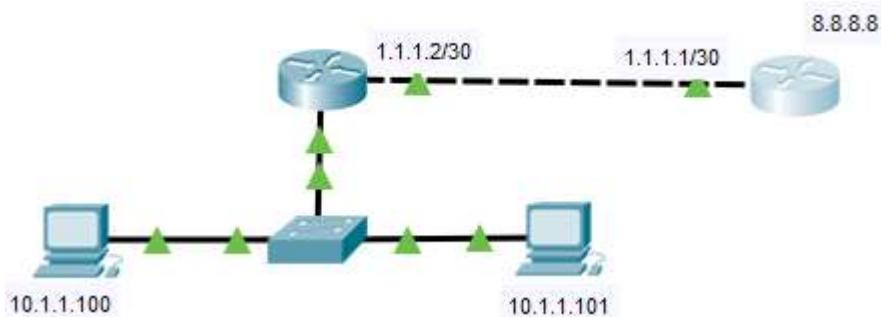
```
Router(config-if)# ip access-group 1 in
```

Ejemplo: denegar el acceso a internet del host 10.1.1.101 y permitir el resto de la subred.



```
Branch(config) #access-list 1 deny 10.1.1.101
Branch(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Branch(config)# interface GigabitEthernet 0/1
Branch(config-if)# ip access-group 1 out
```

Una lista de acceso por protocolo, por dirección, y por interface (es de salida o de entrada).



```
interface GigabitEthernet0/0
```

```
ip address 10.1.1.1 255.255.255.0
```

```
ip nat inside
```

```
interface GigabitEthernet0/1
```

```
ip address 1.1.1.2 255.255.255.252
```

```
ip nat outside
```

```
access-list 1 deny host 10.1.1.101
```

```
access-list 1 permit 10.1.1.0 0.0.0.255
```

```
ip nat inside source list 1 interface GigabitEthernet0/1 overload
```

Nota: para ver las listas de acceso se usa el comando: **show Access-list**. Para borrar una lista de acceso: **no Access-list 1**.

```
R1#show access-lists
```

```
Standard IP access list 1
```

```
10 deny host 10.1.1.101 (4 match(es))
```

```
20 permit 10.1.1.0 0.0.0.255 (8 match(es))
```

#### 1.20.4. Listas de acceso extendidas

Revisan origen y destino, filtran protocolos específicos y aplicaciones específicas (puertos específicos), el número de lista va del 100 al 199 y del 2000 al 2699 también pueden ser nombradas (se recomiendan su uso cerca de origen).

Ejemplo: permitir todo tcp/ip menos telnet al host 172.16.2.1 desde la red 10.1.1.0/24

```
Router(conf)# access-list 100 deny tcp 10.1.1.0 0.0.0.255 172.16.2.1 0.0.0.0 eq 23
```

```
Router(conf)# access-list 100 permit ip any any
```

```
Router(conf)# interface gigabitEthernet 0/1
```

```
Router(conf- If) # ip Access-group 100 in
```

### 1.20.5. Radius y tacacs

Ambos se puede usar para comunicar el router y el servidor AAA, TACACS+ se considera más seguro, debido a que todos los intercambios de protocolo son encriptados y RADIUS solo la contraseña no así el nombre de usuario.

Los factores críticos de TACACS son 3: Los factores críticos de RADIUS son 4:

- Separa authentication y authorization
- Encripta todas las comunicaciones
- Utiliza el puerto TCP 49
- Combina authentication y autorization como un proceso
- Encripta solo password
- Usa UDP 1645 o 1812 para autenticación y UDP 1646 o 1813 accounting
- Admite tecnologías de acceso remoto 802.1x y protocolos de inicio de sesión.

#### Configurando RADIUS

```
R1(config)#aaa new-model
```

```
R1(config)#radius server SERVER-R
```

Por defecto los enrutadores cisco usan el puerto udp 1645 para autenticarse y el 1646 para contabilidad, pero IANA ha reservado los puertos udp 1812 y 1813 respectivamente

```
R1(config-radius-se)#address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
```

```
R1(config-radius-se)#key RADIUS-PASSWORD
```

Nota: para verificar que la autenticación esta funcionando correctamente usar

```
# test aaa group radius USUARIO PASSWORD legacy
```

#### Configurando TACACS+

Habilitamos aaa

```
R1(config)#aaa new-model
```

designamos el nombre servidor tacacs (se puede configurar multiples servidores)

```
R1(config)#tacacs server SERVER-T
```

configuramos la direccion ip del servidor tacacs, se puede modificar el puerto de Authentication y accounting

```
R1(config-server-t)#address ipv4 192.168.1.101
```

mejora el rendimiento TCP al mantener una unica conexion TCP durante la vida de la sesion

```
R1(config-server-t)#single-connection
```

Se configura una clave secreta compartida para cifrar la transferencia de datos, esta clave es la misma que en el servidor TACACS

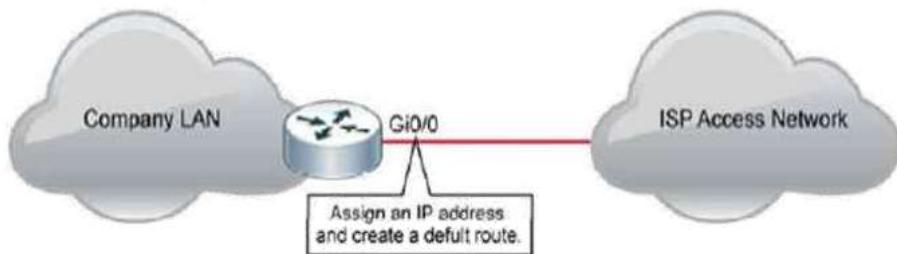
```
R1(config-server-t)#key TACACS-PASSWORD
```

## 1.21. Servicios IP

Conectarse a internet significa conectarse a la red global de acceso público, cuando se trata de sucursales (bancos) se trata de redes WAN cuya interconexión no depende de una salida a internet, el método de conexión puede ser mediante fibra óptica, cable de cobre, o de manera inalámbrica. El proveedor de internet ISP, es el encargado de proporcionarme dicha conexión, existen dos maneras de proporcionarme una conexión a internet mediante dirección IP, la manera estática (una sola dirección IP que me permite salir a internet) y la manera dinámica DHCP(cada cierto tiempo cambia la dirección).

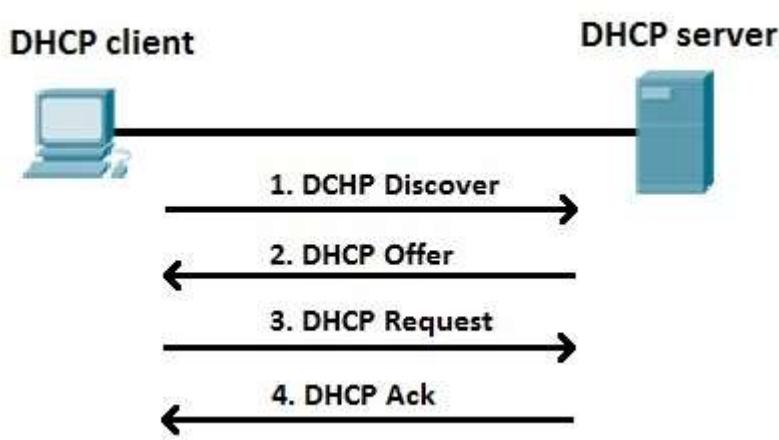
De manera estática se debe configurar manualmente en la interfaz una dirección IP y una ruta por defecto.

```
Router(config)# interface GigabitEthernet 0/0
Router(config-if)# ip address 209.165.200.225 255.255.255.224
Router(config-if)# no shutdown
Router(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.254 1
```



## 1.22. DHCP (Dynamic Host Configuration Protocol)

Protocolo de configuración dinámica de host (capa 7 debido a que es una aplicación en si misma), depende de un pool (rango de direcciones), el servidor cumple cuatro tareas al momento de designar (el router puede funcionar como servidor de DHCP):



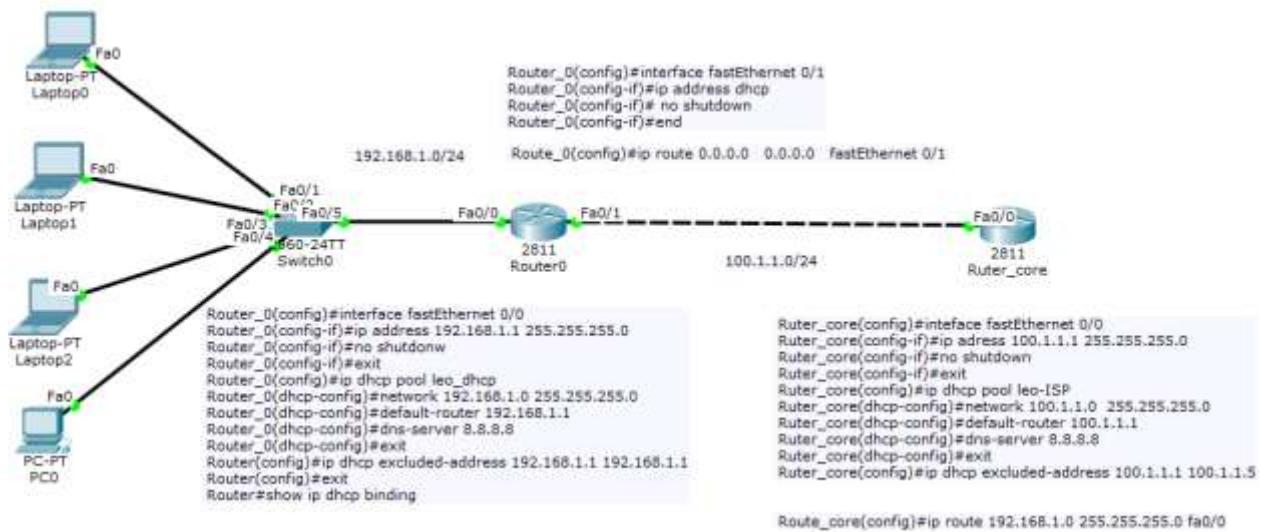
**1.- discovery (Broadcast).**- El cliente no tiene una dirección IP, mandar un mensaje para descubrir al servidor.

**2.- offer (unicast).**- El servidor responde con un mensaje de oferta

**3.- request (broadcast).**-Manda un mensaje de requerimiento de dirección IP.

**4.- ack (unicast).**- El servidor manda un mensaje donde le asigna una dirección IP.

Cuando no hay más IP en DHCP el servidor auto asigna una **APIPA** (Automatic private internet protocol address) 169.254.0.0/16, eso también ocurren cuando no existe quién le asigne al host una dirección IP.

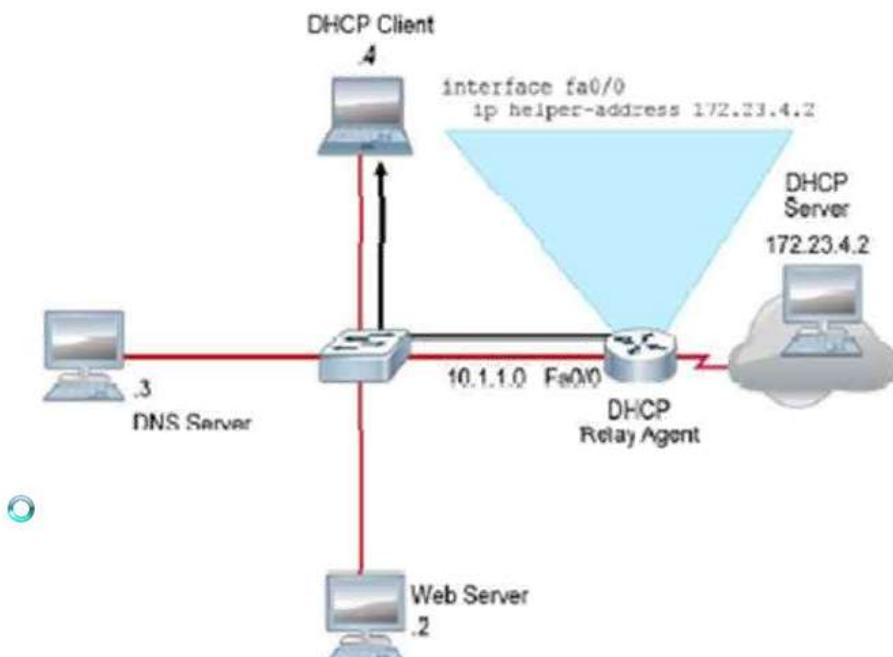


También se utiliza este protocolo en redes VLAN. Me muestra las direcciones IP asignadas **show ip dhcp binding**

### 1.2.2.1. DHCP con Relay agent (agente de trasmisión)

Normalmente la adquisición de parámetros de IP usando DHCP se hace por Broadcast (Difusiones) de subred, y por lo tanto no pasa por los Routers (Enrutadores). La primera solución es poner un servidor DHCP en cada subred que no es conveniente. Entonces tienes la opción de poner un único servidor DHCP, donde creas ámbitos diferentes, uno para cada subred.

Los clientes que están en la misma red del servidor, lo tomarán directamente, los clientes que están en otra red diferente deben llegar al DHCP a través del DHCP Relay Agent. Éste escuchará los pedidos de los clientes, los reenviará al DHCP, el DHCP le responderá al Relay Agent, y este último le responderá al cliente "como si fuera" el DHCP.

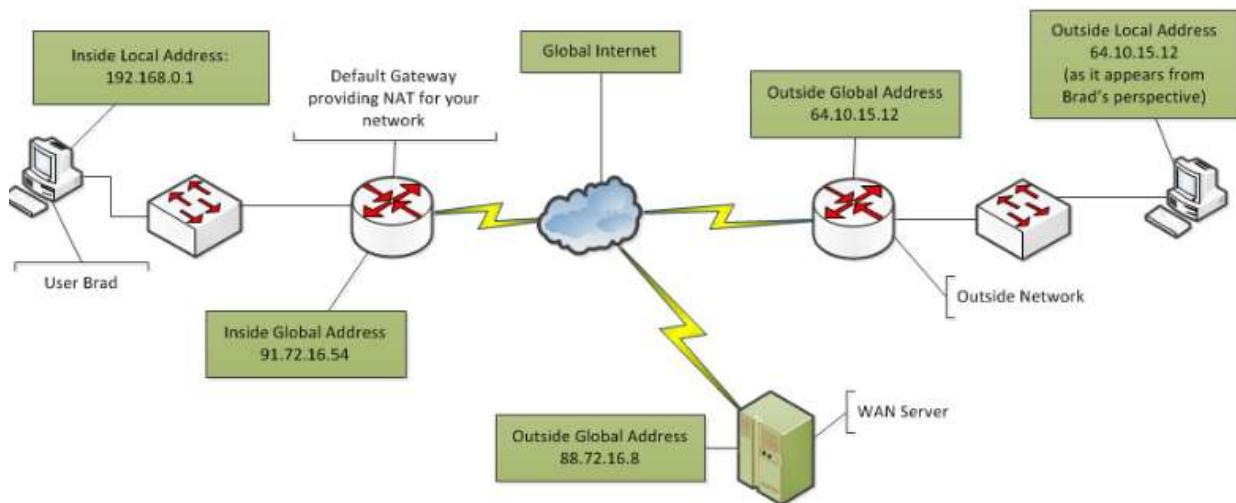
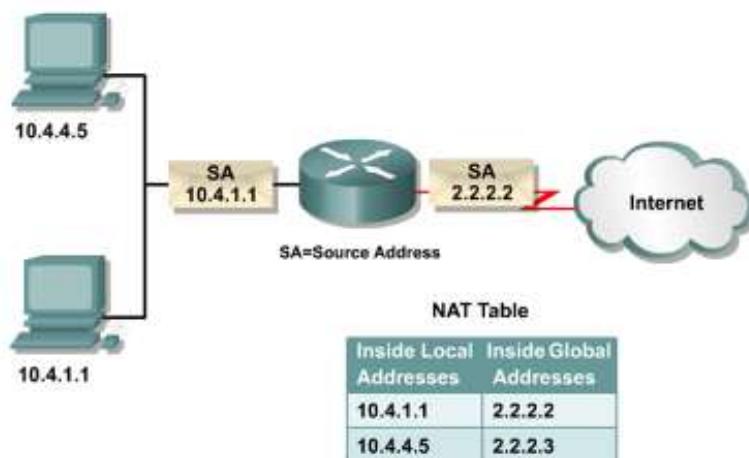


El comando se aplica a la interface de entrada a la red local en este caso fa 0/0, y se le indica al ip del servidor DHCP 172.23.4.2 que está conectado a otra interfaz (red distinta).

```
Router(conf)#interface fastethernet 0/0
Router(conf-if)#ip helper-address 172.23.4.2
```

### 1.23. NAT (Network Address Translation)

NAT nos permite hacer traducciones de IP (de una red a otra red), privadas a privadas, públicas a públicas o públicas a privadas y viceversa. El router lo que hace es crear una tabla NAT donde anotó en la dirección IP local y la dirección IP con la que va a salir. Existen tres tipos de NAT, nat estatico, nat dinamico, pat.



- Inside local.- dirección de la red local direcciones privadas.
- Inside global.- dirección pública con la que salgo de mi red local.
- Outside local.- La dirección que maneja el proveedor de internet (no lo conocemos).
- Outside global.- De hacia dónde quiere llegar ej. Google 8.8.8.8.

#### 1.23.1. NAT estática

Asignación de dirección IP uno a uno (correo electrónico).



```

interface GigabitEthernet0/0
description LAN1
ip address 10.1.1.1 255.255.255.0
ip nat inside

```

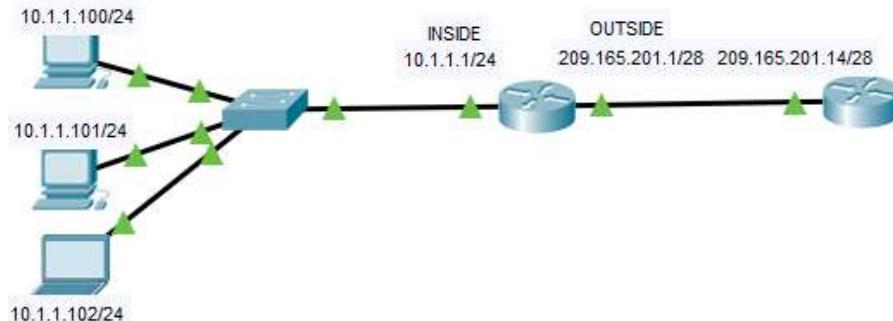
```

interface GigabitEthernet0/1
description WAN
ip address 209.165.201.1 255.255.255.240
ip nat outside
!
ip nat inside source static 10.1.1.2 209.165.201.5
ip route 0.0.0.0 0.0.0.0 209.165.201.14

```

### 1.23.2. NAT dinámica

Asignación de IP de muchos a muchos, mediante un pool (servicios de DNS). La cantidad de direcciones que se traducirán deben ser equivalentes, ejemplo si usamos 3 direcciones locales necesitamos mínimamente 3 direcciones públicas



```

interface GigabitEthernet0/0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
interface GigabitEthernet0/1
ip address 209.165.201.1 255.255.255.240

```

```

ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
ip nat pool NAT-DINAMIC 209.165.201.2 209.165.201.4 netmask 255.255.255.240
ip nat inside source list 1 pool NAT-DINAMIC
!
ip route 0.0.0.0 0.0.0.0 209.165.201.14

```

**Nota:** nos muestra la tabla de traducción: **show ip nat translation**

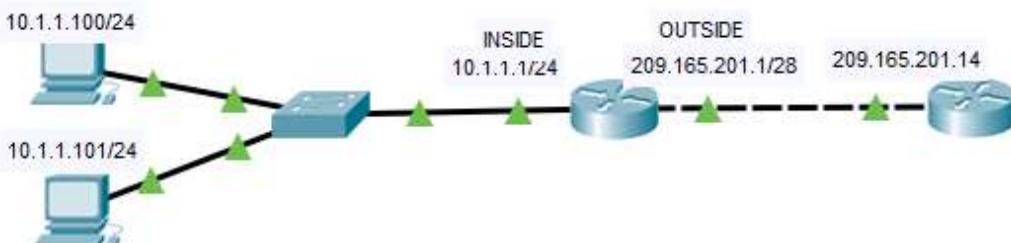
```

R2#show ip nat translations
Pro Inside global     Inside local      Outside local      Outside global
icmp 209.165.201.2:81 10.1.1.101:81  8.8.8.8:81        8.8.8.8:81
icmp 209.165.201.2:82 10.1.1.101:82  8.8.8.8:82        8.8.8.8:82
icmp 209.165.201.2:83 10.1.1.101:83  8.8.8.8:83        8.8.8.8:83
icmp 209.165.201.2:84 10.1.1.101:84  8.8.8.8:84        8.8.8.8:84
icmp 209.165.201.3:53 10.1.1.102:53  8.8.8.8:53        8.8.8.8:53
icmp 209.165.201.3:54 10.1.1.102:54  8.8.8.8:54        8.8.8.8:54
icmp 209.165.201.3:55 10.1.1.102:55  8.8.8.8:55        8.8.8.8:55
icmp 209.165.201.3:56 10.1.1.102:56  8.8.8.8:56        8.8.8.8:56
icmp 209.165.201.4:63 10.1.1.100:63  8.8.8.8:63        8.8.8.8:63
icmp 209.165.201.4:64 10.1.1.100:64  8.8.8.8:64        8.8.8.8:64
icmp 209.165.201.4:65 10.1.1.100:65  8.8.8.8:65        8.8.8.8:65
icmp 209.165.201.4:66 10.1.1.100:66  8.8.8.8:66        8.8.8.8:66

```

### 1.23.3. PAT (Port Address Traslation)

Asignación de IP muchos a uno, se maneja puerto de 16 bits. Permite conectar a Internet muchos equipos utilizando únicamente una dirección IP. Dicha solución consiste básicamente en "jugar" con los puertos para multiplexar las conexiones de varios equipos a través de una conexión de salida. Gracias a la PAT.



interface GigabitEthernet0/0

ip address 10.1.1.1 255.255.255.0

ip nat inside

!

interface GigabitEthernet0/1

ip address 209.165.201.1 255.255.255.240

```
ip nat outside
```

```
!
```

```
access-list 1 permit 10.1.1.0 0.0.0.255
```

```
ip nat inside source list 1 interface GigabitEthernet0/1 overload
```

```
ip route 0.0.0.0 0.0.0.0 209.165.201.14
```

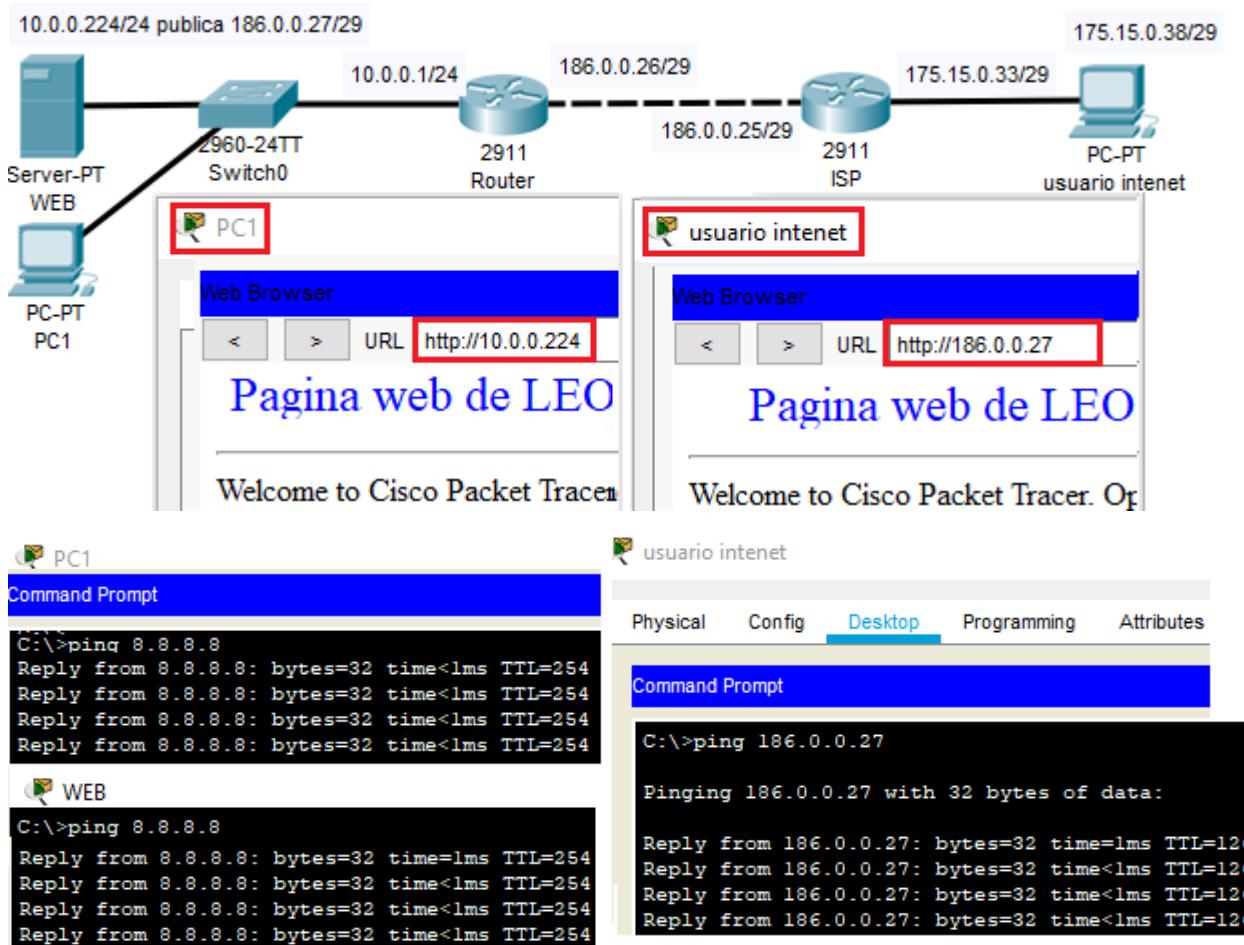
**Nota1:** %Dynamic Mapping in Use, Cannot remove o el mensaje del %Pool outpool in use, cannot destroy. Usted está intentando cambiar a la parte de una configuración del NAT que sea responsable de crear las traducciones dinámicas que todavía existen en la tabla de traducción. Deberá limpiar la tabla de traducciones que se está utilizando antes de aceptar el cambio. Puede llevar más de un intento

```
# clear ip nat translation *
```

**Nota 2:** overload significa que existe una relación de muchos a uno entre las direcciones "privadas" y las direcciones "públicas".

#### 1.23.4. Aplicación nat para página web

Se tiene un servidor web con la IP privada 10.0.0.224/24, en la misma red se encuentran otros usuarios que necesitan salida a internet, además que usuarios de internet deben acceder al servicio web.



**ISP**

```
#interface GigabitEthernet0/0
ip address 175.15.0.33 255.255.255.248
#interface GigabitEthernet0/1
ip address 186.0.0.25 255.255.255.248
#interface Loopback0
ip address 8.8.8.8 255.255.255.0
```

**Router**

```
#interface GigabitEthernet0/0
ip address 10.0.0.1 255.255.255.0
ip nat inside
#interface GigabitEthernet0/1
ip address 186.0.0.26 255.255.255.248
ip nat outside
#ip route 0.0.0.0 0.0.0.0 186.0.0.25
#ip access-list extended internet
deny ip host 10.0.0.224 any
permit ip 10.0.0.0 0.0.0.255 any
#ip nat inside source list internet interface GigabitEthernet0/1 overload
#ip nat inside source static 10.0.0.224 186.0.0.27
```

### 1.24. Calidad de servicio QoS

Es la calidad de los dispositivos para priorizar un tipo de tráfico, como trasmitir voz y datos simultáneos. El tráfico de voz y video es sensible a retardo, paquetes perdidos y jitter (variación del retardo o tiempo de llegada de paquetes). Calidad de servicio garantiza ancho de banda a un tráfico o aplicación determinado.

## Bandwidth Use without QoS control



## Bandwidth Use with QoS control



## Mecanismos de QoS

- **Best effort** (default): no hay prioridad
- **Integrated Services Model- IntServ RSVP**: Ruta QoS prenegociada de extremo a extremo.
- **Differentiated Services Model-DiffServ**: en cada router prioriza el tráfico de acuerdo a una configuración.

## Etiquetado de tráfico

Capa 2: CoS Class of Service (clase de servicio), 3bits

Capa 3:ToS Type of Service (tipo de servicio), 3 bits y DSCP differential Services Code Point, 6 bits

DSCP se usa en los routers y en los switches se marca las tramas con CoS

### 1.24.1. MQC Modular QoS Command Line Interface

El modelo de implementación de QoS, identifica y clasifica los flujos de tráfico, aplica políticas de QoS, define las interfaces en las cuales la política será aplicada.

- **Class-map**: asocia uno o varios atributos, con el QoS determinado a ese tráfico. Los atributos varían según el hardware.

Match on	Catalyst 2950	Catalyst 3550	Description
access-group	X	X	Access group
ip dscp	X	X	A specific DSCP value or a list of values
ip precedence		X	A specific IP precedence value or a list of values
any		X	Any packet
class-map		X	A nested class-map
destination-address		X	A destination MAC address

- **Policy-map**: crea la política de tráfico, contiene 3 elementos nombre de la política, clase de tráfico y la política QoS.

#### Ejemplo:

Cualquier tráfico que ingrese a esa interfaz se denomina crítico

```
#class-map match-any critical
```

```
match interface fastEthernet 0/1
```

Se asigna un ancho de banda de 10Mbps a un tráfico indicado por el class-map

```
#policy-map Politica01
```

Class critical

Bandwidth 10000

Aplicamos a la interfaz

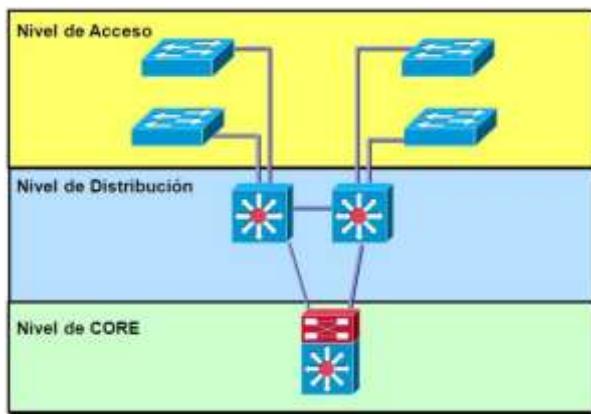
```
# interface Gigaethernet 0/1
```

Service-policy output Politica01

## 2.1. Diseño de una red LAN

Se divide en 2 y 3 niveles dependiendo del tamaño de la implementación, la de dos niveles tiene Acceso y Core/Distribution (core colapsado) que es donde se encuentra el gateway. De tres niveles, Core donde se encuentra el Gateway, Distribución (conexiones de F.O.) y Acceso

El diseño de red LAN se divide en 3 niveles



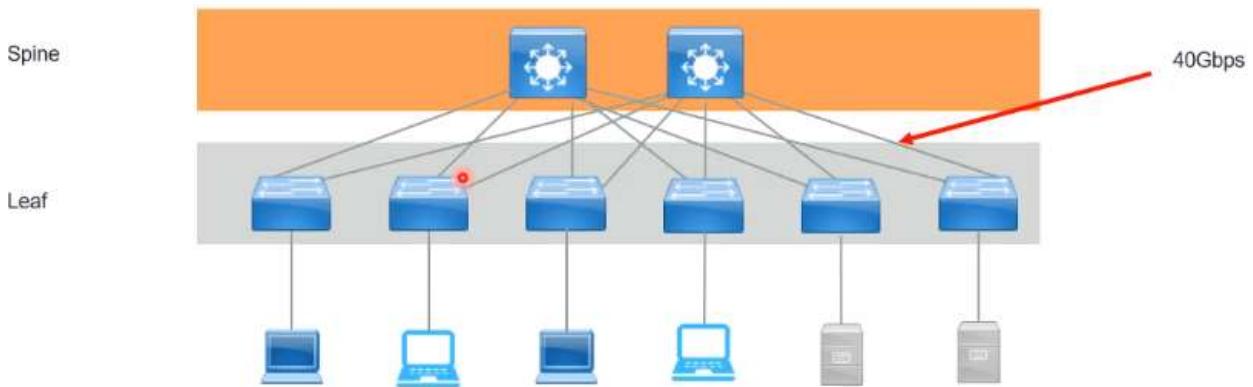
- **Core:** Equipos de gama alta ofrecen alta velocidad de distribución de datos, conectividad las 24hr, equipos como 6800 y 6500.
- **Distribución:** Se trata de equipos multi-capa, generalmente se maneja sólo un equipo Router o Switch que ofrece servicios de conectividad, políticos de conectividad, políticos de seguridad equipos como switch, Router como 3560, 3750 3850.
- **Acceso:** permite el acceso al cliente, el control del mismo, proveen la conectividad con dispositivos finales laptops, teléfono IP, celular, servicio de seguridad, y switch equipos como 2960 o 2950.

En un entorno de proveedor, en la capa Core se usa en equipos como 7200, en la capa de distribución equipos como el 4000, y en la capa de acceso equipos como el 800, debido a que en la capa de acceso se encuentran los clientes.

### 2.1.1. Topología Spine and Leaf

Usada en los data center, no tiene spanning tree usa ACI VXLAN, tráfico de Este a Oeste (tráfico entre servidores), elimina los cuellos de botella. En Spine se tiene los equipos principales altas velocidades

(cisco nexus, libre de bucles). En Leaf se usa switches que conectan equipos servidores y tienen una conexión doble hacia los equipos de Spine.



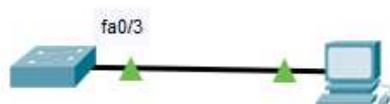
## 2.2. VLAN (virtual área network)

Es un método para crear redes lógicas independientes dentro de una misma red física.

Varias VLAN pueden coexistir en un único switch físico o en una única red física. Se trata de un grupo de usuarios o pc, con tareas comunes separados de los demás.

- Provee seguridad (lo que haga cada grupo es independiente de otro).
- Flexibilidad (independiente del espacio físico específico, se trata de una separación lógica).
- Segmentación (separar en distintas subredes).

### 2.2.1. Creación de VLAN



Switch(config)#vlan 2

Switch(config-vlan)#name Sales

Show vtp status.- Nos verifica el número de Vlan que podemos crear

```
Switch#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MDS digest : 0x7D 0x5A 0xA6 0x0E 0x5A 0x72 0xA0
0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

#### Asignacion de puerto

```
interface FastEthernet0/3
switchport access vlan 2
switchport mode access
```

Al puerto que se le asignó a la vlan se llama acceso (Switch a pc), una sola VLAN por puerto acceso (excepto con una vlan de voz).

**Show vlan brief:** comando de verificación.

Switch#show vlan brief			
VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
2	Sales	active	Fa0/3
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Por defecto existe la vlan 1 que ya está creada, todos los puertos que no se les haya asignado una Vlan pertenecen a esta Vlan por defecto. Las VLANs 1002, 1003, 1004, 1005 están presentes por defecto están reservadas para “token ring” y FDDI.

**Show interfaces fastethernet0/3 switchport:** nos muestra detalles específicos de la interface.

```
Switch#show interfaces fastEthernet 0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 2 (Sales)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

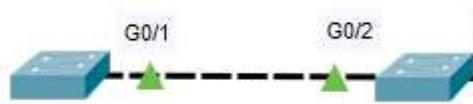
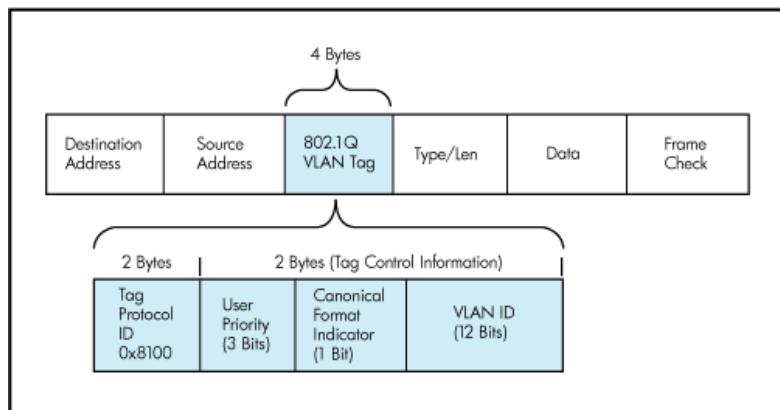
### 2.2.2. Trunk (Troncal)

Troncal se llama a la conexión entre Switch por donde que atraviesan varias Vlan (switch a switch o switch a router), puede transportar varias VLAN, la troncal utiliza encapsulación 802.1q. Ejemplo el dato que llega al switch es encapsulado y etiquetado “TAG”. Es un entramado o *framing* a nivel de capa 2 se manejan datos tipo trama.

La abreviación de 802.1q es “dot1q” lo que adiciona a la trama 4 Bytes (transforma la trama), y soporta 4096 VLAN (vlan ID 12 bits) y contiene FCS (*Frame Check Sequence*) revisión de errores.

*Nota: dot1q está configurado por defecto en capa 2, solo se configura en capa 3 (catalys 3560) comando “switchport trunk encapsulation dot1q”.*

802.1q combina múltiples VLAN por un mismo puerto llamado troncal, cada trama tiene su propia etiqueta que identifica la VLAN a la cual pertenece.



```
interface GigabitEthernet0/1
```

```
switchport mode trunk
```

```
switchport trunk native vlan 99 ( indica la vlan que no se etiquetara)
```

```
switchport trunk allowed vlan 7,8,9 ( permite solo las vlans seleccionadas, remplaza)
```

```
switchport trunk allowed vlan add 10 (adiciona las vlans a las ya configuradas, no remplaza)
```

```
switchport trunk allowed vlan remove 10 (remueve la vlan indicada)
```

Nota: en este ejemplo se cambió la Vlan nativa de la 1 a la 99, esta configuración se debe hacer en ambos switch.

**# Show interface fastethernet0/3 swichport:** nos muestra detalles específicos de la interface.

**# Show interface trunk:** me muestra las interfaces en la troncal

```
SW2#show interfaces trunk
Port      Mode       Encapsulation  Status        Native vlan
Gig0/2    on        802.1q        trunking     99

Port      Vlans allowed on trunk
Gig0/2    1-1005

Port      Vlans allowed and active in management domain
Gig0/2    1,2

Port      Vlans in spanning tree forwarding state and not pruned
Gig0/2    1,2
```

## 2.2.3. Vlan nativa

Me permite administrar, por defecto es la 1, esta vlan administrativa no se etiqueta, todo puerto que no se le asigne una vlan pertenecerá por defecto a la vlan nativa. Algunas consideraciones que se deben tener con VLAN:

- Para cambiar la VLAN nativa se ingresa en las interfaces troncales y se coloca:  
**switchport trunk native vlan 99**
- Verificar el número máximo de VLAN que puede soportar de switch:  
**Show vtp status**
- La VLAN 1 es asignada por defecto como vlan administrativa.
- Usar una VLAN dedicada para administración (telnet, ssh).
- Mantener el tráfico entre VLAN separados.
- Cambiar la Vlan nativa a una distinta a la vlan1 por seguridad.
- Asegurarse que la VLAN nativa (es la única que no se etiqueta) es manejada en todos los enlaces.
- Deshabilitar el DTP (Dynamically Trunking Protocol, es un negociante del enlace troncal habilitado por defecto en el switch, que permite acceso según la tabla a continuación).

Switch(config-if)#**switchport nonnegotiate** //desactiva la auto negociación.

# Show interfaces fastethernet0/3 switchport

```
SW2#show interfaces gigabitEthernet 0/2 switchport
Name: Gig0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Inactive)
```

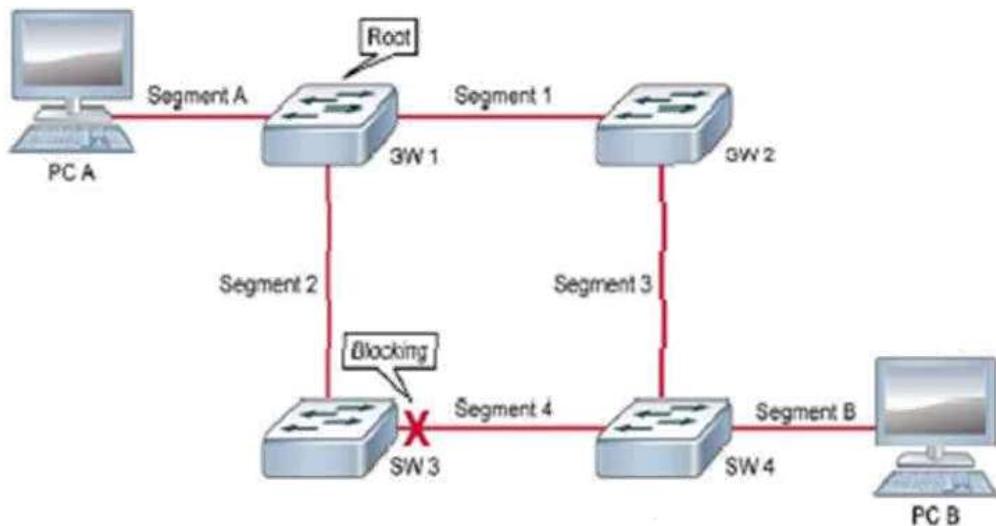
#### DTP maneja la siguiente tabla

PUERTO	Acceso	Auto	desirable	Troncal
<b>Acceso</b>	<b>Acceso</b>	acceso	acceso	X
<b>Auto</b>	Acceso	<b>acceso</b>	troncal	Troncal
<b>Deseable</b>	Acceso	troncal	<b>troncal</b>	troncal
<b>Troncal</b>	X	troncal	troncal	<b>troncal</b>

Nota: el modo de DTP por defecto depende del IOS

### 2.3. Redundancia física en una LAN

Nos permite evitar posibles puntos de falla a través de un respaldo (backup).



Este tipo de configuración ocasiona la trama duplicada, duplicación de direcciones Mac y tormenta de Broadcast y el switch se cae. Para evitar esto se usa el **802.1d STP** (Spanning tree protocol), que permite bloquear un puerto, este puerto puede recibir tráfico pero se encontrara en **modo espera**.

#### 2.4. Enrutamiento entre VLAN

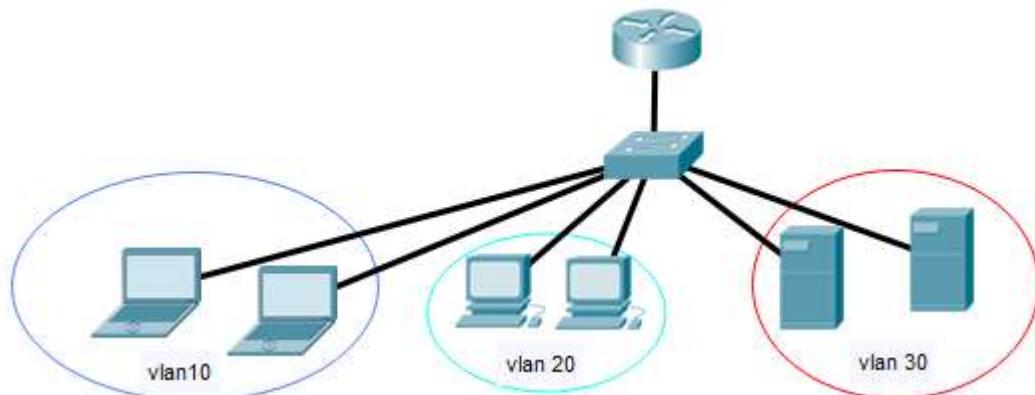
El switch no separa redes, para hacer router Vlan se usa “Router on a stick” existen 3 formas:

##### 2.4.1. Por cada VLAN del switch una interface en el router

No es recomendable si tuviéramos 30 Vlan necesitaríamos 30 puertos en el router.

##### 2.4.2. Router on stick

Permite crear sub interfaces, por cada VLAN se tiene una sub interface, en el router cada interface soporta 4 millones de sub interfaces. Router on stick es un método bastante práctico pero genera cuello de botella.



```
W-2960#show run
```

```
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
```

```
interface GigabitEthernet0/0
```

```
no shutdown
```

```
exit
```

```
interface GigabitEthernet0/0.1
```

```

interface FastEthernet0/6                         encapsulation dot1Q 10
switchport access vlan 20                           ip address 10.0.0.1 255.255.255.0
switchport mode access
interface FastEthernet0/11                         encapsulation dot1Q 20
switchport access vlan 30                           ip address 172.16.0.1 255.255.255.0
switchport mode access
interface GigabitEthernet0/1                        encapsulation dot1Q 30
switchport trunk allowed vlan 1,10,20,30            ip address 192.168.1.1 255.255.255.0
switchport mode trunk
interface GigabitEthernet0/0.10                    encapsulation dot1Q 1 native

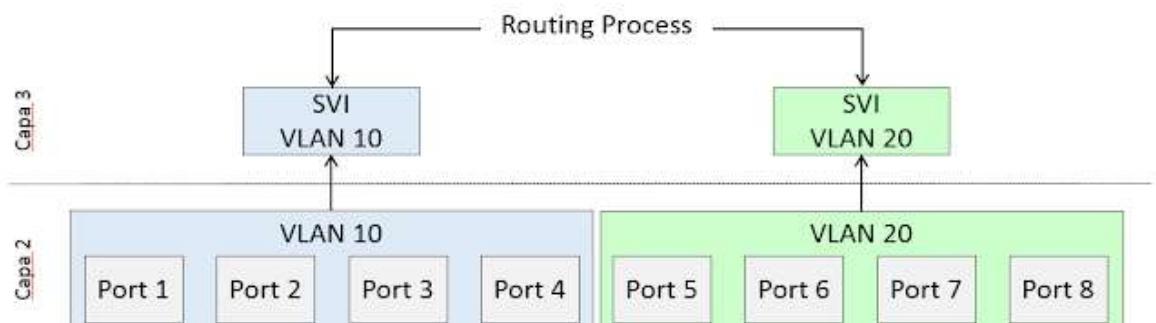
```

#### 2.4.3. SVI (Switch Vlan interface)

Se utiliza switch multicapa (capa 3) conectado a switch de capa dos, donde se forma por cada vlan una interface vlan con su IP. Una SVI es el default gateway de las terminales que forman parte del dominio de broadcast definido por una VLAN, en este método no se crea cuello de botella, es independiente del puerto. Los switches Catalyst (tanto capa 2 como capa 3) presentan una interfaz SVI creada por defecto que es la interfaz VLAN1. Dado que la VLAN 1 es por defecto la VLAN de gestión en switches Catalyst, esta es la interfaz en la que se ingresa la configuración IP necesaria para el acceso por Telnet, SSH, HTTP y HTTPS. El comando `interface vlan [ID]` permite crear una SVI asociada a la VLAN cuyo ID se aplica, e ingresar al modo de configuración de esa interfaz.

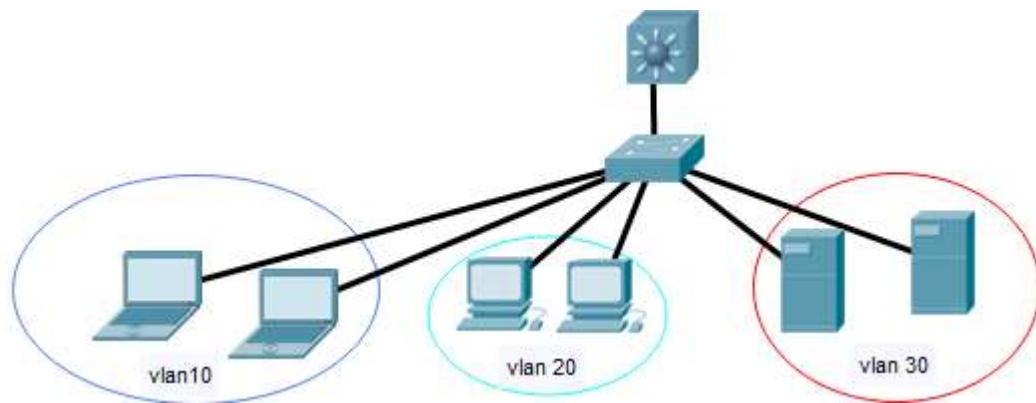
- En los switches de capa 3 la SVI opera como gateway de la LAN, permitiendo enrutar el tráfico hacia y desde vlans sin necesidad de un router.
- Bridging de vlans.
- Protocolos de enrutamiento.

Nota: es necesario habilitar el enrutamiento con un “ip routing”



El comando “`interface vlan “ID”`” permite crear una SVI asociada a la VLAN. Ademas que se necesita habilitar el enrutamiento con el comando “`ip routing`”

Ejemplo:



W-2960#

```

interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access

interface FastEthernet0/6
  switchport access vlan 20
  switchport mode access

interface FastEthernet0/11
  switchport access vlan 30
  switchport mode access

interface GigabitEthernet0/1
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk

```

SW-3560#

```

ip routing

interface GigabitEthernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30

interface Vlan10
  ip address 10.0.0.1 255.255.255.0

interface Vlan20
  ip address 172.16.0.1 255.255.255.0

interface Vlan30
  ip address 192.168.1.1 255.255.255.0

```

## 2.5. IOS CISCO

Sistema operativo de cisco, permite manejar funcionalidades de protocolos y redes, seguridad y control de acceso, alta velocidad de tráfico entre dispositivos, escalabilidad de módulos.

- Modo usuario >
- Modo privilegiado #
- Modo configuración global (**config**)#

Existen dos formas de ayuda sensitiva “argumento y question mark (show ?)”, mensajes de error e historial de comandos que almacena por defecto 10 últimas líneas.

### 2.5.1. Parámetros de seguridad que nos ofrece cisco

Administración de acceso al dispositivo se lo hace a través de telnet (inseguro debido a que sólo hace autenticación), SSH (encripta y hace autenticación), al acceder remotamente evitamos estar físicamente cerca del dispositivo.

- **Protección acceso al modo privilegiado:** Se habilita una contraseña para pasar del modo cliente (USER EXEC MODE) al modo privilegiado (PRIVILEGED EXEC MODE), la misma será en texto plano.

```
Router(config)#enable password CONTRASEÑA
```

Para habilitar una contraseña cifrada se usa

```
Router(config)# enable secret CONTRASEÑA
```

Para verificar la configuración se usa

```
Router#show running-config | include enable
```

- Encriptación de todos las contraseñas que estén en texto plano

```
Router(config)#service password-encryption
```

- Seguridad a través del cable consola

```
Sw(config)# line console 0
```

```
Sw(config-line)# password CONTRASEÑA
```

```
Sw(config-line)# login
```

```
Sw(config-line)# exec-timeout 5 // límite de tiempo de espera de actividad 5 minutos 0 segundos
```

- Seguridad remota telnet vty (virtual terminal)

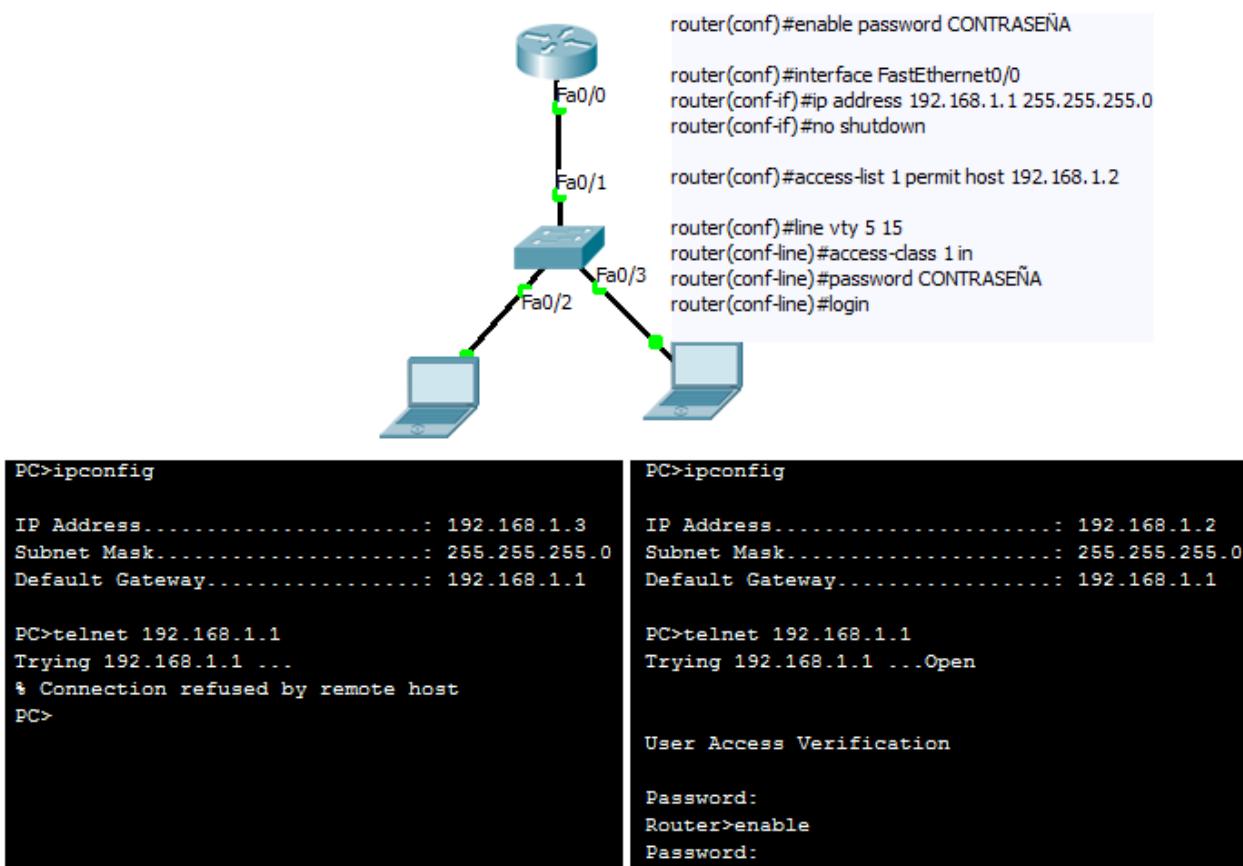
```
Router(config)#line vty 0 15 // 0 a 15 significa número de conexiones en total 16
```

```
Router(config-line)# login
```

```
Router(config-line)# password CONTRASEÑA
```

```
Router(config-line)# exec-timeout 5
```

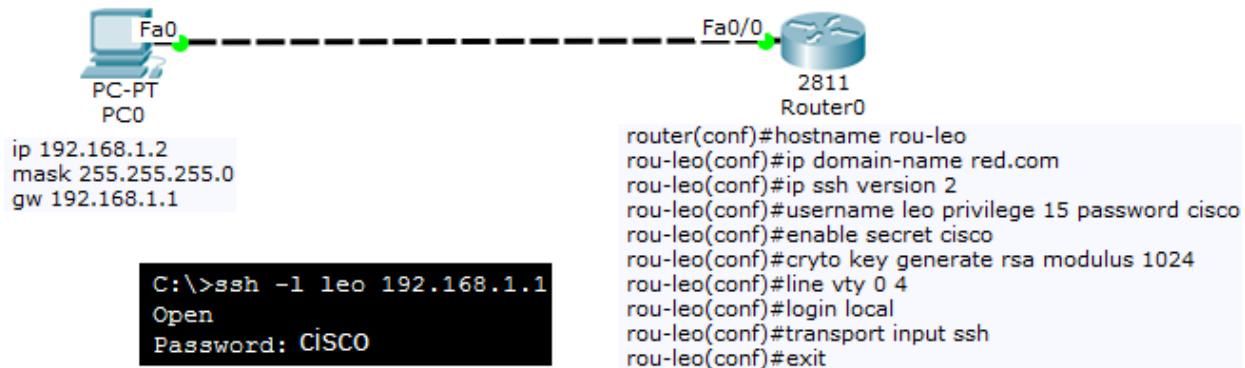
#### 2.5.1.1. Ejemplo de Access list con telnet.



Nota.- al tener acceso mediante telnet a un puerto interface, se tendrá acceso a las demás interfaces del dispositivo.

### 2.5.1.2. Seguridad remota ssh

Es una manera más segura de acceder al dispositivo, SSH encripta el texto introducido posee una autenticación fuerte en (RSA), maneja el puerto 22.



Switch#**show ip ssh** /// verifica si está habilitado ssh

Switch# **show ssh** ///verifica las conexiones el dispositivo

Se puede limitar el acceso remoto mediante listas de acceso como se muestra continuación.

```

#access-list 1 permit 10.1.1.0  0.0.0.255
#access-list 1 deny any log
#line vty 0 15
#access-class 1 in
  
```

**Nota:** MD5 (Message-Digest Algorithm 5) es un **algoritmo** de criptográfico de 128 bits ampliamente usado. Uno de sus usos es el de comprobar que algún archivo no haya sido modificado (integridad).

RSA (Rivest, Shamir y Adleman) Es un algoritmo asimétrico cifrado de **bloques**, que utiliza una clave pública, la cual se distribuye (en forma autenticada), y otra privada, la cual es guardada en secreto por su propietario.

Telnet solo se puede administrar mediante modo cli, mientras SSH se administra mediante cli y GUI (método gráfico)

### 2.5.1.3. Asegurar los puertos

Una forma de asegurar los puertos es inhabilitarlos

The Fa0/1 and Fa0/2 interfaces are disabled in the example.

```
SwitchX(config)# interface range FastEthernet0/1 - 2
SwitchX(config)# switchport access vlan 999
SwitchX(config-if-range)# shutdown
SwitchX # show running-config
<... output omitted ...>
vlan 999
  name Unused
!
interface FastEthernet0/1
  switchport access vlan 999
  shutdown
!
interface FastEthernet0/2
  switchport access vlan 999
  shutdown
<... output omitted ...>
```

#### 2.5.1.4. Port Security

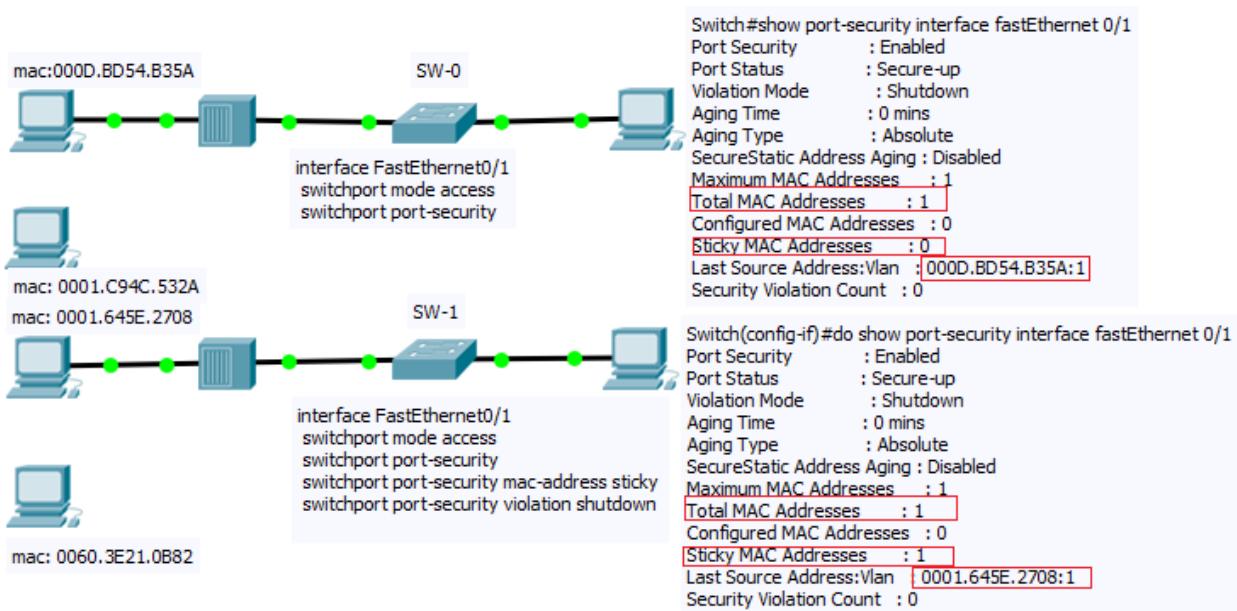
Asegura el dispositivo a través de direcciones MAC, se habilita una MAC por puerto, si se conecta una dirección MAC no autorizada, se puede configurar 3 acciones

- **Shutdown:** inhabilite el puerto (acción por defecto)
- **Restrict:** se envía una notificación SNMP al administrador y el tráfico del puerto se permite únicamente a la MAC especificadas, del resto se descarta. inhabilita el puerto temporalmente
- **Protect:** sólo se permite tráfico de la MAC permitidas en la configuración descartando el tráfico del resto, no se notifica sobre la intrusión, no notifica con alarmas SMTP

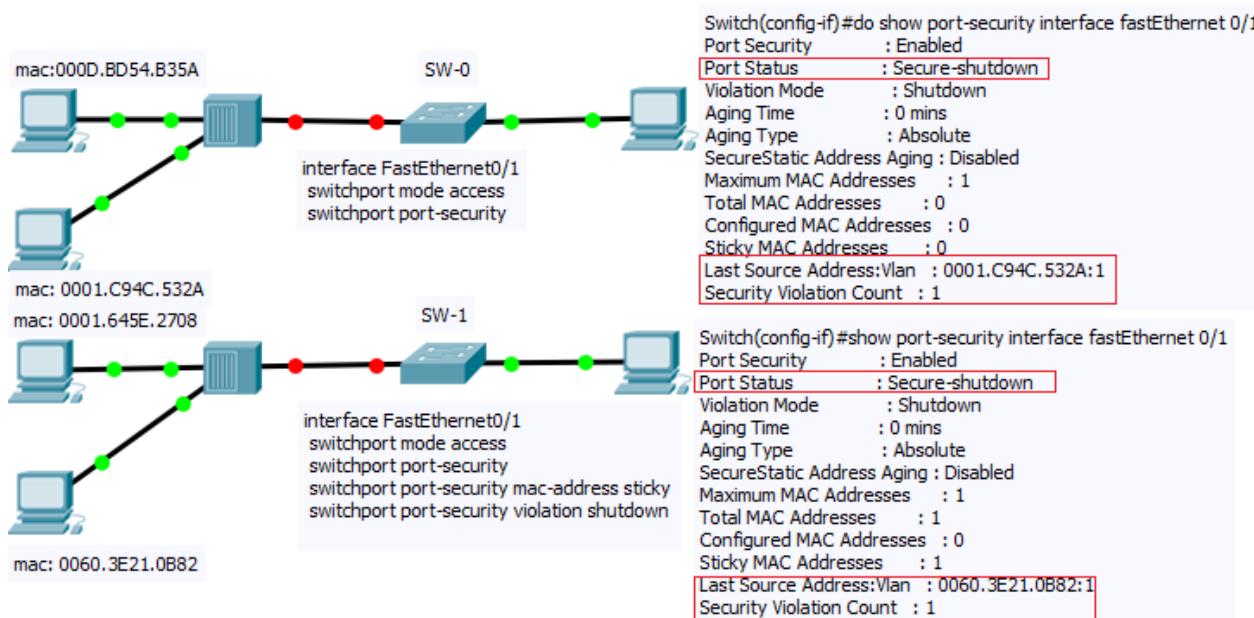
```
SwitchX(config)# interface FastEthernet0/5
SwitchX(config-if)# switchport mode access
SwitchX(config-if)# switchport port-security
SwitchX(config-if)# switchport port-security maximum 1
SwitchX(config-if)# switchport port-security mac-address sticky
SwitchX(config-if)# switchport port-security violation shutdown
```

1. Enable port security.
2. Set the MAC address limit.
3. Specify the allowed MAC addresses (optional).
4. Define the violation action.

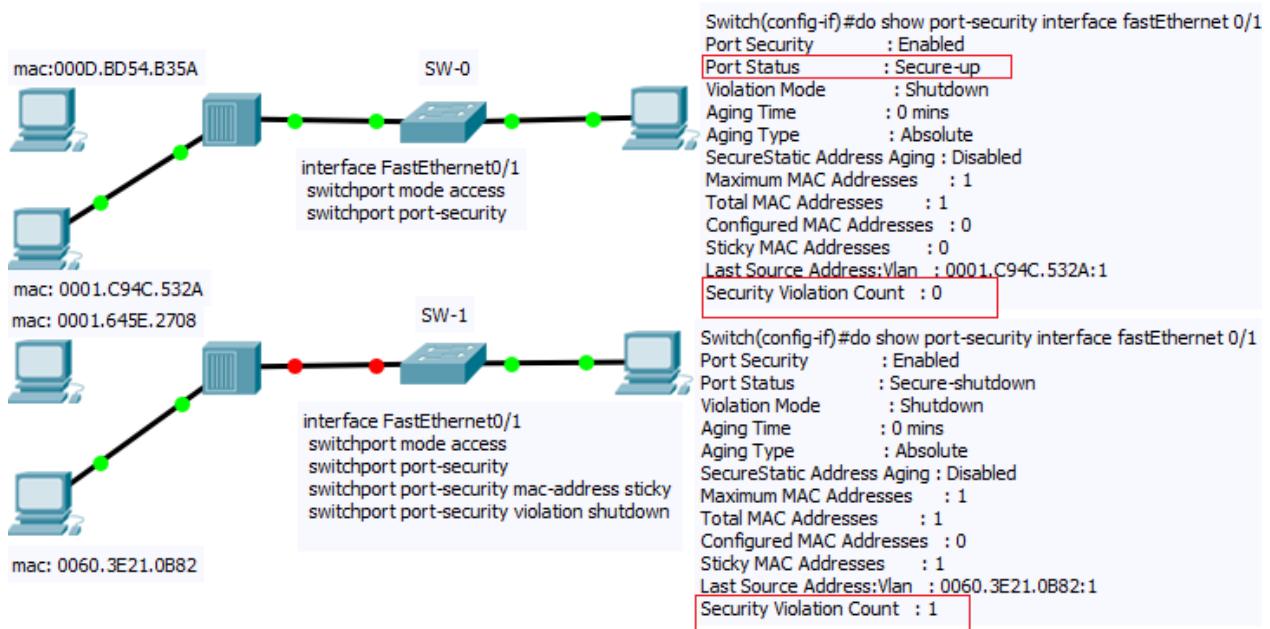
Ejemplo con Sticky y sin Stiky



Añadimos una pc a cada hub para bloquearlo



Eliminamos el primer enlace y volvemos a habilitar el puerto, para habilitar se usa el comando **shutdown** y no **shutdown**



La característica de aprendizaje **sticky** permite agregar direcciones aprendidas dinámicamente a la configuración en ejecución. La primera MAC prevalece y por más que lo volvamos a levantar el puerto este se volverá a bloquear hasta que solo este la Mac de la primera conexión.

**Switch# show port-security interface Fastethernet 0/5**

**Switch# show interface status // el estado de las interfaces**

**Una manera automática de levantar el puerto es.**

**Switch(config)# Errdisable recovery cause pssecure-violation**

**Switch(config)# Errdisable recovery interval 30**

Para mostrar el estado de los puertos se usa no soportado por packet tracer

**#Show control-plane host open-port**

#### 2.5.1.5. Asegurando la consola del equipo

Sin encriptacion ni usuarios

**Router(config)#line console 0**

**Router(config-line)# password contraseña**

**Router(config-line)# login**

Con usuarios

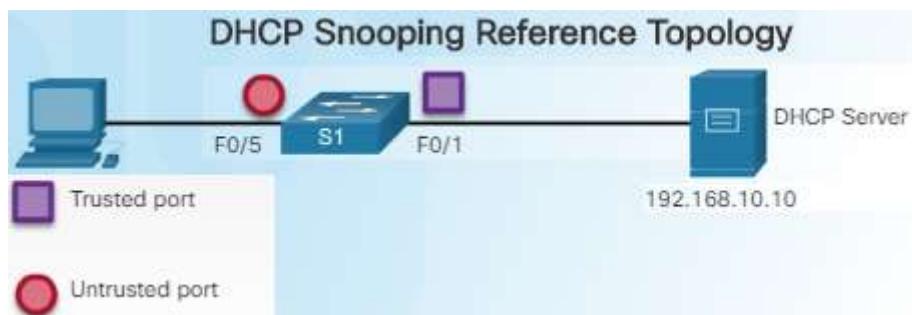
**Router(config)#Username leo password contraseña**

**Router(config)#Line console 0**

**Router(config-line)#Login local**

#### 2.5.1.6. DHCP Snooping

Un ataque DHCP spoofing es un ataque de suplantación dhcp ocurre cuando un servidor DHCP falso se conecta a la red y proporciona configuración de IP falso a clientes legítimos. Los ataques de DHCP spoofing se pueden mitigar usando DHCP snooping (espiar) en puertos de confianza.



Enable DHCP snooping.

Configure DHCP snooping on VLANs 5, 10, 50-52.

Configure la interface f0/1 como cofiable.

Configure las interfaces no confiables f0/5-24 con un snooping rate limit de 6.

```
S1(config)# ip dhcp snooping
```

```
S1(config)# ip dhcp snooping vlan 5, 10, 50-52
```

```
S1(config)# interface f0/1
```

```
S1(config-if)# ip dhcp snooping trust
```

```
S1(config)# interface range f0/5 - 24
```

```
S1(config-if-range)# ip dhcp snooping limit rate 6
```

### 2.5.2. Protocolo NTP (Network Time Protocol)

Sincroniza los relojes de distintos dispositivos, mediante un servidor NTP. También sincroniza los datos del Syslog

```
Router(conf)# ntp server "ip del servidor"
```

```
Router(conf)# ntp update-calendar
```

### 2.5.3. Mensajes de interrupción (syslog)

Nos informan sobre los cambios realizados aparecen en la memoria ram, se recomienda guardarlos.

```
Router(conf)# login "ip del servidor"
```

```
Router(conf)# service timestamps log datatime msec // los mensajes incluirán el tiempo
```

```
Router(conf)# login trap "emergency, alert, critical, error, warning, notification, informational, debugging"
```

// Opcional, especie de filtrado según la gravedad

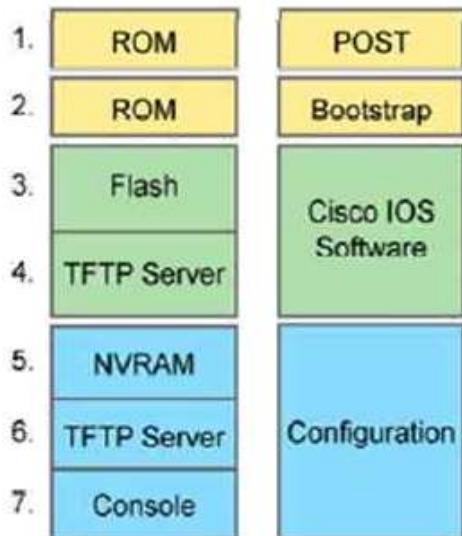
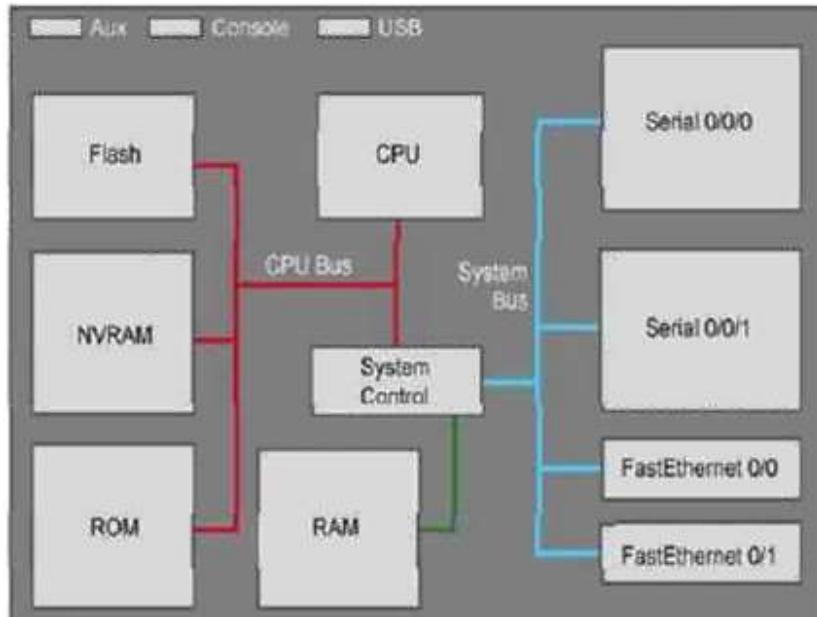
```
#show login // muestras los mensajes logs
```

## 2.6. La administración de dispositivo cisco

Se tiene básicamente 4 tipos de memorias

- **NVRAM (Startup configuration):** almacena las configuraciones a ejecutar o sea guarda las configuraciones.
- **RAM (Running configuration):** corre las configuraciones que se están ejecutando, memoria volátil

- **ROM (Read Only Memory):** contiene sistema de arranque del dispositivo, configuraciones de arranque, tiene un sistema de diagnóstico de hardware **POST** (Power On Self Test), **Bootstrap** código de arranque o código de registro 0x2102 (indica cómo va a iniciar el sistema). Si no arranca el IOS entra en modo **Rommon** (ROM monitor). Se puede ver esta información con “show version”. Si el código de registro es 0x2102 indica que todo está bien, y busca la imagen en la memoria flash (Router)
- **FLASH (IOS, backup configuration):** Almacena la imagen del IOS la descomprime e instala en la RAM (esto ocurre cada vez que se enciende el dispositivo). También sirve para Backup.



#### Como arranca el dispositivo

- 1.-Testeo de hardware (**post**)
- 2.-Indica cómo va a arrancar el dispositivo **bootstrap** 0x2102
- 3.-Busca la imagen IOS en la memoria flash, y lo carga en la memoria RAM
- 4.- si no encuentra la imagen en la memoria flash, el sistema busca en un servidor TFTP, y lo carga en la memoria RAM
- 5.-En la memoria NVRAM se encuentran las configuraciones guardadas y las carga en la memoria RAM,
- 6.- si no encuentra las configuraciones en la memoria flash, el sistema busca en un servidor TFTP.
- 7.- si no encuentra las configuraciones guardadas en la NVRAM o en el servidor TFTP. Entra al modo dialogo

**Nota.-** Si no hay la imagen en la FLASH ni en el TFTP se va al modo rommon (ROM monitor).

**Show running-config:** permite verificar las configuraciones que se están ejecutando

**Show startup-config:** permite verificar las configuraciones guardadas NVRAM

**Show flash:** permite identificar la imagen que está corriendo o archivos de respaldo

**Copy running-config startup-config:** copia las configuraciones que se están ejecutando (RAM) a memoria NVRAM, otra forma es con el comando “**write**”

**Copy startup-config running-config:** carga las configuraciones guardadas (NVRAM) a la memoria RAM para ejecutarse.

**Erase startup-config:** borra las configuraciones guardadas en la NVRAM

**Reload:** va delante de “eraser” recarga las configuraciones

**Show startup-config | (include, begin, exclude, section) hostname:** filtra las configuraciones guardadas, solo mostrará el hostname

**Show clock:** muestra la hora

**Show ip route:** tabla de enrutamiento

**Show ip interface brief:** resumen de las interfaces instaladas

**#setup:** ingresa al modo de configuración dialogo, que es un kernel (software de configuración básica).

### 2.6.1. Configuración de registro

Es un código de 16 bits almacenado en la NVRAM, le indica al router como arrancar el sistema, los últimos cuatro bits son el campo de booteo.

- 0x2102 operación normal
- 0x0 irá directo a roomon
- 0x1 buceo manual de la imagen
- 0x2 o 0xf revisar el IOS
- 0x2142 no pasa por la NVRAM ni por el servidor TFTP, va directo al modo consola (dialogo).

Esta configuración entrará en funcionamiento en el próximo reinicio (usado password recovery).

### 2.6.2. Servidor TFTP (Trivial file transfer Protocol)

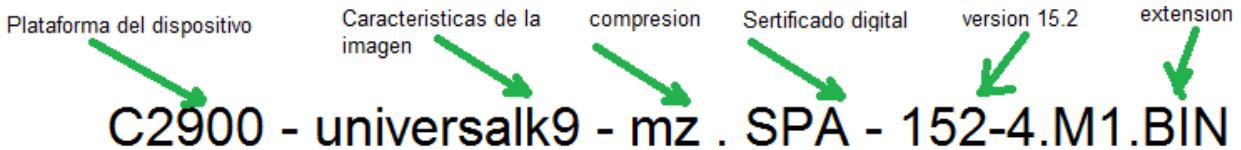
Es un protocolo de transmisión de archivos pequeños de (capa 7). Es muy utilizado para transferir archivos entre máquinas en forma automática a través de UDP (orientado a velocidad) en el puerto 69 de capa 4. Nos permite hacer un *Backup* o respaldo de las configuraciones del sistema.

```
tokyo#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm] y
Writing tokyo.2 !!!!!!! [OK]
```



En un ambiente VoIP, es utilizado para cargar archivos de firmware en, teléfonos y otros dispositivos.

### 2.6.3. Nomenclatura de una imagen IOS.



**Ejemplo:** Realizar un Backup de la memoria flash del router a un servidor tftp

```
Router# show flash0: archivos_backup/configuracion_enero2019.conf
```

```
Router# copy flash0: tftp: /C:/archivos_backup/configuracion_enero2019.conf //le pedirá información de la ip  
del servidor tftp
```

**Ejemplo:** Pasar de servidor a router.

```
Router# copy tftp: flash0: // le pedirá información de la ip del servidor tftp y del archivo
```

**Ejemplo:** Seleccionar la imagen que se desea correr después de reiniciar.

```
Router(config)#boot System flash0: //c2900-universalk9-mz.spa-152-4.m1.bin
```

O

```
Router(config)#boot System bootflash0:c2900-universalk9-mz.spa-152-4.m1.bin
```

Verificar la integridad del archivo

```
Router# verify /md5 flash0:// c2900-universalk9-mz.spa-152-4.m1.bin
```

Copiar de la memoria RAM a la NVRAM

```
Router# copy running-config startup-config
```

Reiniciar

```
Router# reload
```

**Ejemplo:** Si se quiere guardar en la NVRAM y también pasar al servidor TFTP

```
Router# copy tftp running-config
```

**Nota:** la operación se realiza en un formato sin encriptar.

#### 2.6.4. Password recovery (recuperar contraseña)

Modo rommon que es un modo de recuperación de password accediendo a la memoria ROM en el cual se guardan las configuraciones básicas que permite iniciar y mantener el router

**En el router:**

- Conectar el router y la pc mediante cable consola, con el programa putty ingresar al modo ROM monitor
- Apagar el router
- Encender el router en el momento de encender presionar varias veces la tecla "break" o "crt + pausa" o "crt + shit + pausa". Esperar a que aparezca.  
rommon 1 >
- Cambiar la configuración del registro 0x2102 por la de 0x2142 de manera que se salte la configuración a cargar almacenado en la Nvran (donde se encuentra los password) y que no busque en el servidor TFTP. Yendo directo a la configuración de Dialogo.  
rommon 1 > 0x2142

- rommon 1 > reset

Se saltara el registro y se ingresara al router

- Continue with configuration dialog? [yes/no] no
- Router> enable

Copiar de la configuración NVRAM a la RAM

- Router# copy startup-config running-config
- Router# configure terminal

Cambiar contraseña

- Router(config)#enable secret cisco

Se debe volver al registro anterior caso contrario cada vez que se reinicie se saltara directo a la configuración de dialogo

- Router(config)#config-register 0x2102

Guardar las configuraciones

- Router# write

#### En el Switch:

- Conecte una PC el puerto de consola del switch mediante el software putty,
- Desconecte el interruptor cable de alimentación,
- Pulse el botón de modo y al mismo tiempo conecte el cable de alimentación al interruptor.  
Puede soltar el botón de modo de un segundo o dos después de que el LED por encima del puerto se apaga.
- Se iniciara el sistema de archivos flash:  
switch# **flash\_init**
- Cargar archivos de cualquier ayuda (opcional)  
switch# **load\_helper**
- Mostrar el contenido de la memoria Flash:  
Switch# **dir flash:**

```
3 drwx 10176 Mar 01 2001 00:04:34 HTML
6 -rwx 2343 Mar 01 2001 03:18:16 config.text
171 -rwx 1667997 Mar 01 2001 00:02:39 c2950-i6q412-mz.121-14.EA1.bin
7 -rwx 3060 Mar 01 2001 00:14:20 vlan.dat
172 -rwx 100 Mar 01 2001 00:02:54 env_vars
7741440 bytes total (3884509 bytes free)
```

- Cambie el nombre del archivo de configuración para “**config.text.old**” este archivo contiene la contraseña definida.

Switch# **rename flash: config.text flash: config.text.old**

- Reiniciar el sistema

Switch# **boot**

Continue with the configuration dialog? [yes/no]: no

Switch> **enable**

- Cambie el nombre del archivo de configuración a su nombre original:

Switch# **rename flash:config.text.old flash:config.text**

- Copie el archivo de configuración en la memoria:

Switch# **copy flash:config.text system:running-config**

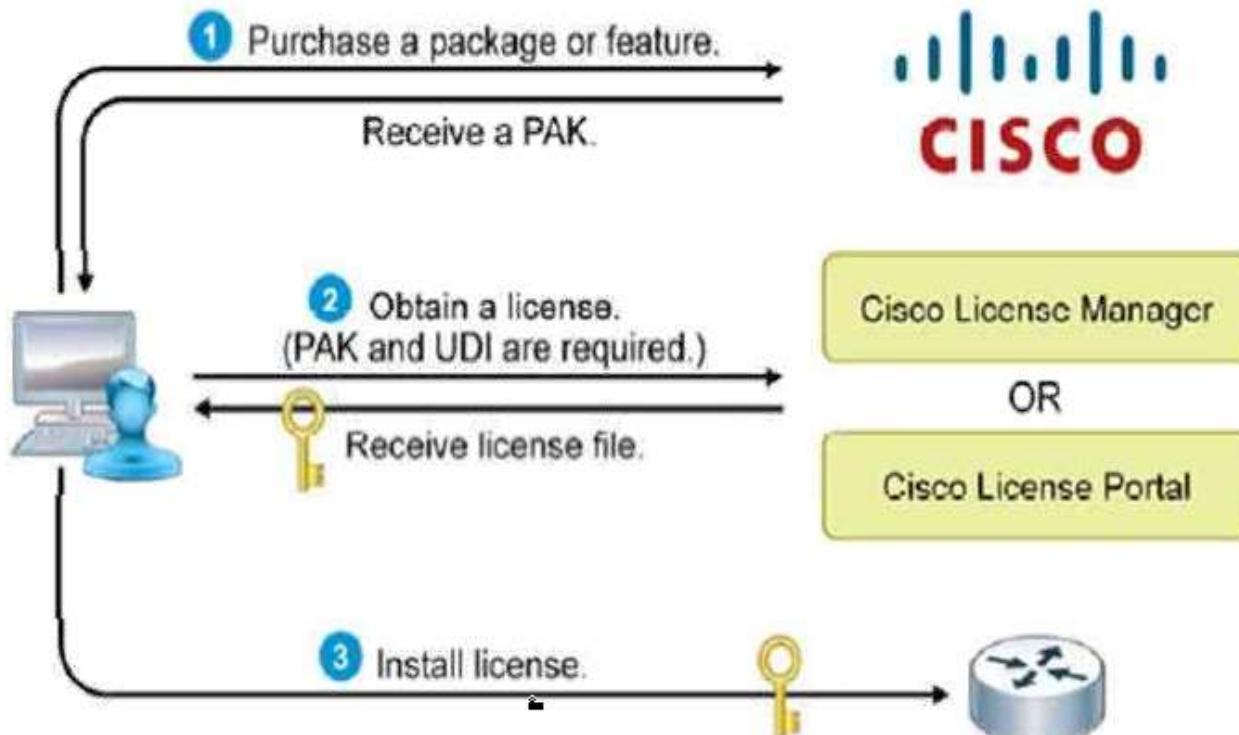
- Cambie la contraseña

Switch (config)# **enable secret password**

Switch# **copy running-config startup-config**

## 2.9. Licencia

## Licensing Overview



```

Router# show license
Index 1 Feature: ipbasek9
    Period left: life time
    License Type: Permanent
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Medium
Index 2 Feature: securityk9
    Period left: Not Activated
    Period Used: 0 minute 0 second
    License Type: EvalRightToUse
    License State: Not in Use, EULA not accepted
    License Count: Non-Counted
    License Priority: None
  
```

Instalar la licencia.

```

R1# license install flash0:uck9-2900-SPE150_k9-FHH12250057.xml
R1# reload
Instalación de licencia de evaluación
  
```

```
R1(config)# license boot module c2900 technology-package uck9
R1# reload
```

Use of this product feature requires an additional license from Cisco, together with an additional payment. You may use this product feature on an evaluation basis, without payment to Cisco, for 60 days. Your use of the product, including during the 60-day evaluation period, is subject to the Cisco End User License Agreement at

Backup de la licencia

```
R1# license save flash:all_licenses.lic
```

Desintalar la licencia

```
Router(config)# license boot module c3900 technology-package uck9 disable
Router(config)# exit
Router# reload

Router# license clear uck9
Router# configure terminal
Router(config)# no license boot module c3900 technology uck9 disable
Router(config)# exit
Router# reload
```

### 3.1. Introducción a IPv6

IPv6 nace debido a que IPv4 no era capaz de soportar la carga de direccionamiento IP. IPv4, dispone de  $2^{32}$  o 4.294.967.296 direcciones, los cuales se están volviendo insuficientes. Por este motivo, la IETF, Internet Engineering Task Force), ha trabajado en una nueva versión del Protocolo de Internet IPv6, con una longitud de 128 bits o 16 bytes, es decir  $2^{128}$  direcciones IP, cada bloque de 4 valores hexadecimales se conoce como Hexlet.

- Ejemplo una forma de representar la dirección es:

2001:**0DB8:010F:0001:0000:0000:0000:0ACD** = 2001:DB8:10F:1::ACD

La máscara ya no se requiere en su lugar se coloca el número de bits de área de red ejemplo: /64

IPv6 tiene representación hexadecimal, la organización encargada de asignar la IP es la IANA, que se subdivide en sus regionales.

AFRINIC

AFRICA

APNIC

ASIA Y AUSTRALIA

ARIN

EEUU

LACNIC

CENTRO Y SUD AMERICA

### 3.1.1. Soluciones planteadas por IPv4

Para extender la vida de IPv4 se crearon

- CIDR (Classless Inter-Domain Routing):
- VLSM (Variable Length Subnet Mask)
- NAT
- DHCP

### 3.1.2. Problemas con IPv4

- NAT, que no permite hacer la comunicación directa de extremo a extremo
- NAT, inhabilita la comunicación debido a la dificultad de su implementación haciéndolo menos seguro.
- Algunas aplicaciones no están relacionadas con NAT, otro motivo para la implantación de IPv6 es la seguridad, IPv6 es más segura.
- Cuando diferentes redes usan la mismo espacio de direcciones privadas ellos tienden a fusionarse produciendo colisiones

### 3.1.3. Beneficios de IPv6

- Mayor espacio de direcciones.
- Cabecera de IPv6 es más simple que de IPv4
- Traducción de IPv6 a IPv4, mecanismos de traducción.
- Seguridad que incluye IPsec de manera nativa (autenticación y encriptación)
- Movilidad, roaming de ISP conservando la misma dirección IP
- Riqueza de transmisión debido a que incluye un conjunto de herramientas de transmisión.
- Autoconfiguración, mediante mensajes multicast de descubrimiento.
- Calidad de servicio QoS y Clase de servicio CoS (priorización de paquetes)

### 3.1.4. Tipos de direccionamiento en IP v6

No existe Broadcast solo *Unicast*, *Multicast*, *Anycast* (direcciónamiento al más cercano).

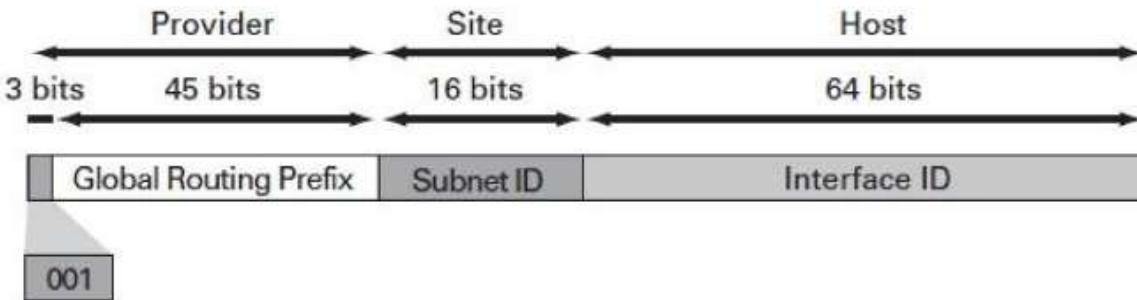
Dirección loopback, (equivale a 127.0.0.1 de IPv4) ::1

#### 3.1.4.1. Global Unicast Address 2000::/3

Las direcciones **Global Unicast** en IPv6 son el **equivalente de las direcciones IP públicas en IPv4**. Estas direcciones IP pueden ser encaminadas a través de la Internet. Los primeros 3 bits de estas direcciones IP están compuestos por los valores 001 Binario, por lo tanto, el prefijo de estas direcciones IP siempre tendrá un valor hexadecimal de 2000 con una máscara /3.

Lo anterior significa que los **primeros 3 bits** dentro de una dirección Global Unicast deben de ser siempre **0010 (en binario)**, y la máscara de 2000/3 significa que sólo podemos hacer variaciones después de los primeros tres bits dentro del primer octeto para establecer el Prefijo Global de Enrutamiento (Global

Routing Prefix).



350523

Para Latinoamérica tenemos a **LACNIC** que nos asigna una porción de red **2001:1200::/23**

Fuente: <http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml>

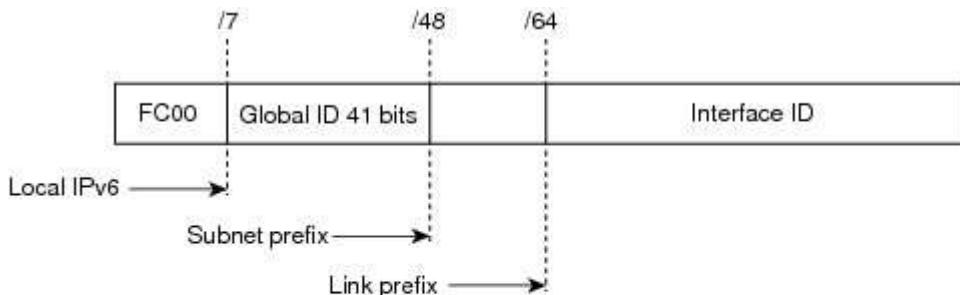
#### *3.1.4.2. Unicast local unicast o Unicast Site-Local FC00 :: /7 FD00::/7*

Son equivalentes a las direcciones IP privadas en IPv4. A diferencias de las direcciones Link-Local, estas pueden ser encaminadas fuera del segmento local, es decir, podemos enviar paquetes entre diferentes segmentos de la red LAN pero no hacia el Internet.

En las direcciones Site-Local, los primeros 7 bits se establecen con los valores 1111 1100 0000 0000, por lo tanto, el prefijo de estas direcciones tendrá un valor en hexadecimal de FC00 :: /7. Los siguientes 57 bits están compuestos por el ID de red. Los últimos 64 bits son el identificador de la interfaz o nodo, y estos se configuran de la misma forma que las direcciones Link-Local, tomando 48 bits de la dirección MAC y luego agregando 16 bits con los valores FFFE.

A continuación tenemos un ejemplo de una dirección Site-Local.

FC00::CE00:3BFF:FE85:0



- Prefix — FC00::/7 prefix to identify local IPv6 unicast addresses.
- Global ID — 41-bit global identifier used to create a globally unique prefix.
- Subnet ID — 16-bit subnet ID is an identifier of a subnet within the site.
- Interface ID — 64-bit ID

23/23/23

Nota: Originalmente, en 1995, el RFC 1884 reservó el bloque FEC0 :: / 10 para las direcciones Site-local, que podrían ser utilizadas dentro de un "sitio" para redes privadas IPv6. Posteriormente, en octubre de 2005, se publicó el RFC 4193 , reservando el bloque de direcciones FC00 :: / 7 para su uso en redes IPv6 privadas y definiendo el término asociado direcciones locales únicast.

### 3.1.4.3. Unicast Link-Local FE80::/10

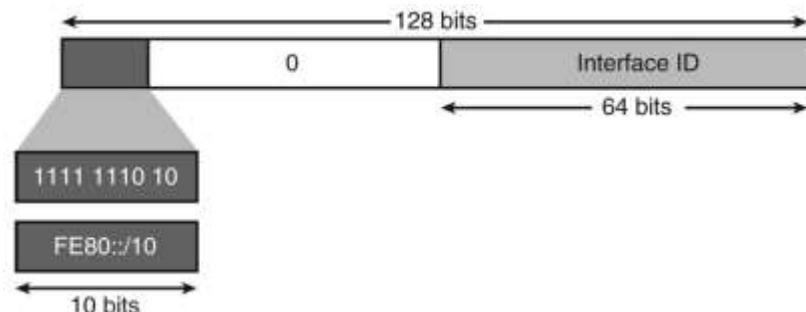
Son el equivalente a las direcciones IP privadas APIPA 169.254.0.1 – 169.254.255.254 /16 en IPv4. Estas son asignadas a una interface de manera automática a partir del momento que activamos el protocolo IPv6 en un nodo. Se utiliza para obtener el **Interface ID** único.

El prefijo de estas direcciones es **FE80::/10**. Estas direcciones **NO pueden ser encaminadas a través de los Routers** fuera del segmento local, de ahí deriva su nombre. El propósito principal es proporcionar direccionamiento IP automático a los nodos en caso que no exista un servidor DHCP.

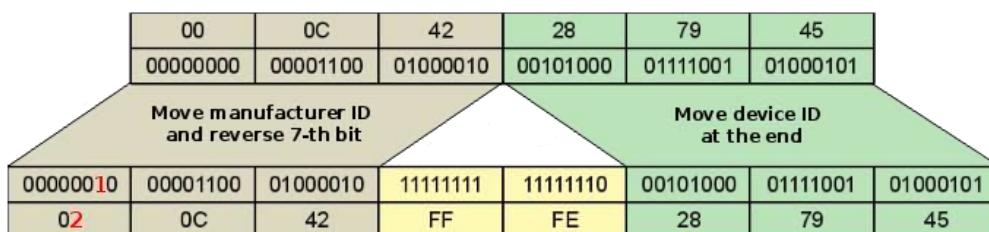
Una dirección IPv6 Link-Local comienza con el prefijo FE80::/10 (los primeros 10 bits), luego los bits del 11 hasta 64 (los siguientes 54 bits) se configuran con valores de ceros (0000). De esta manera se forma la porción de red representada por los primeros 64bits.

FE80:0000:0000:0000/10

La porción de nodo, que son los últimos 64 bits, se forma con el formato EUI-64. El formato EUI-64 toma los 48 bits de la dirección MAC de la tarjeta Ethernet y le coloca 16 bits adicionales predefinidos por el protocolo IPv6 (FFFE). FE80::211:21FF:FE6C:C86B



**48-bit MAC address**



**64-bit EUI-64 address**

- Paso 1. Se tiene la dirección mac de una interface fastethernet 000a.f36a.a547
- Paso 2. La dirección mac se encuentra formada por 48 bits se le suma a la mitad de la dirección mac 16 bits que en formato hexadecimal es FFFE

000a.f3**FF.FE**6a.a547

- Paso 3. Se invierte el bit 7 contando por el octeto de mayor peso posicional

000a= 0000 00**0** 0000 1010

020a= 0000 00**1**0 000 1010

Tendríamos 0**2**0a.f3ff.fe6a.a547

- Paso 4. Hasta aquí tendríamos 64 bits usando EUI-64, ahora completamos con la unicast link local FE80::/10 completando con ceros hasta tener los 64 bits faltantes.

FE80.0000.0000.0000.020a.f3ff.fe6a.a547

#### 3.1.4.4. Dirección IPv6 multicast FF00

En IPv6 el tráfico multicast opera de la misma forma que lo hace en IPv4. Una dirección multicast en IPv6 puede definirse como un **identificador para un grupo de nodos**. Un nodo puede pertenecer a uno o varios grupos multicast. Los nodos pueden escuchar en múltiples direcciones multicast al mismo tiempo. Pueden unirse o dejar el grupo multicast en cualquier momento.

Una dirección **multicast siempre empieza por FF00**. Las direcciones multicast no pueden ser utilizadas como direcciones origen ni como destinos intermedios en una cabecera de routing.

Bits →	8	4	4	112
	1111 1111	Flags	Scope	Grupo Multicast

Flags: 000T, donde:

T = 0: dirección asignada de forma global y permanente (IANA)  
T = 1: dirección asignada de forma local y temporal

Scope (0-F): valor que indica el ámbito o alcance de la emisión. Puede haber 16 ámbitos diferentes. El grupo multicast puede ser cualquiera.

#### 3.1.4.5. Dirección Ipv6 anycast

Una dirección anycast IPv6 es una dirección que es asignada a más de una interface (que normalmente pertenecen a diferentes nodos), con la propiedad que un paquete enviado a una dirección anycast es enrutado a la interface más cercana que tenga dicha dirección de acuerdo con las métricas de los protocolos de enrutamiento.

n bits	128-n bits
Prefijo de Subred	0

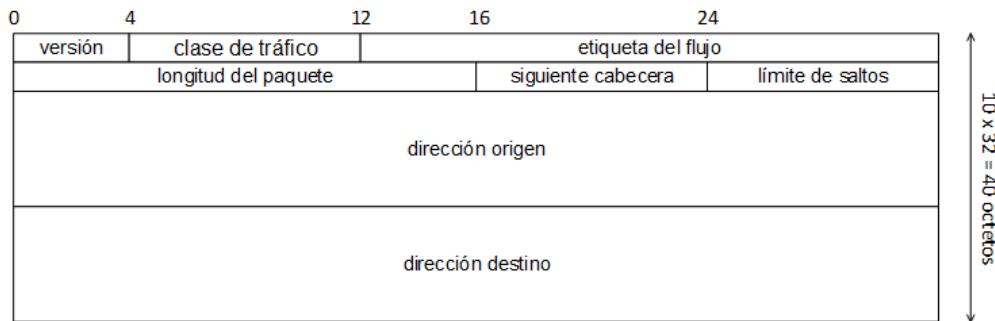
Dirección anycast del router de la subred

## 3.2. Cabecera de IPv6 y IPv4

Los campos que permanecen igual son el “tipo de versión” y la longitud total de 32 bits (0-31), se adiciona la etiqueta de flujo (flow level).

Formato de la Cabecera IP (Versión 4)						
0-3	4-7	8-15	16-18	19-31		
Versión	Tamaño Cabecera	Tipo de Servicio		Longitud Total		
Identificador		Flags	Posición de Fragmento			
Time To Live		Protocolo	Suma de Control de Cabecera			
Dirección IP de Origen						
Dirección IP de Destino						
Opciones			Relleno			

Nota.- Tamaño de la cabecera es de 20 Bytes



Nota.- El tamaño de cabecera de IPv6 es de 40 bytes y carga 32 bits

### 3.3. ICMP v6 (internet control message protocol versión 6)

Verifica conectividad en capa 3 de la misma manera que ICMP v4, tiene una carga de 32 Byte realiza.

ICMP TYPE	DESCRIPTION
1	Destino inaccesible (unreachable)
128	Solicitud (ecco request)
129	Petición (ecco replay)
133	Routes solicitation
134	Router advertisement
135	Netghbor solicitation
136	Netghbor advertisement

En ICMP v6, **ARP tiene su equivalente llamado Neighbor Discovery**. El paquete de ICMPv6 se identifica como 58 en el campo de “next header”

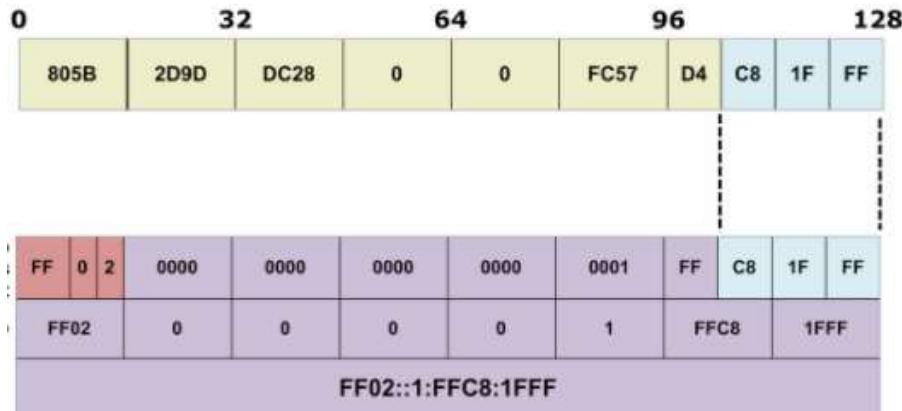
### 3.4. Direcciones Multicast de nodo solicitado

Son esencialmente lo mismo que una dirección IPv4 de broadcast. Para reducir el número de dispositivos que deben procesar tráfico, utilice una dirección multicast de nodo solicitado.

Una dirección multicast de nodo solicitado es una dirección que coincide solo con los últimos 24 bits de la dirección IPv6 unicast global de un dispositivo. Los únicos dispositivos que deben procesar estos paquetes son aquellos que tienen estos mismos 24 bits en la porción menos significativa que se encuentra más hacia la derecha de la ID de interfaz. Una dirección IPv6 multicast de nodo solicitado se crea de forma automática cuando se asigna la dirección unicast global o la dirección unicast link-local. La dirección multicast de nodo solicitado consta de dos partes:

- Prefijo multicast **FF02:0:0:0:0:1:FF00::/104**: los primeros 104 bits de la dirección multicast de todos los nodos solicitados.

- 24 bits menos significativos: los 24 bits finales o que se encuentran más hacia la derecha de la dirección multicast de nodo solicitado. Estos bits se copian de los 24 bits del extremo derecho de la dirección unicast global o unicast link-local del dispositivo.



- FF02::1 ----- All Nodes (link-local)
- FF02::5 ----- OSPFv3 Routers
- FF02::6 ----- OSPFv3 Designated Routers
- FF02::A ----- EIGRPv3 Routers
- FF02::D ----- PIM Routers
- FF05::2 ----- All Routers (site-local)

### 3.5. Multicast mapeo sobre Ethernet

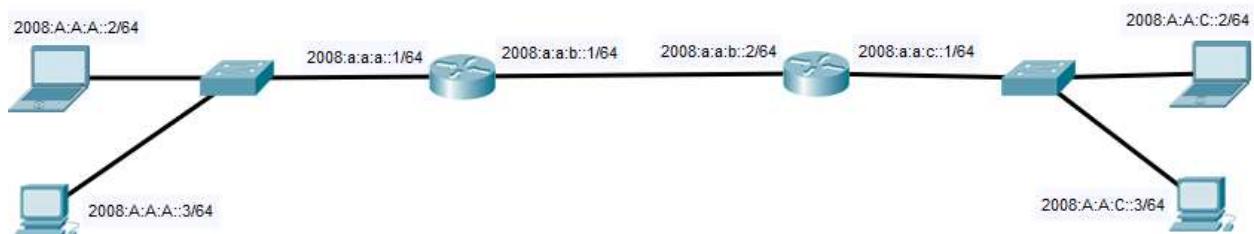
Es una Mac virtual que no está presente en una interface Ethernet, se utiliza los últimos 32 bits del ipv6 nodo solicitado y se le añade 16 bits en hexadecimal 3333

FF02::1:**FFC8:1FFF**

Ethernet Mac: **3333.FFC8.1FFF**

### 3.6. Ejemplo de red en ipv6

- Enrutamiento estático.



#ipv6 unicast-routing

#interface GigabitEthernet0/0

ipv6 address 2008:A:A:A::1/64

#ipv6 unicast-routing

#interface GigabitEthernet0/0

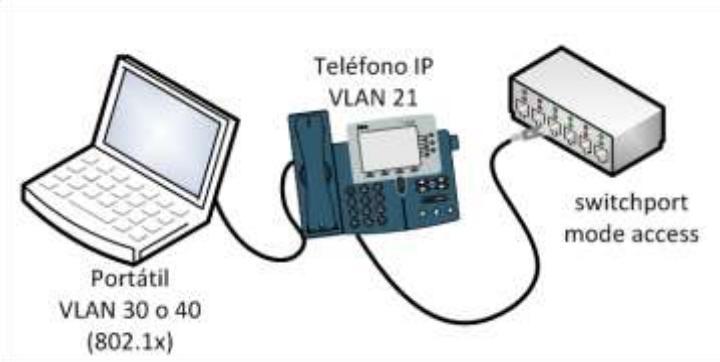
ipv6 address 2008:A:A:C::1/64

```
#interface GigabitEthernet0/1
    ipv6 address 2008:A:A:B::1/64
    #ipv6 route 2008:A:A:C::/64 2008:A:A:B::2
#interface GigabitEthernet0/1
    ipv6 address 2008:A:A:B::2/64
    #ipv6 route 2008:A:A:A::/64 2008:A:A:B::1
```

Comandos de verificación: Show ipv6 interface, Show ipv6 interface brief, ping ipv6 “dirección”

#### 4.1. Vlan DE VOZ

Usado en telefonía, existe en switch de capa 2 un servicio llamado COS (class of service) tiene prioridad sobre los datos. **En una misma interface se puede asignar una Vlan de datos y una Vlan de voz.** Por temas de seguridad se recomienda cambiar la vlan nativa a 99.



La forma para crear Voice Vlans es la siguiente.

```
Sw(conf)#vlan 3
Sw(conf-vlan)# name telefony
SW(conf)#interface fastethernet 0/2
Sw(conf-if)#switchport voice vlan 3
```

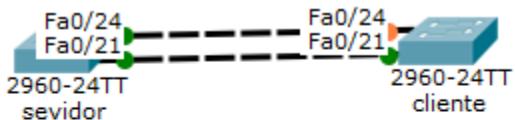
**Nota.-** “Show interface fastethernet 0/2 switchport” nos muestra la información de las Vlans.

#### 4.2. Troncal

Una troncal me permite la comunicación entre Vlans en aplicación de capa 2, utiliza 802.1q que nos permite encapsular en “Tag” la Vlan será de 12 bits (4096 Vlan). En cisco se tiene también la encapsulación ISL (**inter switch link**) adiciona un campo para poder encapsular la trama.

La configuración de la troncal es la siguiente.

```
SW1# configure terminal
SW1# interface FastEthernet0/1
SW1(config if)# switchport mode trunk
SW1(config-if)# switchport trunk native vlan 99
SW1(config-if)# switchport trunk allowed vlan 2,3,99
```



```
troncal para modelo 30 para arriba de capa 3
sw(conf)#interface range fastether 0/21 - 24
sw(conf-if)#switchport trunk encapsulation dot1q
sw(conf-if)#switchport mode trunk
```

#### 4.2.1. Protocolo dinámico troncal (DTP)

Negocia el estado del puerto de manera automática, se recomienda configurar manualmente “switchport mode trunk/acceso” seguido de “switchport nonegotiate” **por defecto los puertos son dynamic desirable.**

```
Switch(config-if)# switchport mode dynamic auto/desirable
```

PUERTO	Dynamic auto	Dinamic desirable	Trunk	Access
Dynamic auto	Acceso (solo pasa la vlan nativa)	troncal	troncal	Acceso (solo pasa la vlan nativa)
Dynamic desirable	troncal	troncal	troncal	Acceso (solo pasa la vlan nativa)
Trunk	troncal	troncal	troncal	No pasa nada de informacion
Access	Acceso (solo pasa la vlan nativa)	Acceso (solo pasa la vlan nativa)	No pasa nada de informacion	Acceso (solo pasa la vlan nativa)

show dtp //verifica si está ejecutándose DTP

```
Switch#show dtp
Global DTP information
  Sending DTP Hello packets every 30 seconds
  Dynamic Trunk timeout is 300 seconds
  3 interfaces using DTP
```

Show interface trunk //muestra el estado de los puertos troncales

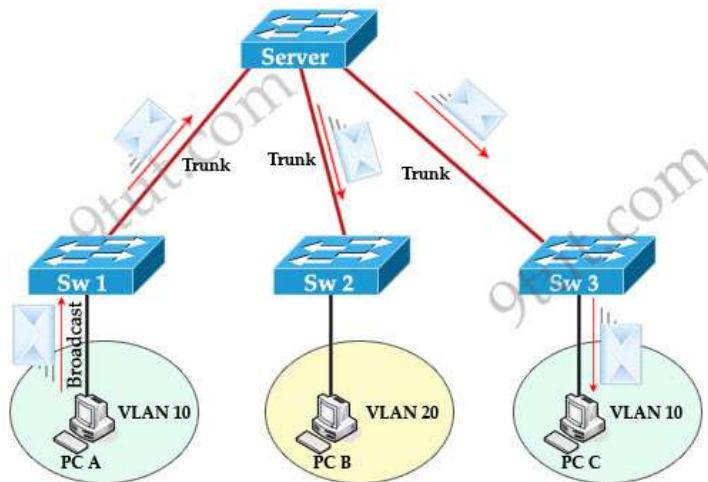
```
Switch#show interfaces trunk
Port      Mode        Encapsulation  Status      Native vlan
Gig0/1    desirable   n-802.1q       trunking   1
```

Show interfaces gigabitethernet 0/1 switchport

```
Switch#show interfaces gigabitEthernet 0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

#### 4.2.2. VTP (Vlan trunking protocol)

Es un protocolo de mensajes de capa 2 usado para configurar y administrar VLANs (sincroniza y propaga VLANs). Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. Intercambia información entre clientes y sincroniza con el último cambio que hubo entre servidor y cliente.



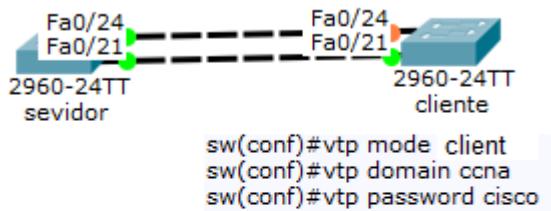
VTP opera en 3 modos distintos:

- **Server:** Es el modo por defecto. Desde él se **pueden crear, eliminar o modificar VLANs**. Transmite su configuración al resto de switches del mismo dominio VTP y sincronizar dicha configuración con la de otros servidores. Debe haber al menos un servidor. Se recomienda autenticación MD5.
- **Client:** En este modo no se pueden crear, eliminar o modificar VLANs, **tan sólo sincronizar** esta información basándose en los mensajes VTP recibidos de servidores en el propio dominio.
- **Transparent:** crea, elimina o modificar VLANs localmente. Su nombre se debe a que **no sincroniza las actualizaciones VTP recibidas**, tan sólo las reenvía a los switches del mismo dominio.

```

show vtp status
show vtp password
show spanning-tree vlan 1
configuracion VTP servidor cliente
sw(conf)#vtp mode server
sw(conf)#vtp domain ccna
sw(conf)#vtp password cisco
sw(conf)#vlan 10
sw(conf-vla)#name diez
sw(conf)#vlan 20
sw(conf-vla)#name veinte
sw(conf)#interface range fastether 0/1 - 4
sw(conf-if)#switchport mode access
sw(conf-if)#switchport access vlan 10
sw(conf-if)#exit
sw(conf)#interface range fastether 0/21 - 24
sw(conf-if)#switchport mode trunk

```



```

sw(conf)#vtp mode client
sw(conf)#vtp domain ccna
sw(conf)#vtp password cisco

```

Nota: solo se copia vlan, por ello se debe asignar puertos manualmente

**Número de revisiones**, el que tiene el mayor número de revisiones remplazara la información de los demás, cada vez que se crea una Vlan el número de revisiones subirá. La configuración transparente solo propaga no sincroniza.

Nota:

- El que tenga número mayor de revisión, copia las Vlans
- Al cambiar de dominio el número de revisión vuelve a 0
- Si el password vtp es distinto el número de revisión es 0
- Vtp envía sus mensajes de actualización cada 5 minutos
- Por defecto el switch viene en modo servidor y sin dominio.
- Para detener VTP se usa “switchport nonegotiate”
- VTPv1 y VTPv2, en un enlace se debe tener versiones iguales.

VTP versión 2 (V2) no es muy diferente de VTP versión 1 (V1). La principal diferencia es que VTP V2 presenta el soporte para **Token Ring VLAN**. Si está utilizando VLAN de Token Ring, necesita habilitar VTP V2. De lo contrario, no hay ninguna razón para usar VTP V2

#### 4.2.2.1. VTP pruning

Mejora el ancho de banda evita caminos innecesarios en las Vlans solo funciona en el modo servidor-cliente.

### 4.3. Redundancia física en una LAN

#### 4.3.1. Spanning Tree Protocol STP IEEE 802.1d

En una red para evitar colisiones y redundancia de información se bloquea puertos (STP) para ello se siguen los siguientes pasos.

**1.- Se designa una raíz o Root Bridge** dependerá de la **Bridge ID [Prioridad (dec 32768 ó hex 8000) + MAC]**.

**2.- Puerto raíz o Root Port**, será el puerto que tenga el **menor costo para llegar a la raíz**

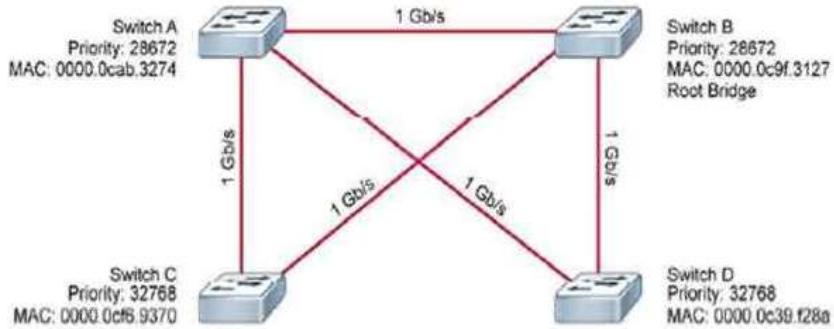
- 10Mbps (costo 100) Ethernet
- 100Mbps (costo 19) Fastethernet
- 1Gbps (costo 4) Gigaethernet
- 10Gbps (costo 2) Tengigaethernet

En el caso que se tenga el mismo costo, se escoge al que tiene el menor Bridge ID (prioridad + MAC) en caso de empate se usa el Port Id que es la “Prioridad de puerto + Identificador de puerto” (ejem. Fa0/1 port id 128.1, fa0/19 port id 128.19).

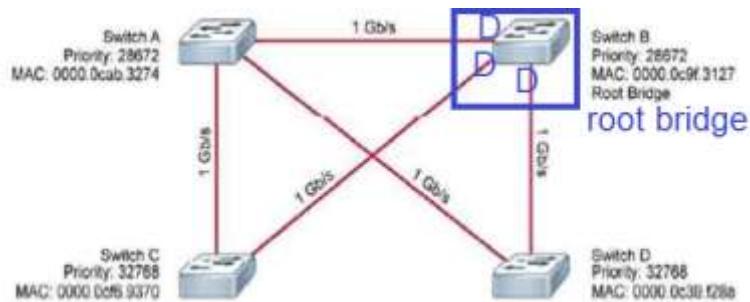
**Nota.-** todo switch debe tener un Root Port, cuando recibe el mejor BPDU de un switch el puerto se convierte en Root Port. El identificador de puerto tiene como valor por defecto el 128

**3.- se designa al el que sobra como Non Designe** que será **bloqueado**

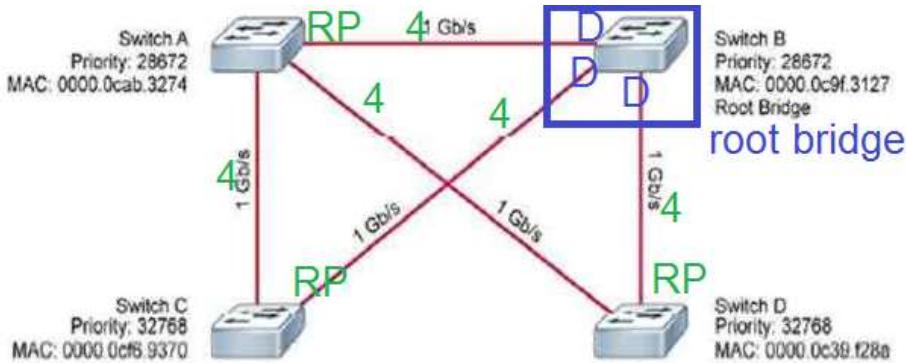
**Ejemplo 1.**



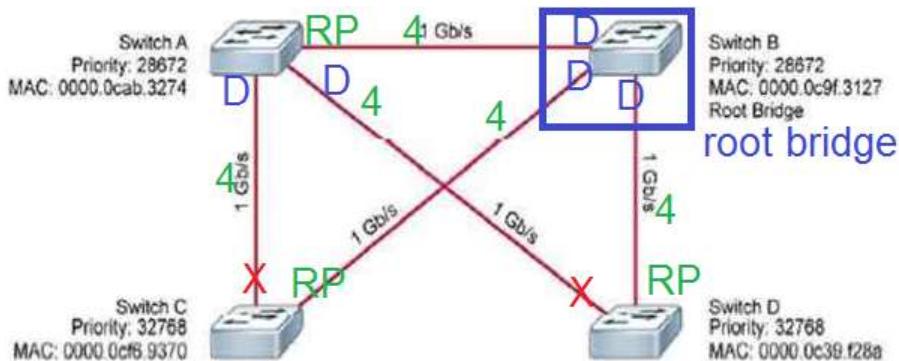
**Paso 1** determinar cuál es el root bridge, comparando primeramente la prioridad y si habría igualdad probar el valor de la dirección MAC. SW-A prioridad 28672, SW-B prioridad 28672, SW-C prioridad 32668, SW-D prioridad 32768, se descarta la prioridad del SW-C y SW-D, el root bridge se determina entre el SW-A y SW-B como se tiene igualdad de la prioridad se verifica la MAC, SW-A 0000.0CAB.3274, SW-B 0000.0C9F.3127, como el menor es el SW-B este es el root bridge por lo tanto sus puertos son designados.



**Paso 2** determinamos el root port, determinando el costo, por ser gigabit su costo es 4.



**Paso 3** tenemos dos enlaces que no están definidos entre SW-A con SW-C y SW-A con SW-D, vemos que el costo para llegar al root bridge es el mismo por lo que comparamos la prioridad, el que tenga menor prioridad será puerto designe y el otro será bloqueado.



### Ejemplo 2. Switch#show spanning-tree vlan 1

Switch#show spanning-tree

VLAN0001		VLAN0001	
Spanning tree enabled protocol ieee		Spanning tree enabled protocol ieee	
Root ID	Priority 32769	Root ID	Priority 32769
	Address 0001.C919.55A0		Address 0001.C919.55A0
<b>Cost</b>	<b>19</b>	This bridge is the root	
Port	1 (FastEthernet0/1)	Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec	Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID	Priority 32769 (priority 32768 sys-id-ext 1)	Bridge ID	Priority 32769 (priority 32768 sys-id-ext 1)
	Address 0002.1632.C511		Address 0001.C919.55A0
Hello Time	2 sec Max Age 20 sec Forward Delay 15 sec	Hello Time	2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time	20	Aging Time	20
Interface	Role Sts Cost Prio.Nbr Type	Interface	Role Sts Cost Prio.Nbr Type
Fa0/1	Root FWD 19 128.1 P2p	Fa0/2	Desg FWD 19 128.2 P2p
Fa0/2	Altn BLK 19 128.2 P2p	Fa0/1	Desg FWD 19 128.1 P2p

**Paso 1:** El root bridge, (prioridad + MAC) la prioridad es la misma 32768+1, se decide por la que tiene menor Mac, por ello el Root bridge es el switch de la derecha y sus puertos serán “Port designed”

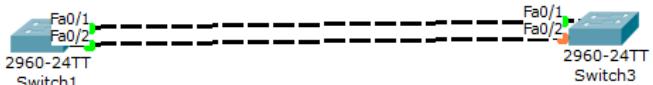
**Paso 2:** Root Port, esto se decide en el switch de la izquierda, como ambos enlaces para llegar al Root Bridge son fastethernet 100Mbps su costo es 19, la prioridad tambien es la misma 32768+1, así que verificamos el **Port ID** (Prioridad de puerto + Identificador de puerto) pero esto no lo vemos en el switch de la izquierda sino en el de la derecha el Switch root bridge. De sus puertos fa0/1 y fa0/2 tendrán el mismo identificador de puerto de valor 128 pero vemos que el identificador de interface es 1 y del otro es 2 así que el “fa0/1 con 128.1” es el menor ósea que el interfaz del switch de la izquierda que se conecta a este puerto es el Root port. El otro interfaz será el Non Designed que es el bloqueado

Switch#show spanning-tree

Interface	Role	Sts	Cost	Prio.Nbr	Type	Interface	Role	Sts	Cost	Prio.Nbr
Fa0/1	Root	FWD	19	128.1	P2p	Fa0/2	Desg	FWD	19	128.2
Fa0/2	Altn	BLK	19	128.2	P2p	Fa0/1	Desg	FWD	19	128.1

#### 4.3.2. Designar el Root Bridge

Se lo puede realizar cambiando la prioridad, los valores deben darse en múltiplos de 4096. Si a la prioridad por defecto (32768) se le resta en 1 unidad (4096) su resultado sería 28672.

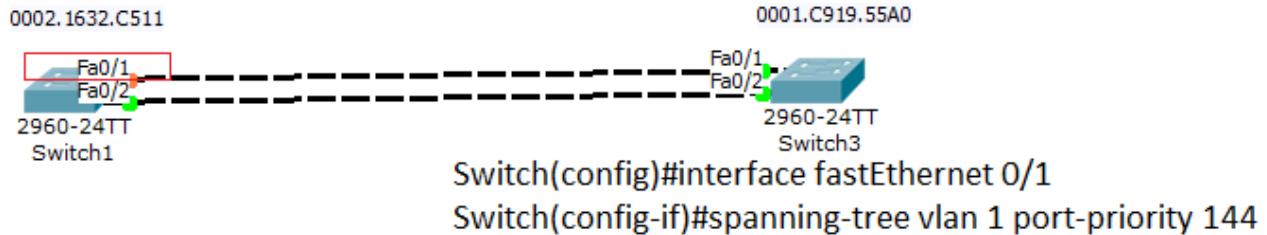
		0002.1632.C511	0001.C919.55A0
		Fa0/1	Fa0/1
<b>Switch(config)#spanning-tree vlan 1 priority 28672</b>			
<b>VLAN0001</b> Spanning tree enabled protocol ieee Root ID Priority 28673 Address 0002.1632.C511 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec		Spanning tree enabled protocol ieee Root ID Priority 28673 Address 0002.1632.C511 Cost 19 Port 1 (FastEthernet0/1) Hello Time 2 sec Max Age 20 sec Forward Delay	
Bridge ID Priority 28673 (priority 28672 sys-id-ext 1) Address 0002.1632.C511 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 20		Bridge ID Priority 32769 (priority 32768 sys-id-ext 1) Address 0001.C919.55A0 Hello Time 2 sec Max Age 20 sec Forward Delay Aging Time 20	
Interface Role Sts Cost Prio.Nbr Type Fa0/1 Desg FWD 19 128.1 P2p Fa0/2 Desg FWD 19 128.2 P2p		Interface Role Sts Cost Prio.Nbr Type Fa0/2 Altn BLK 19 128.2 P2p Fa0/1 Root FWD 19 128.1 P2p	

Otra manera es

(conf)#spanning-tree vlan1 root primary //reduce dos unidades de 4096 se le asigna 24576

(conf)#spanning-tree vlan1 root secondary //reduce una unidad de 4096 se le asigna 28672

También se puede cambiar el identificador de puerto en unidades de 16 hasta 240



#### 4.3.3. Estados de STP

Son 4 estados:

- **(20 s) Blocking:** recibe BPDU pero no los envía, se descartan las tramas, no se actualizan las direcciones MAC.
- **(15 s) Listening:** decide quién es el root bridge
- **(15 s) Learning:** actualiza las direcciones MAC
- **(0 s) Forwarding (envío):** se envía y recibe datos

Nota: las BPDU se mandan cada 2 s

#### 4.3.4. Tipos de Spanning Tree Protocol (STP)

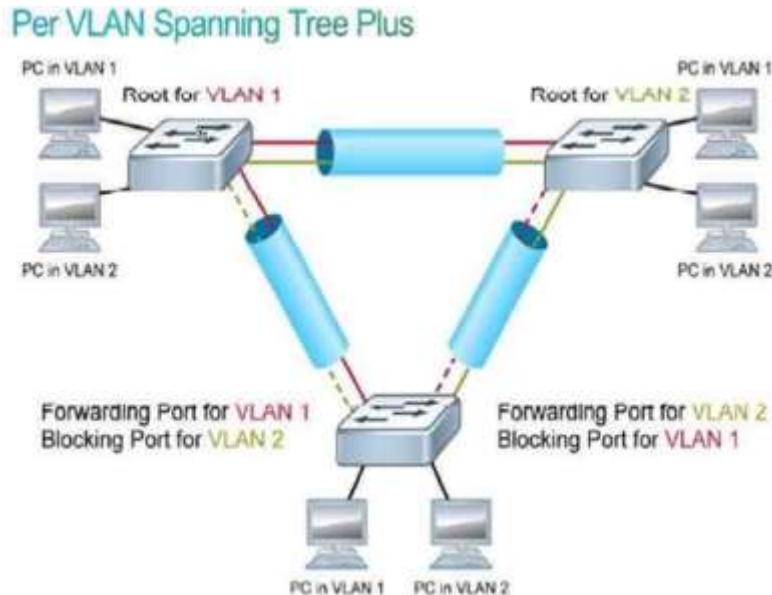
Sus principales características son:

- Evita tormenta de Broadcast
- Evita múltiples copias de la trama
- Evita inestabilidad de direcciones MAC
- En cisco se tiene Pvst +, exclusivo de cisco.

Los distintos tipos de STP son:

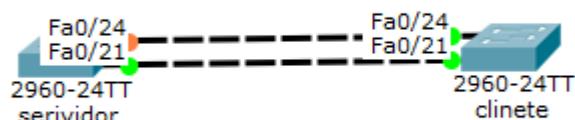
Los distintos tipos de STP son:

- **IEEE 802.1d:** Es el común solo soporta **una instancia para todas las Vlans**.
- **Per-VLAN Spanning Tree plus PVST +:** De Cisco mantiene **una instancia de STP para cada Vlan configurada en la red.**



- **802.1s Multiple Spanning Tree Protocol (MSTP):** Agrupa varias Vlan en una sola instancia SPT
- **802.1w Rapid Spanning Tree Protocol (RSTP):** tiene convergencia pasar de un estado a otro en aproximado de 0 segundos (a los otros les toma alrededor de 50s). RSTP gasta los roles del puerto STP agregando los roles alternativos y de respaldo. RSTP reduce significativamente el tiempo de reconversión de topología después de una falla de enlace. RSTP proporciona una transición más rápida al estado de reenvío en enlaces punto a punto que STP.
- **Rapid PVST+:** basado en PVST+ pero ofrece convergencia rápida entre troncales  
Sw(conf)#spanning-tree mode rapid -pvst

RAPIT PVST+ (convergencia rápida en troncales)  
en servidor y cliente  
sw(conf)#spanning-tree mode rapid -pvst



deconectar la troncal habilitada y verificar  
el tiempo que la troncal inabilitada reacciona

Protocol	Standard	Resources Needed	Convergence	Number of Trees
STP	802.1D	Low	Slow	One
PVST+	Cisco	High	Slow	One for every VLAN
RSTP	802.1w	Medium	Fast	One
Rapid PVST+	Cisco	Very high	Fast	One for every VLAN
MSTP	802.1s Cisco	Medium or high	Fast	One for multiple VLANs

#### 4.3.5. PortFast y la protección BPDU (Bridge Protocol Data Units)

PortFast es una característica de Cisco para los entornos PVST+. Cuando un puerto de switch se configura con PortFast, ese puerto **pasa del estado de blocking al de forwarding de inmediato**, omitiendo los estados de transición de STP 802.1d usuales (los estados de listening y learninc). **Puede utilizar PortFast en los puertos de acceso** para permitir que estos dispositivos se conecten a la red inmediatamente, en lugar de esperar a que STP IEEE 802.1D converja en cada VLAN. Los puertos de acceso son puertos conectados a una única estación de trabajo o a un servidor.

En una configuración de PortFast válida, nunca se deben recibir BPDU, ya que esto indicaría que hay otro puente o switch conectado al puerto, lo que podría causar un bucle de árbol de expansión. Los switches Cisco admiten una característica denominada “**protección BPDU**”. Cuando se habilita, la protección **BPDU coloca al puerto en estado deshabilitado por error al recibir una BPDU**. Esto desactiva el puerto completamente. La característica de protección BPDU proporciona una respuesta segura a la configuración no válida, ya que se debe volver a activar la interfaz de forma manual (entrando a la interface colocar el comando shutdown y no shutdown).



#### Comandos de verificación

Show running-config	Verifica que tipo de spanning tree esta habilitado, por defecto en cisco se tiene “spanning-tree mode <b>pvst</b> ”.
Show spanning-tree interface fastethernet 0/1 portfast	indica si la vlan configurada en el puerto que se encuentra en modo acceso tiene habilitado portfast

VLAN0001	disable
----------	---------

show spanning-tree interface fastEthernet 0/1 detail   include BPDU	Indica el número de bpdu envidas y recibidas BPDU: sent 1, received 146
Show interfaces fastethernet 0/1 switchport	Indica si switchport está habilitado, el estado de Administrative mode, operation mode.
	Name: Fa0/1
	Switchport: Enabled
	Administrative Mode: dynamic auto
	Operational Mode: static Access

Nota: cuando se conecta un switch con una PC solo el switch enviara las BPDU no las recibirá

Cuando se conecta dos switch el root brige enviara BPDU constantemente pero solo recibirá el primer BPDU por ello se desactivara portfast, en el caso del otro switch solo enviara bpdu y recibirá varios de igual manera se desactivará portfast, en el caso que “spanning-tree bpdu guard enable” este habilitado en los puertos estos se desactivaran.

#### 4.3.6. Redundancia en switch con Etherchannel

Agrupa dos o más enlaces en uno solo enlace lógico, soluciona el problema de bloqueo de puertos STP evitando el mismo, esta solución me permite unir varios enlaces y hacer que se comporten como uno solo, esto permite conseguir mayor ancho de banda ejemplo si tengo 8 enlaces Ethernet de 10Mbps con etherchannel se tendría un total de 80 Mbps, otra característica es el balaceo de carga.

En caso de tener más de dos enlaces etherchannel se tiene la posibilidad de hacer STP, es un enlace lógico entre switch, se puede agrupar los enlaces de 2, 4, 8 enlaces, provee redundancia si un enlace se corta los demás seguirán transmitiendo.

Se tiene dos protocolos que nos permiten etherchannel y otro método libre de protocolo llamado ON que es exclusivo de cisco:

##### 4.3.6.1. PagP (Port Aggregation Protocol)

Propiedad de cisco tiene dos modos **Desirable** y **Auto**. Los mensajes se envían cada 30s, las configuraciones deben ser las mismas en ambos extremos, por ello se crea una interfaz llamada interface etherchannel, permite agrupar hasta 8 enlaces.

Switch(config-if)#channel-group 1 mode desirable

- **Desirable:** que habilita incondicionalmente PagP
- **Auto:** habilita PAgP solo si se detecta un dispositivo PagP

##### 4.3.6.2. LACP (Link Aggregation Control Protocol) IEEE-802.3ad

Permite conectar distintos fabricantes, dos modos **Active** y **Passive**. Permite agrupar hasta 16 enlaces.

Switch(config-if)#channel-group 1 mode active

- **Activo:** que habilita incondicionalmente LACP
- **Pasivo:** habilita LACP solo si se detecta un dispositivo LACP

#### 4.3.6.3. On-On

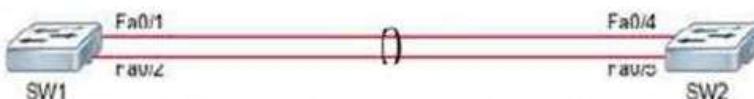
Sin protocolo que habilita solo etherchannel, exclusivo de Cisco

```
Switch(config-if)#channel-group 1 mode on
```

#### 4.3.6.4. Recomendaciones Etherchannel

Los puertos de un extremo u otro deben tener la misma:

- Velocidad y duplexacion, se recomienda forzar el puerto puesto que vienen por defecto en automático o sea que puede cambiar la velocidad de un momento a otro.
- Modo (acceso o troncal)
- Si se tiene una configuración troncal, tiene que contener las mismas Vlans.
- Vlan de acceso en puertos de acceso.- Tiene que contener la misma configuración en ambos extremos tanto en Vlans como en troncal.



Create EtherChannel and configure trunk on SW1.

```
SW1(config)# interface range FastEthernet0/1 - 2
SW1(config-if-range)# channel-group 1 mode active
SW1(config-if-range)# exit
SW1(config)# interface port-channel 1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 1,2,20
```

Create EtherChannel and configure trunk on SW2.

```
SW2(config)# interface range FastEthernet0/4 - 5
SW2(config-if-range)# channel-group 1 mode active
SW2(config-if-range)# exit
SW2(config)# interface port-channel 1
SW2(config-if)# switchport mode trunk
SW2(config-if)# switchport trunk allowed vlan 1,2,20
```

Comandos de verificación

```
#show interfaces port-channel 1
```

```
SW-2#show interfaces port-channel 6
Port-channel6 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 6c50.4d8a.fb01 (bia 6c50.4d8a.fb01)
  MTU 1500 bytes, BW 300000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
```

```
#show etherchannel summary
```

```

SW-1#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
       I - stand-alone   S - suspended
       H - Hot-standby   (LACP only)
       R - Layer3         S - Layer2
       U - in use         f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

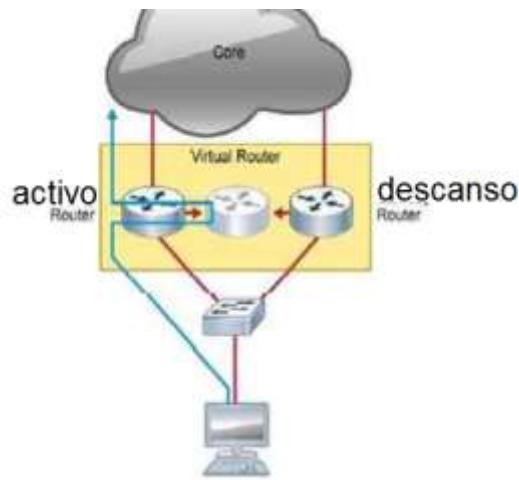
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol      Ports
-----+-----+-----+
1      Po1 (SU)     LACP          Fa0/1 (P)    Fa0/2 (P)    Fa0/3 (P)
                                Fa0/24 (P)

```

#### 4.4. Redundancia a nivel de capa 3 FHRP (First Hop Redundancy Protocol)

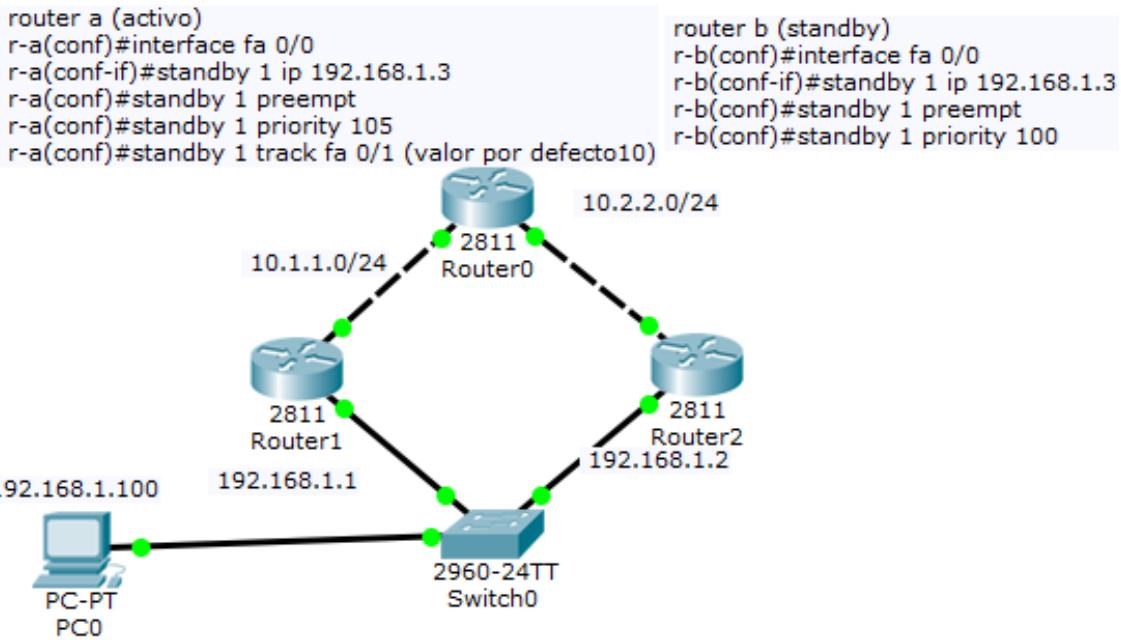
Protocolo de redundancia de primer salto, se refiere a una redundancia de acceso a internet o redundancia de Gateway (tener al menos dos proveedores), de manera de que el servicio no se interrumpa, para lo cual se plantea un router virtual. Usando mínimamente dos routers donde uno estará en modo activo y el otro en modo descanso (Standby) formando entre ambos un router virtual.



Existen 3 tipos de FHRP que son HSRP, VRRP, GLBP

##### 4.4.1. HSRP (Hot Standby Router Protocol)

Define un grupo de routers en activo y en standby, provee una dirección IP virtual y una MAC virtual. El router activo escoge el tráfico de salida a internet, envía “mensajes hello” para saber el estado del enlace. El router standby manda “mensajes hello”, los escucha periódicamente, asume el rol de activo una vez que el otro router no contesta los “mensajes hello”. En ambos routers deben tener la misma dirección IP Virtual configurada.



Nota: comando de verificación “show standby” “show standby brief”

Por **defecto la prioridad es de 100**, el router que tenga la mayor prioridad será el activo, en caso que tengan la misma prioridad será el activo el equipo que mande el primer “hello” por tanto el primero en ser configurado. **Preempt** (preferente), permite que después del cambio de estados activos/standby en caso que se restablezca la red, vuelva a los estados pre-configurados.

Entre sus características principales:

- Dirección multicast 224.0.0.2 UDP puerto 1985
- Prioridad el que tenga más alta es el active router 0-255 por defecto 100
- Hello enviado cada 3s
- En caso de empatar prioridades la IP más grande será el active router
- Cuando el tiempo de espera de los Hello supera los 10s el router standby pasa a ser el active router.
- El protocolo soporta MD5 y texto plano.
- Permite 1 router standby
- Permite balanceo de carga mediante grupos

Al router virtual también se le asigna una dirección MAC virtual la cual es del tipo:

**0000.0c07.acXX** donde las XX son dos números hexadecimales que indican el grupo que se configuro ejemplo “stanby 10 sera la mac 0000.0c07.ac**0a**”.

Los estados por los que atraviesa son:

- Inicial (levanta la interface)
- learn
- Listen (gate way virtual)
- Speak (activa el standby)
- Standby

- Active

#### 4.4.2. VRRP (Virtual Router Redundancy Protocol)

Es un protocolo estándar RFC2338, define el router activo como master, mientras que el resto de routers están en backup state.

- Formato de la MAC **0000.5e00.01xx** donde el número de grupo es XX
- Protocolo por defecto de redundancia.
- Habitual en proveedores de internet.
- **Se puede usar la IP de la interface como la IP de la virtual**
- Dirección multicast 224.0.0.18 puerto 112
- La prioridad desde 1 a 254, por defecto es 100 y la mayor es 254.
- La mayor prioridad define el router master
- Hellos cada 3s
- Preempt habilitado por defecto
- No tiene interface track

```
R1(config)# interface GigE 0/1
R1(config-if)# ip address 192.168.1.2 255.255.255.0
R1(config-if)# vrrp 1 ip 192.168.1.1
R1(config-if)# vrrp 1 priority 110
```

```
R2(config)# interface GigE 0/1
R2(config-if)# ip address 192.168.1.3 255.255.255.0
R2(config-if)# vrrp 1 ip 192.168.1.1
```

Por defecto, los routers VRRP tanto en linux como en Cisco están habilitados con la opción “preempt”, que se asegura de que después de que el master vuelva on-line, después de estar caído, vuelva a ser master, “quitándole” el puesto al master actual.

#### 4.4.3. GLBP (Gateway Load Balancing Protocol)

Es una solución propietaria de Cisco para la redundancia y balanceo de carga en una red IP. GLBP permite la selección automática y recuperación simultánea de los fallas de router de primer salto. GLBP proporciona equilibrio de carga a través de múltiples puertas de enlace (Router) mediante una única dirección IP virtual y múltiples direcciones MAC virtuales. Cada host está configurado con la misma dirección IP virtual, y todos los routers en el grupo de router virtual participan en el envío de paquetes.

GLBP funciona haciendo uso de una sola dirección IP virtual, que se configura como la puerta de enlace predeterminada en los hosts. Los diferentes routers que asumen el papel de reenvío utilizan diferentes direcciones MAC virtuales para la misma dirección IP virtual que se utiliza para enviar paquetes.

A diferencia de HSRP y VRRP, **GLBP no utiliza una única dirección MAC virtual para todo el grupo**. En cambio, el AVG asigna diferentes direcciones MAC virtuales para cada uno de los routers físicos del grupo. Hay dos tipos de routers en una utilización grupo GLBP en redundancia y el equilibrio de carga:

- **Active Virtual Gateway (AVG):** Dentro de un grupo GLBP, un router virtual (puerta de enlace) es elegido como el Active Virtual Gateway (AVG), y es el responsable de la operación del protocolo. Este router AVG tiene el valor de prioridad o la dirección IP más alta en el grupo, responde a todas las solicitudes ARP para direcciones MAC que se envían a la dirección IP del router virtual.
- **Active Virtual Forwarder (AVF):** Un router dentro de un grupo GLBP es elegido como Active Virtual Forwarder (AVF). Este AVF es responsable de reenviar paquetes que son enviados a la

dirección mac asignada por el router AVG. Pueden existir múltiples AVF para cada grupo GLBP. Así, cuando un cliente necesita enviar paquetes al AVG con la dirección IP configurada, solicita la dirección MAC enviando una solicitud ARP (protocolo de resolución de direcciones) en la subred.

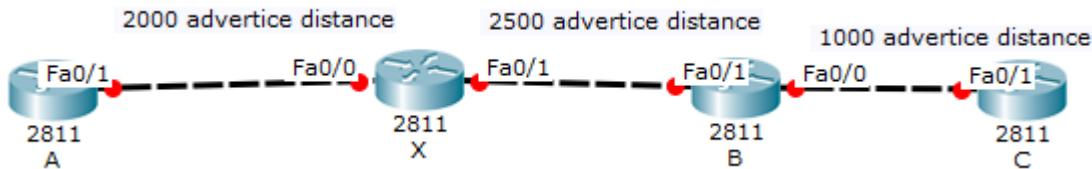
El AVG responderá a estas peticiones ARP con la dirección MAC virtual de cada AVF, basado en un algoritmo de reparto de carga configurado.

### 5.1. Protocolo de enrutamiento dinámico (distancia vector avanzado o híbrido) EIGRP

Protocolo de convergencia rápida (más rápido que OSPF o RIP v2), libre de loops, fácil de configuración, actualizaciones automáticas, permite balanceo de carga (mínimo 4 caminos máximo 16 caminos), de igual o diferente costo, no hay broadcast, summarización manual, soporta VLSM o máscara variable, por defecto permite 100 saltos pero puede aumentarse, soporta múltiples protocolos de red, permite autenticación MD5 (password), EIGRP es exclusivo de Cisco.

EIGRP construye tres tablas:

- **Neighbor Table** (determina cuál es el dispositivo vecino e interface que me conecta a él).
- **Topology Table** (me indica todos los routers que están alrededor).
- **Routing Table** (mejor ruta para llegar a destino).



IP EIGRP Neighbor Table	
Next-Hop Router	Interface
Router A	Ethernet 0
Router B	Ethernet 1

Nos indica que a nuestro router X está conectado al Ethernet 0 el router A y al Ethernet 1 el router B

IP EIGRP Topology Table			
Network	Feasible Distance (EIGRP Metric)	Advertised Distance	EIGRP Neighbor
10.1.1.0/24	2000		Router A (E0)
10.1.1.0/24	2500		Router B (E1)

Obtenemos el **Advertised Distance** el valor con la conexión directa con el vecino, y el **Feasible distance** (metrica) la suma de los Advertised distance para llegar al router, ejemplo el feasible distance para llegar al router C es 3500

The IP Routing Table			
Network	Metric (Feasible Distance)	Outbound Interface	Next Hop (EIGRP Neighbor)
10.1.1.0/24	2000	Ethernet 0	Router A

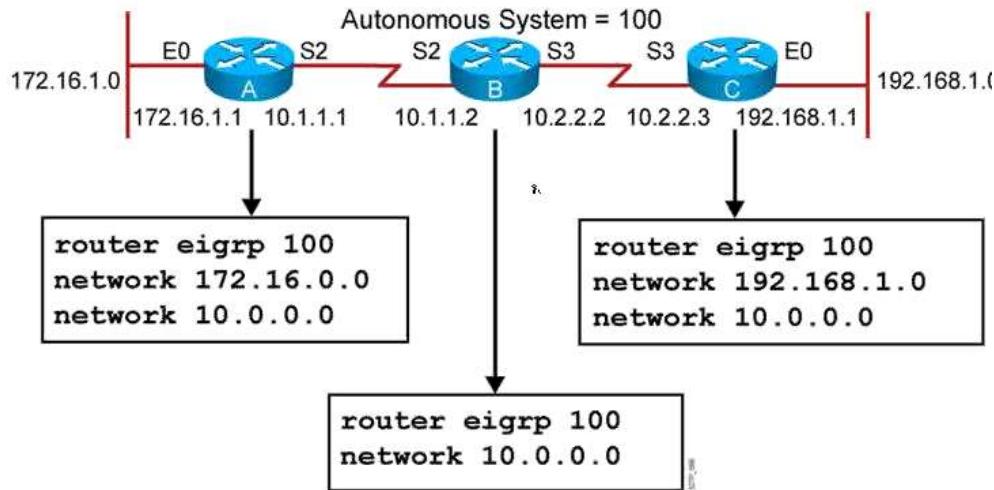
Menor feasible distance es **SUCESOR** o mejor ruta.

Y la ruta alternativa feasible sucesor

Calculo de EIGRP en la tabla de topología, obtiene un valor entre el dispositivo vecino y la interfaz que le permite llegar a él *Advertised distance* y un valor que es la sumatoria de los *advertised distance*

que llamamos *Fesible distance (metrica)* el que tenga la menor métrica será la ruta. A la mejor ruta se la llama successor y rutas alternativas se les llama feasible successor.

```
RouterX(config)# router eigrp autonomous-system
RouterX(config-router)# network network-number
```

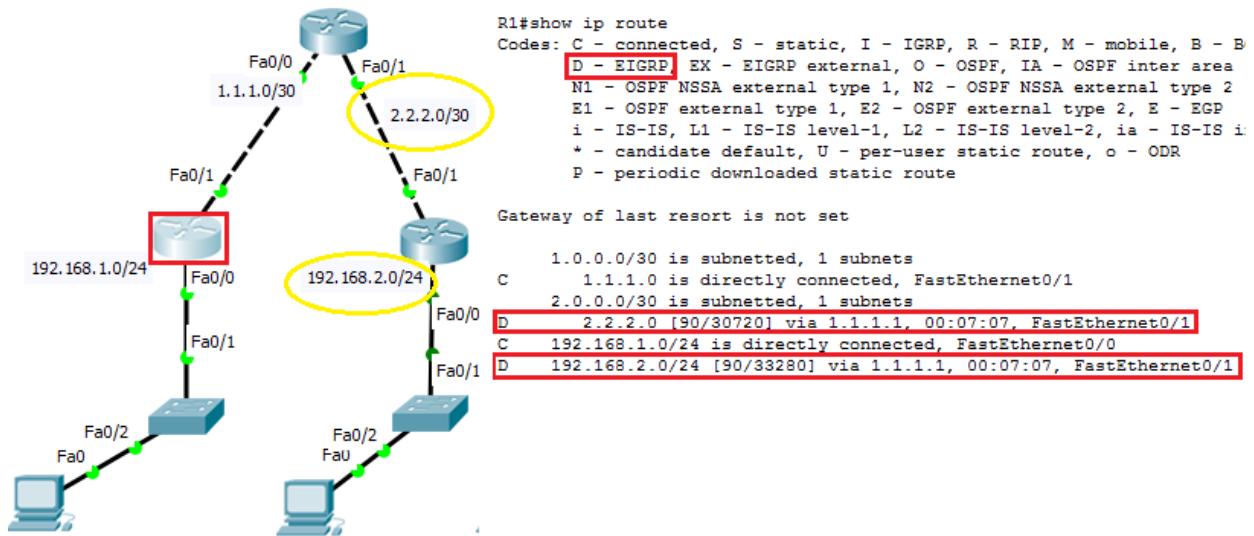


El sistema autónomo “router# router eigrp autonomous-system” es un valor que va de 1 a 65535 (16 bits) este valor debe ser el mismo en todos los routers para que exista conexión automática. Se deben colocar las redes directamente conectadas al router también se puede añadir la wildcard.

Por defecto EIGRP trabaja con class full (sumarización no reconoce otras máscaras que no sean 8/16/24, no sub redes, se debe usar una wildcard “network 10.0.0.0 0.0.0.255”), con la opción “no-auto sumary”, nos permite trabajar con class less (sub redes, máscara variable).

EIGRP soporta class less

*Nota:* “Show ip route eigrp” nos muestra la tabla de enrutamiento de solo eigrp



"show ip protocols" nos muestra parámetros de configuración se han introducidos al router

```
Router# show ip protocols

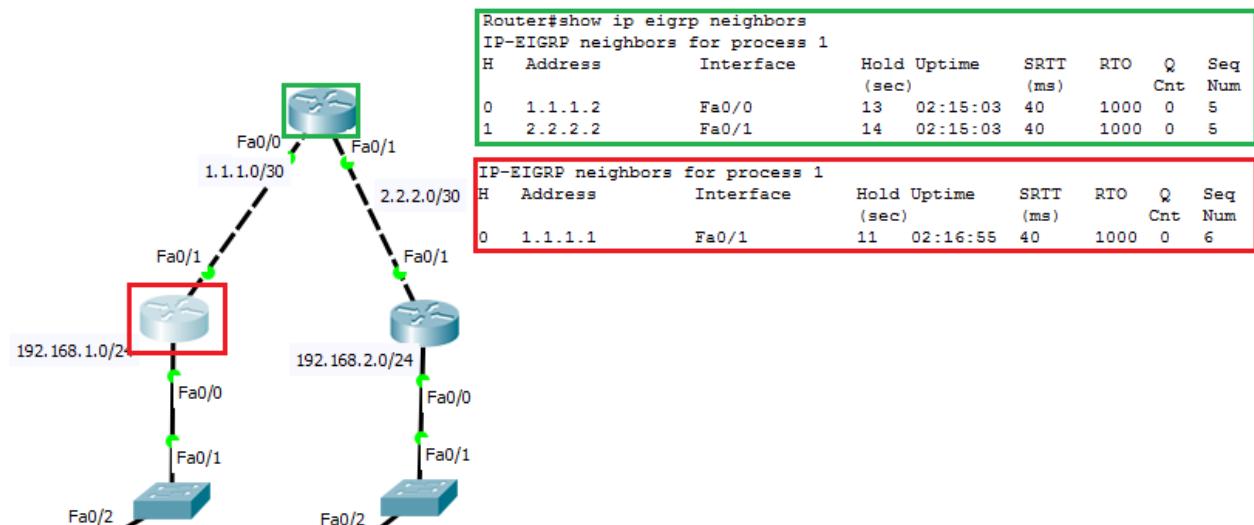
Routing Protocol is "eigrp 1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 1
  Automatic network summarization is not in effect
  Maximum path: 4
Routing for Networks:
  5.5.5.0/30
  1.1.1.0/30
  2.2.2.0/30
Routing Information Sources:
  Gateway          Distance      Last Update
  1.1.1.2           90              0
  2.2.2.2           90              0
Distance: internal 90 external 170
```

"show ip eigrp interfaces" nos muestra la relación de las interfaces conectadas con dispositivos vecinos que tengan configurado eigrp.

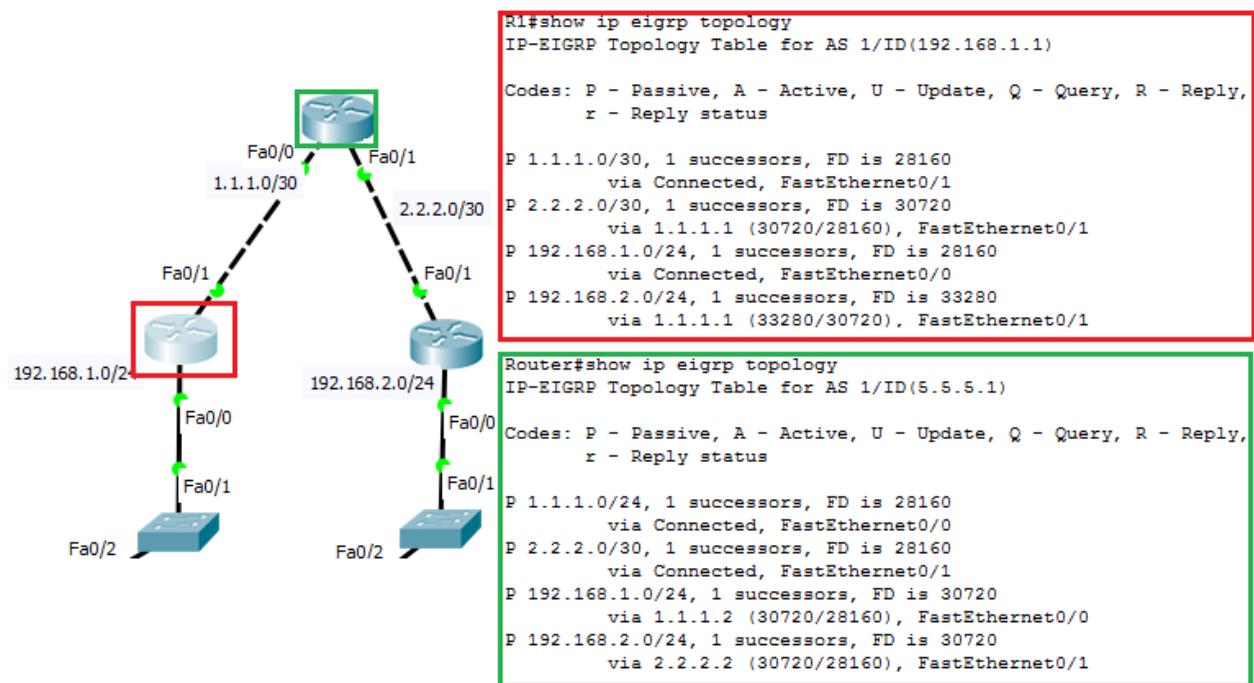
```
IP-EIGRP interfaces for process 1
```

Interface	Peers	Xmit Queue	Mean	Pacing Time	Multicast	Pending Routes
		Un/Reliable	SRTT	Un/Reliable	Flow Timer	
Fa0/0	1	0/0	1236	0/10	0	0
Fa0/1	1	0/0	1236	0/10	0	0

"Show ip eigrp neighbors" información de las redes vecinas y a que interfaz local está conectada.



"show ip eigrp topology" muestra la tabla de topología y Router ID del EIGRP process (IP más alta de la loopback o de la interfaz)

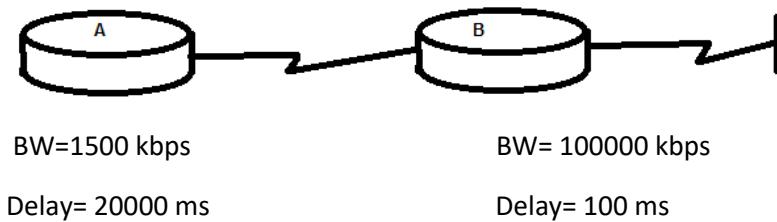


Un comando importante es “show ip eigrp traffic” nos muestra la relación de los mensajes de actualizaciones, solo cuando hay cambios en la ruta (rip cada 30 s). “hello” un mensaje pequeño cada 10s. La métrica es el elemento que utiliza un protocolo de enrutamiento para estimar el mejor camino hacia una red de destino.

$$\text{Metrica} = (BW_{\minimo} + \text{retardo}) * 256$$

$$BW = \frac{10^7}{BW_{\min}[kbps]} \quad ; \quad \text{retardo} = \frac{\sum \text{retardo [mili seg]}}{10}$$

Ejemplo:



Reemplazando en la ecuación:

$$\text{Metrica} = \left( \frac{10^7}{1500} + \frac{(20000 + 100)}{10} \right) * 256 = 2221056$$

Cada router lleva dos métricas:

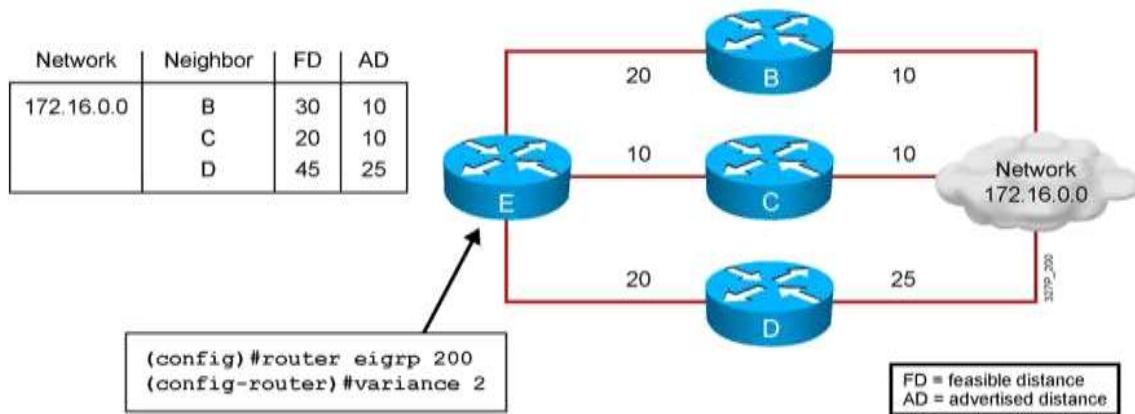
- Advertised distance, estimada por el router vecino
- Feasible distance, estimada por el router local

La métrica de **eigrp usa por defecto el retardo (delay) y el ancho de banda (BW)** pero puede también utilizar la confiabilidad (reliability) y carga (load).

### 5.1.1. Balanceo de carga en EIGRP

EIGRP para hacer un balanceo de carga de diferente costo se usa “variance” que es un numero multiplicador que iguala al de menor costo con el de mayor costo, esto es exclusivo de EIGRP.

Router (configure-router)# variance (valor por defecto 1)



Igualamos las rutas bajas con las altas multiplicando en este caso 2, feasible distance (métricas) seria:

- router E pasando por router B=30 x 2 = 60
- router E pasando por router C=20 x 2 = 40
- router E pasando por router D=45 x 2 = 90

El menor en este caso es pasando por router C seria nuestro sucesor, pero necesitamos hacer balanceo de carga por ello lo aproximamos con su mayor, de acuerdo a esto el balanceo lo haría por el router B y C debido que D se aleja demasiado.

EIGRP por defecto admite 100 saltos se puede configurar hasta 250, OSPF no tiene límites.

**Nota:** para realizar balanceo de carga con enlaces de igual costo se debe escoger el número de caminos máximo 16

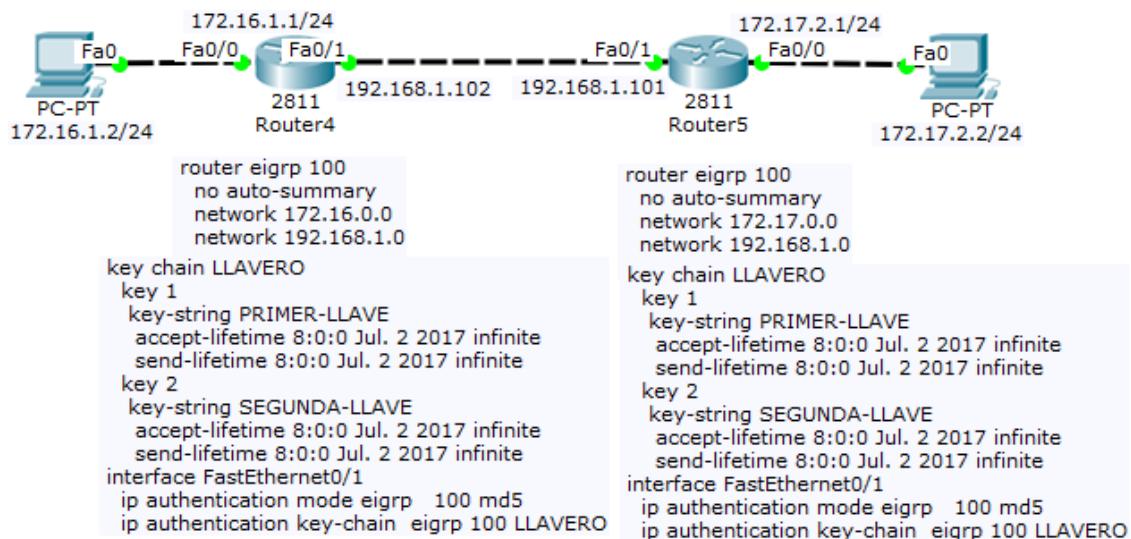
R(config)# router eigrp 100

R(config-router)# maximun-paths "1-16"

### 5.1.2. Autenticación en EIGRP

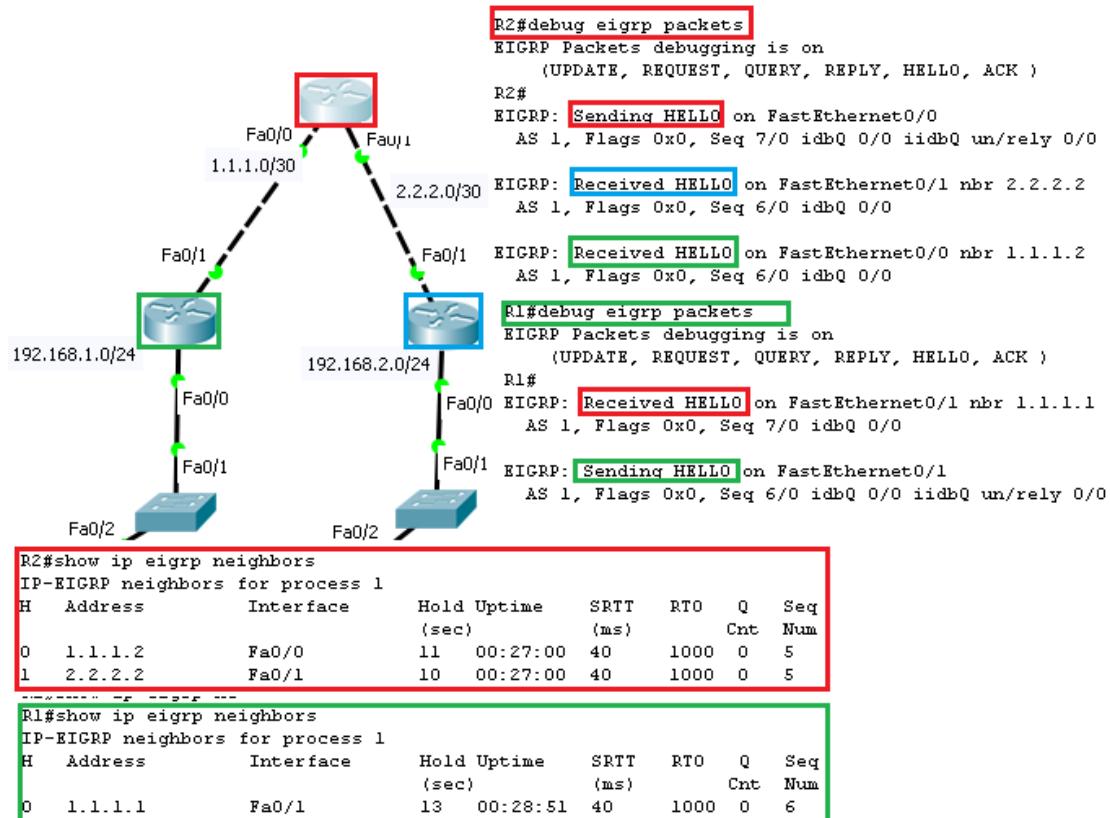
EIGRP admite autenticación MD5 (ios v12.4, v15 usa sha v2 256bits), solo los que tengan credenciales se conecten a la red, no encripta contenido. La autenticación es entre interfaces, deben tener mismo password se sigue los siguientes pasos para la cadena de llaves (llavero).

- Se crea el llavero keychain, grupo de llaves
- Por cada ID de cerradura una llave
- Se identifica la llave
- Se especifica la duración de la llave (obcional)
- Se especifica donde se colocara la llave.



### 5.1.3. Puerto pasivo en EIGRP

El comando permite la supresión de las actualizaciones de enrutamiento en algunas interfaces, mientras que permite intercambiar las actualizaciones normalmente a través de otras interfaces. Con la mayoría de los protocolos de enrutamiento, el comando de interfaz pasiva restringe solo los anuncios salientes, suprime el intercambio de paquetes de HELLO entre dos enrutadores, lo que resulta en la pérdida de su relación de vecinos. Esto evita que se publiquen las actualizaciones de enrutamiento, pero no suprime las actualizaciones de enrutamiento entrantes. Él envió de Hellos en EIGRP es cada 10s, con el comando “debug eigrp packets” podemos ver estos mensajes que intercambian, envio y recepción. **Solo se debe emplear este comando en interfaces que no van a otros routers debido a que no se podrá conocer a la ruta a los vecinos.** El ejemplo de abajo es sin el comando de “passive-interface fastethernet 0/0”



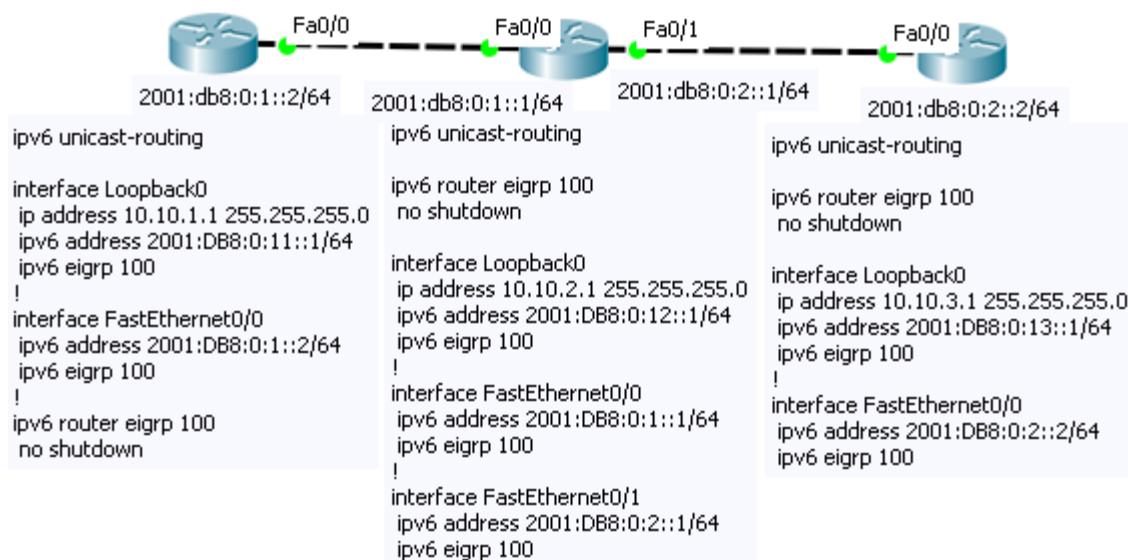
Empleamos el comando en la interface que conecta la LAN

```
R1(config)# router eigrp 1
R1(config-if)# passive-interface default
R1(config-if)# no passive-interface fastethernet 0/1
```

#### 5.1.4. EIGRP en IPv6

- Para verificar la adyacencia de una ruta en ipv6 se usa “show ipv6 eigrp neighbor”
- Se debe verificar que tengan el mismo sistema autónomo
- Las direcciones multicast en ipv6 son FF02::A

A diferencia de ipv4 en eigrp ipv6 no se requiere declarar sentencias de red, lo que se hace es habilitar en cada interface “ipv6 eigrp AS”. Por defecto el proceso de enrutamiento EIGRP en ipv6 se encuentra caído “shutdown”. El ID de router en eigrp ipv6 debe ser una ipv4 que se toma de una interface loopback



#### 6.1. Protocolo de Enrutamiento OSPF (open short phat firts)

Protocolo link-state, estandarizado soporta varias marcas. Es classless o sea que soporta VLSM, usa como métrica el costo, Viene como reemplazo de RIPv2. Permite levantar la relación de vecindad mediante los paquetes HELLO, que es enviado cada 10 s en redes punto a punto y 30 s en redes multi acceso (Non Broadcast Multi Access) NBMA. (no hay broadcast en ospf)

El **Dead interval** es el intervalo en segundos para informar que el vecino esta caido su valor es de 40s para punto a punto y 120s para redes multi acceso. La base de datos se actualiza cada 30 min o cuando hay cambios en la red.

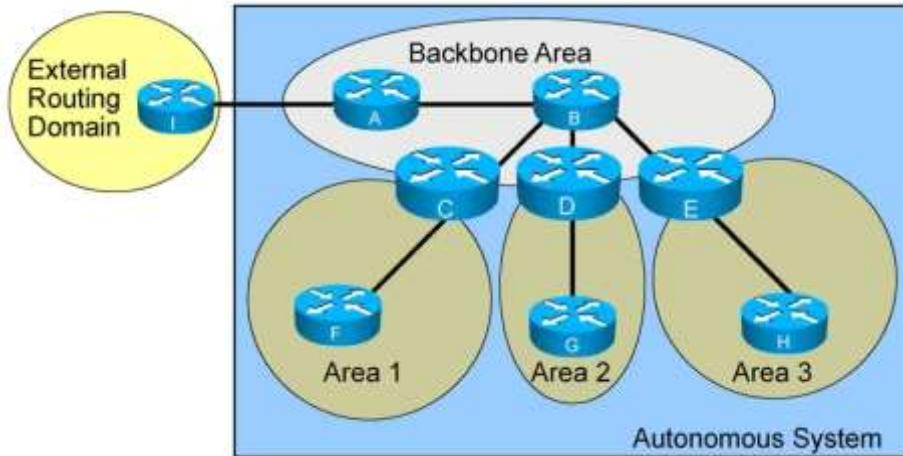
Lo primero que hace OSPF es inundar con paquetes LSA (link state advertise) de manera multicast a la dirección 224.0.0.5 (satura la red solo en principio), de esa manera obtiene información de toda la red en una base de datos “ospf link state data base, LSDB” y mediante su algoritmo SPF realiza su diagrama de red usando el costo.

#### 6.1.1. Areas OSPF

Es un protocolo jerárquico, para segmentar la red la divide en áreas, lo que minimiza las entradas de enrutamiento y localiza los impactos dentro un área en otras palabras lo que se consigue al segmentar la

red en áreas es que limita los cambios o actualizaciones de red dentro de una sola área, osea el cambio en un área es independiente del resto.

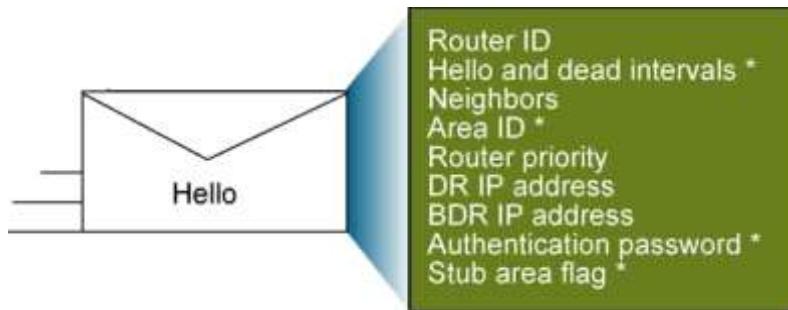
- Área 0 o backbone es el área principal donde todas las demás áreas están conectadas a esta.
  - Los routers que comunican el área 0 con las áreas inferiores se denominan Area border router (ABR) estos routers tienen una interfaz en el área 0 y otra interfaz en otra área. Separan en zonas las inundaciones de LSA, es el punto principal para la sumarización de direcciones de áreas, mantiene el link state data base de cada área con la cual se está conectada.
  - Los routers inferiores, internos o non backbone tienen todas sus interfaces dentro de un área, estos routers usan un enlace virtual para conectarse con el área 0 o Backbone.
- Las distintas áreas siempre se tienen que conectar al área 0.



- El router ASBR (Autonomous System boundary Router) se encarga de conectar a OSPF con protocolo de enrutamiento EIGRP, RIP, BGP.

#### 6.1.2. Paquete Hello

Es un paquete que contiene Router ID, destino, la prioridad, el área al cual pertenece, password de autenticación.



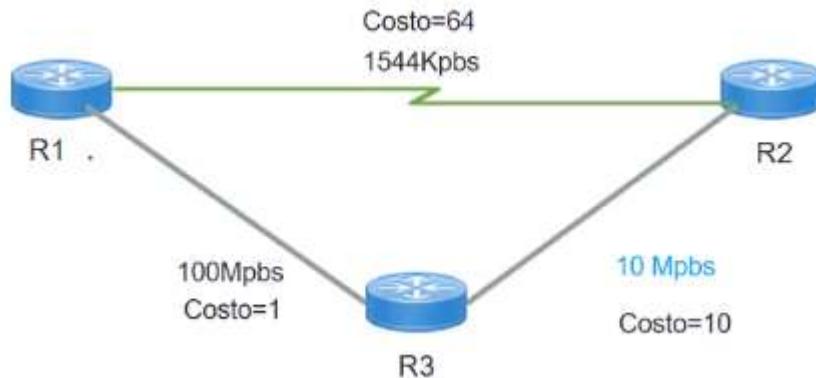
Nota: si no se tiene el mismo intervalo de tiempo hello no se forma adyacencia. El Dead interval si no se recibe un hello en 40 s significa que la interface está down.

#### 6.1.3. Métrica de OSPF

El algoritmo de OSPF Utiliza como métrica el costo, a menor costo mejor camino

$$\text{costo} = \frac{\text{ancho de banda referencial}}{\text{ancho de banda el interface}} = \frac{100 \text{ Mbps}}{\text{BW interface}}$$

Ejemplo: la ruta de R1-R2 = 64 de costo y la ruta R1-R2-R3= 11 costo, la mejor ruta es la del costo menor



Nota: para interfaces de gigabit hacia arriba, se debe ajustar el ancho de banda de referencia.

R2(config)# router ospf "process ID"

R2(config-router)# auto-cost reference-bandwidth "el valor está en Mbits"

Tambien se puede ajustar el costo por interfaz

R1(config)# interface fastEthernet 0/1

R1(config-if)# ip ospf cost 1

#### 6.1.4. Configuración de OSPF

- En OSPF solo se coloca las redes directamente conectadas al router.

router(conf)# router ospf (process-id, que va de 1 a 65535).

**Nota:** El sistema autónomo AS es de EIGRP y process-id es de OSPF a diferencia de EIGRP el process id puede ser distinto.

router(conf-rou)# network (address) (wildcard-mask) área (área-id)

Ejemplo 1.

Router(conf)# router ospf 100

Router(conf-ruta)# Network 10.1.1.2 0.0.0.0 area 0 //interface local que conecta a la red

Ejemplo 2.

Router(conf)# router ospf 100

Router(conf-ruta)#Network 10.1.1.0 0.0.0.255 area 0 //la red directamente conectada

#### 6.1.5. El router id

Es el número identificador asignado al router es el identificador para mandar los HELLOs,

- el primer criterio es usar la IP más alta de la interface loopback,
- si no está configurada la loopback el segundo criterio es la IP más alta de las interfaces activas.
- El tercer criterio es designar manualmente insertando el router-ID.

#### 6.1.6. Estados de ospf.-

- **Down state**, no tiene ninguna relación de adyacencia con otro router
- **Init state**, se envía el mensaje HELLO al otro router y viceversa
- **Two-way state**, se forma el estado de adjacencia

- **Exstart state**, (en redes multi-acceso donde varios routers están unidos por un switch) donde los router no intercambian tablas de enrutamiento entre routers si no que se establece DR (designen router) que es el router al cual los demás routers le envían la tabla de enrutamiento debido a que no se envían tabla de enrutamiento entre ellos, este DR es el que tiene mayor prioridad (por defecto 1) en caso que tengan la misma prioridad se escoge la loopback mas alta sino hay loopback o la ip más alta. También se escoge BDR (backup designed router) de esta manera se establece adyacencia entre los router
- **Exchange state**
- **Loading state**
- **Full state**, los router intercambian tablas de enrutamiento

#### 6.1.7. Tipos de paquetes de OSPF.-

- **Hello**, multicast 224.0.0.5, descubre y mantiene vecinos, designa quien es el Designed Router y Backbone Design Router.
- **DBD data base description**, contiene los LSA o (link state advertise) que ayudan a construir la (link state date base) LSDB por ello **verifica la sincronización** de data base.
- **LSR (Link State Request)**, se genera cuando falla la verificación de LSA dentro DBD por ello el router requiere específicamente archivos link-state de otro router vecino y envía el LSU
- **LSU**, contiene la lista de LSA que se deben actualizar este paquete también se usa para inundar
- **LSAck**, verifican la confiabilidad de los LSA osea que indica que los LSU fueron recibidos y reconoce los otro tipos de paquetes

#### 6.1.8. Creación de adyacencia

Crea adyacencia si tiene el mismo:

- **Hello interval**, 10s en (LAN, Punto a Punto) y 30s (punto multipunto frame relay)
- **Dead interval**, 40s en (LAN, Punto a Punto) y 140s (punto multipunto frame relay)
- **Tipo de red**, o sea mascara
- **ID de área**
- **Password**

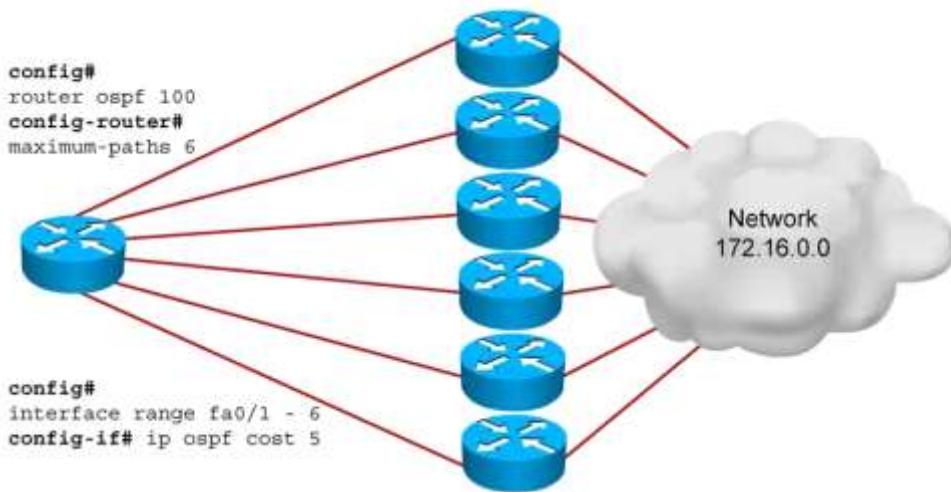
#### 6.1.9. LSA link state advertise

Comunica la topología de enrutamiento local del enrutador a todos los demás enrutadores locales en la misma área OSPF. Comando de verificación “show ip data base”

- Tipo 1: LSA enrutador, son los LSA propios de cada router, contienen los link de los router conectado directamente a ellos.
- Tipo 2: de redes multiacceso (routers conectados mediante un switch) como ethernet, usa la dirección de la interfaz IP del Designed Router
- Tipo 3: Creados por los Area Border Router, contienen la lista de subredes de áreas adjuntas.
- Tipo 4: identifican los router de borde (router que conectan a redes que no son OSPF)
- Tipo 5: anuncian los prefijos de redes que sean distribuidas por ASBR
- Tipo 6: no se usan en cisco
- Tipo 7: áreas nnsa, reemplazan los de tipo 5

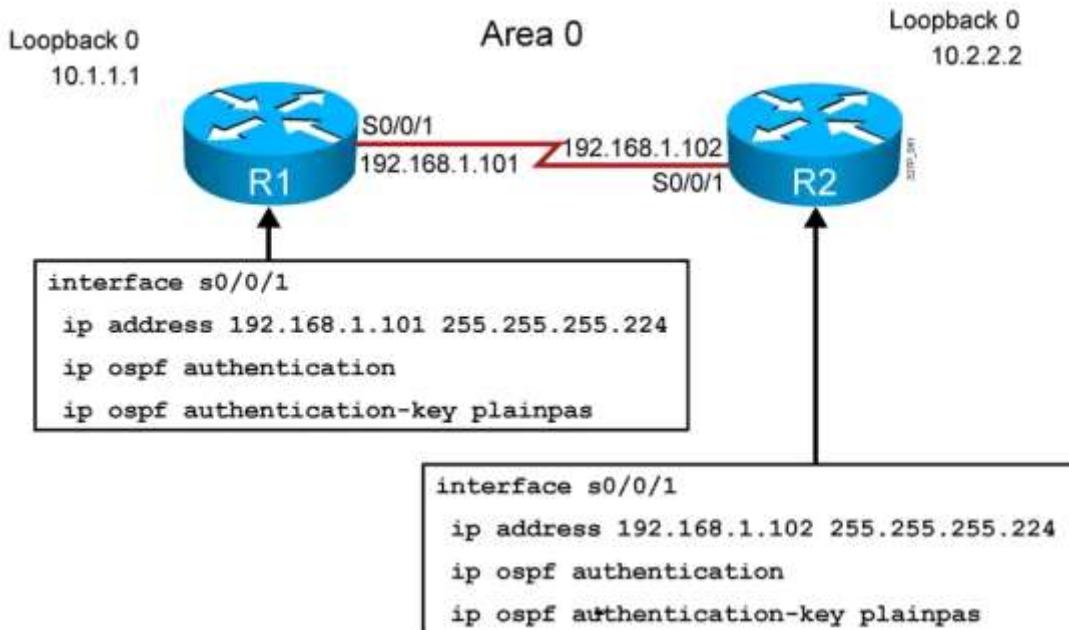
#### 6.1.9. Balanceo de carga

En ospf se permite hacer balanceo de carga (4 por defecto a 16) pero solo en rutas de igual costo, no interesa el ancho de banda



#### 6.1.10. Ospf autenticación

Soporta dos tipos de autenticación en texto plano o claro y md5



```
RouterX# debug ip ospf events
```

```

OSPF:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30

```

```

OSPF: rcv. v:2 t:1 l:48 rid:200.0.0.117
aid:0.0.0.0 chk:6AB2 aut:0 auk:

```

```
RouterX# debug ip ospf packet
```

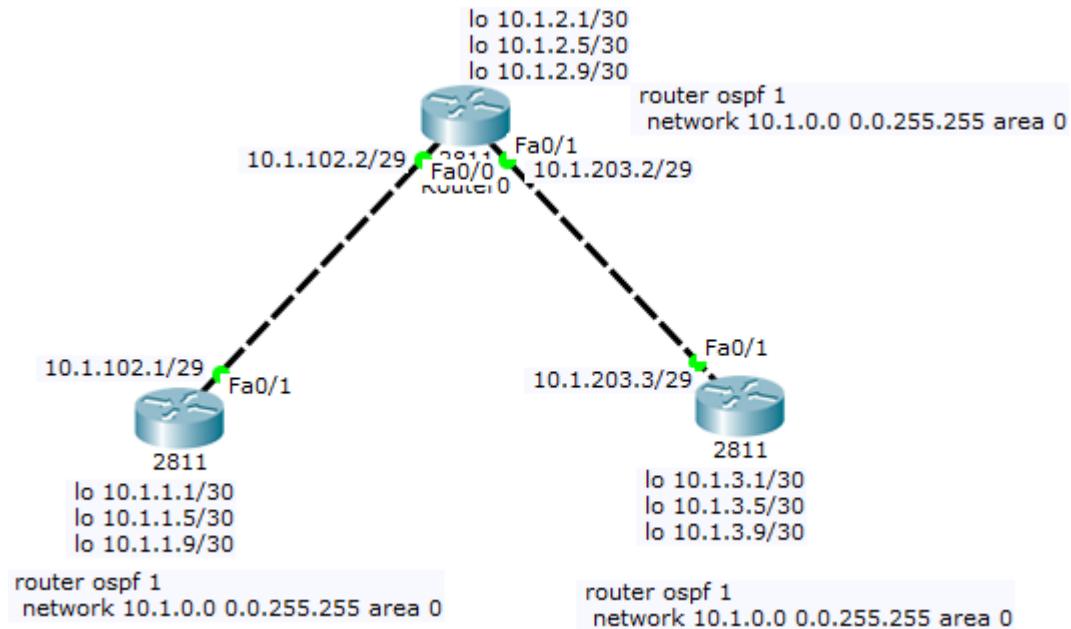
```

OSPF: rcv. v:2 t:1 l:48 rid:200.0.0.116
aid:0.0.0.0 chk:0 aut:2 keyid:1 seq:0x0

```

Nota: Aut es autenticación, el valor 0 indica que no hay autenticación, 1 autenticación en texto plano, 2 autenticaciones encriptado

### 6.1.11. OSPF sumarizado



Router derecho vemos las rutas directamente conectadas

```

Router#show ip route connected
C 10.1.3.0/30  is directly connected, Loopback31
C 10.1.3.4/30  is directly connected, Loopback32
C 10.1.3.8/30  is directly connected, Loopback33
C 10.1.203.0/29  is directly connected, FastEthernet0/1
  
```

Las rutas aprendidas mediante ospf

```

Router#show ip route ospf
 10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
O     10.1.1.1 [110/3] via 10.1.203.2, 00:11:15, FastEthernet0/1
O     10.1.1.5 [110/3] via 10.1.203.2, 00:11:15, FastEthernet0/1
O     10.1.1.9 [110/3] via 10.1.203.2, 00:11:15, FastEthernet0/1
O     10.1.2.1 [110/2] via 10.1.203.2, 00:12:08, FastEthernet0/1
O     10.1.2.5 [110/2] via 10.1.203.2, 00:12:08, FastEthernet0/1
O     10.1.2.9 [110/2] via 10.1.203.2, 00:12:08, FastEthernet0/1
O     10.1.102.0 [110/2] via 10.1.203.2, 00:11:25, FastEthernet0/1
  
```

```
RouterX# show ip ospf
  Routing Process "ospf 50" with ID 10.64.0.2
<output omitted>

  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Number of areas transit capable is 0
  External flood list length 0
    Area BACKBONE(0)
    Area BACKBONE(0)
      Area has no authentication
      SPF algorithm last executed 00:01:25.028 ago
      SPF algorithm executed 7 times
<output omitted>
```

```
RouterX# show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived,
C - connected, S - static, E - EGP derived, B - BGP derived,
E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route

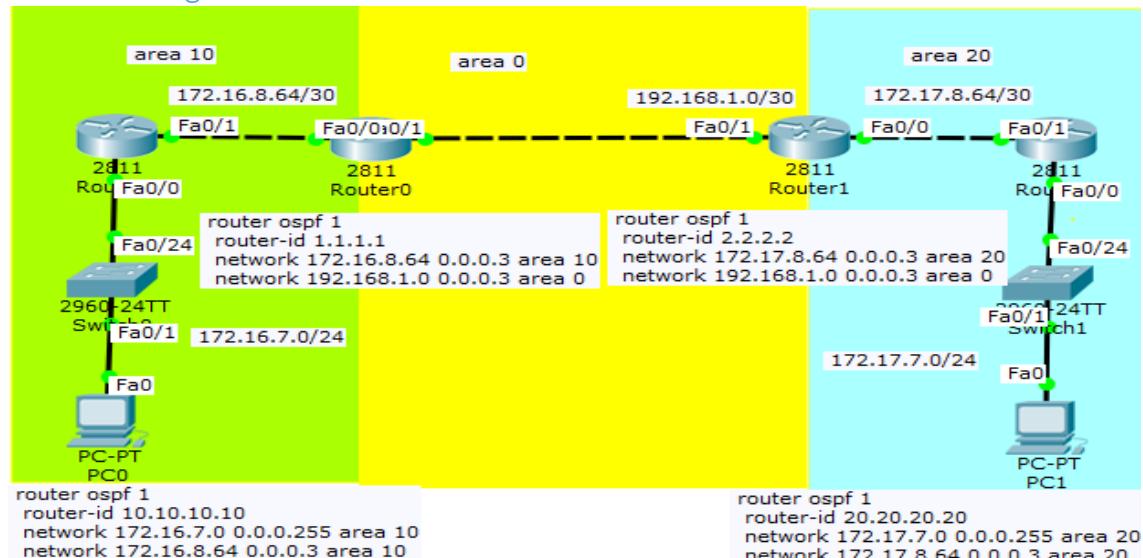
Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O 10.110.0.0 [110/5] via 10.119.254.6, 0:01:00, Ethernet2
O IA 10.67.10.0 [110/10] via 10.119.254.244, 0:02:22, Ethernet2
O 10.68.132.0 [110/5] via 10.119.254.6, 0:00:59, Ethernet2
O 10.130.0.0 [110/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.128.0.0 [170/10] via 10.119.254.244, 0:02:22, Ethernet2
```

```
RouterX# show ip ospf interface ethernet 0

Ethernet 0 is up, line protocol is up
Internet Address 192.168.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.168.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 192.168.254.10, Interface address 192.168.254.10
Backup Designated router id 192.168.254.28, Interface addr 192.168.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.254.28 (Backup Designated Router)
  Adjacent with neighbor 192.168.254.10 (Designated Router)
```

### 6.1.12. Configuración áreas



### 6.1.13. OSPF v3 para IPv6

Desarrollado para IPv6, maneja las tablas de topología, IP routing, adyacencia de manera independiente.

Algoritmo de enrutamiento SPF (shortest path first, el camino más corto primero). ID del router 32bits.

Características:

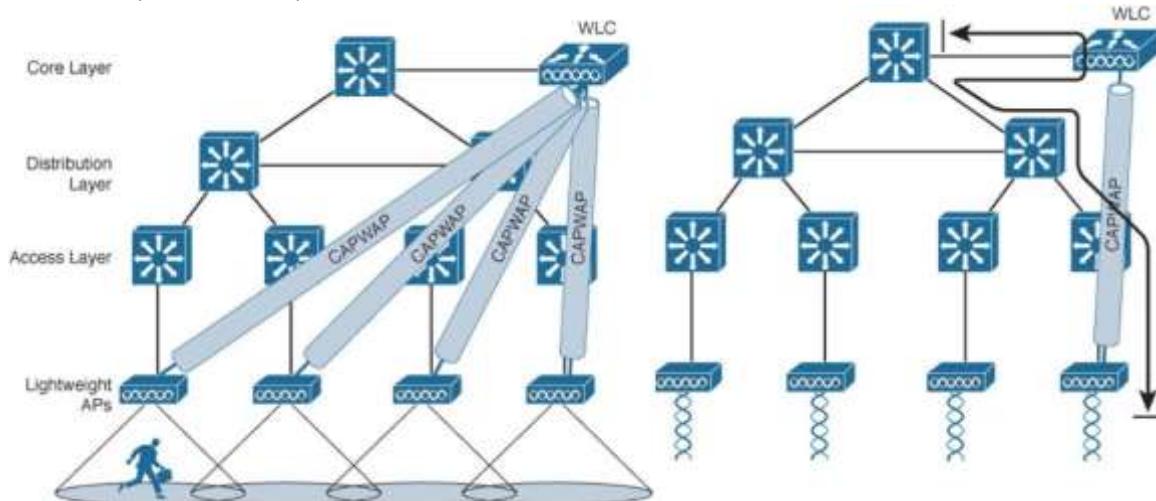
- Anuncios: utilizando IPv6
- Dirección de origen: link-local de la interfaz de salida
- Dirección multicast: FF02::5
- Dirección de Multicast de DR/BDR: FF02::6
- Anuncio de redes: dentro de la interface “**router(config-if)# ipv6 ospf id-process area id-área**”
- IP routing: **#ipv6 unicast-routing**

<b>router#configure terminal</b>	Ingrese al modo de configuración global
<b>router(config)#ipv6 unicast-routing</b>	Habilite IPv6 unicast forwarding
<b>router(config)#interface interface</b>	Ingrese a la interfaz
<b>router(config-if)#ipv6 ospf process-id area area</b>	Habilite OSPFv3 en la interfaz
Para IOS versión 15 en adelante: <b>router(config-if)#ospfv3 process-id area area</b>	
<b>router(config)#ipv6 router ospf process-id</b>	Ingrese al modo de router configuration mode. En el modo de configuración global.
<b>router(config-router)#router-id ip-ad</b>	Configure el router-ID que usará OSPFv3. Requerido.

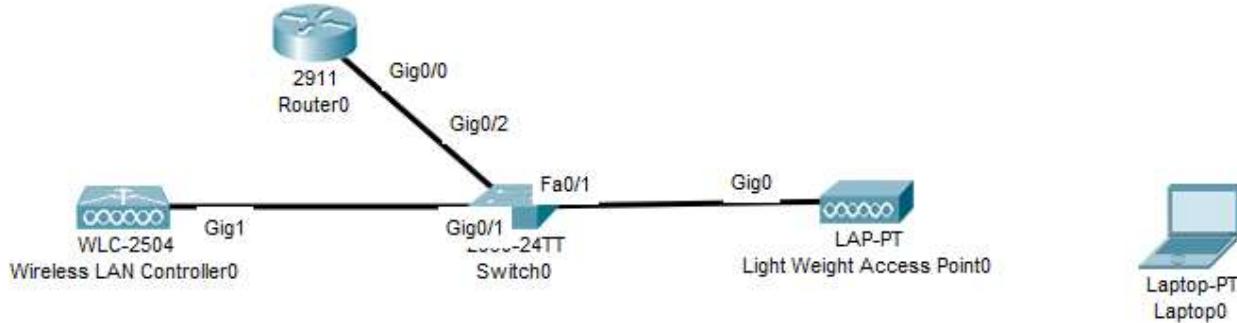
<b>show ipv6 ospf</b>	Muestra Procesos OSPF
<b>show ipv6 ospf interface</b>	Muestra detalles sobre OSPF en las interfaces
<b>show ipv6 ospf neighbor</b>	Muestra la lista de vecinos
<b>show ipv6 ospf database</b>	Muestra la Base de datos o LSDB
<b>show ipv6 route ospf</b>	Muestra las rutas OSPF

## 7.1. Configuración de una red Wireless

### 7.1.1. Arquitectura Split-MAC centralizada



El tráfico se canaliza desde el LAP (lightweight) al WLC (Wireless LAN Controller). La ruta de dos entre dos usuarios inalámbricos donde el tráfico del primer cliente pasa por el LAP donde se encapsula en el túnel CAPWAP, luego viaja hasta la capa central para alcanzar el wlc, donde no está encapsulado. Para pasar al otro cliente el proceso se revierte y el tráfico vuelve a bajar por el túnel para llegar al mismo LAP para volver al aire.



#### Paso 1. Router

```

ip dhcp excluded-address 10.0.0.1 10.0.1.10
ip dhcp pool SISTEMAS
network 10.0.1.0 255.255.255.0
default-router 10.0.1.1
interface FastEthernet0/0.1
encapsulation dot1Q 1
ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 10.0.1.1 255.255.255.0
    
```

#### Paso 2. Configuración del Switch

Vlan 10
Name sistemas

#### Conexión del WLC

interface GigabitEthernet0/1
switchport trunk allowed vlan 1,10
switchport mode trunk

#### Conexión de Lightweight AP, usamos puerto acceso debido a que las vlans viajan por el túnel CAPWAP

Interface fasEthernet 0/1
Switchport access vlan1
Switchport mode access

#### Conexion al router

Interface G0/2
switchport mode trunk

### Paso 3. Configuracion del wlc

The screenshot shows the Cisco Wireless Controller (WLC) interface. On the left, there's a sidebar with 'Supervisión' (Monitoring) and 'Pícaros' (Clients). The main area is titled 'RESUMEN DE RED' (Network Summary). It displays two sections: 'Redes inalámbricas' (Wireless Networks) with 1 entry and 'Puntos de acceso' (Access Points) with 0 entries. At the top right, there are several icons and a search bar. The 'Avanzado' button in the top right corner is highlighted with a red box. In the navigation bar at the top, the 'WIRELESS' tab is also highlighted with a red box.

Verificamos la lista de Access Point registrados en el wlc, y el modo de conexión, ip de configuracion

This screenshot shows the detailed configuration for the AP-3702. The 'General' tab is selected in the top navigation bar. Under 'General', the AP Name is set to 'AP-3702'. The 'AP Mode' dropdown is set to 'local' and is highlighted with a red box. The 'IP Address(Ipv4/Ipv6)' field is set to '192.168.1.34' and is also highlighted with a red box. Other fields like Location, Admin Status, and Port Number are also visible. The 'Advanced' tab is selected in the top navigation bar.

This screenshot shows the 'Controller > Interfaces' configuration page. The 'Interfaces' tab is selected in the top navigation bar. The table lists three interfaces: 'management', 'service-port', and 'virtual'. The 'management' interface is highlighted with a red box. The columns include 'Interface Name', 'VLAN Identifier', 'IP Address', 'Interface Type', and 'Dynamic AP Management'. The 'management' interface has an IP address of '192.168.1.30' and is of type 'Static' with 'Enabled' dynamic AP management.

En interfaces se ve 3 interfaces creadas por management, que es la interfaz que nos conectamos para la administración web <https://192.168.1.30> la misma puede ser usada para una red wlan.

Paso 4. Creamos una interfaces para Sistemas.

### Interfaces > New

Interface Name	<input type="text" value="Sistemas"/>
VLAN Id	<input type="text" value="10"/>

Apply

### Interfaces > Edit

< Back

Apply

#### General Information

Interface Name	Sistemas
MAC Address	00:0c:29:25:7f:b9

#### Configuration

Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	<input type="text" value="0"/>
NAS-ID	<input type="text" value="none"/>

#### Physical Information

Port Number	<input type="text" value="1"/>
Enable Dynamic AP Management	<input type="checkbox"/>

#### Interface Address

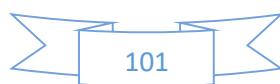
VLAN Identifier	<input type="text" value="10"/>
IP Address	<input type="text" value="10.0.1.254"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="10.0.1.1"/>
IPv6 Address	<input "::"="" type="text" value=""/>
Prefix Length	<input type="text" value="128"/>
IPv6 Gateway	<input "::"="" type="text" value=""/>
Link Local IPv6 Address	<input type="text" value="fe80::20c:29ff:fe25:7fb9/64"/>

#### DHCP Information

Primary DHCP Server	<input type="text" value="10.0.1.1"/>
Secondary DHCP Server	<input type="text"/>

#### Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Addr
<a href="#">management</a>	untagged	192.168.1.30	Static	Enabled	::/128
<a href="#">service-port</a>	N/A	172.16.1.30	Static	Disabled	::/128
<a href="#">sistemas</a>	10	10.0.1.254	Dynamic	Disabled	::/128
<a href="#">virtual</a>	N/A	2.2.3.3	Static	Not Supported	



Paso 5. Creamos la WLAN, el SSID es el nombre que veremos en nuestros dispositivos móviles

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar includes MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COMMANDS. The WLANS tab is selected. On the left, a sidebar shows 'WLANS' expanded, with 'WLANS' and 'Advanced' options. The main area displays a table header with columns: WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, Security Policies. A red box highlights the 'Create New' button and the 'Go' button next to it. Below the table, the URL 'WLANS > New' is visible, along with '< Back' and 'Apply' buttons.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
	WLAN	perfil de sistemas	wifi-sistemas		
ID	2				

En Radio Policy, escojemos las bandas de frecuencia a, b, ac, n o all. El Broadcast SSID indica si es visibles en los dispositivos móviles a la hora de conectarnos, no hacerlo visible no aumenta seguridad.

The screenshot shows the 'Edit 'perfil de sistemas'' configuration page. The 'General' tab is selected. The configuration includes:

- Profile Name:** perfil de sistemas
- Type:** WLAN
- SSID:** wifi-sistemas
- Status:** Enabled (checkbox checked)
- Security Policies:** [WPA2][Auth(802.1X)]  
(Modifications done under security tab will appear after applying the changes.)
- Radio Policy:** All
- Interface/Interface Group(G):** sistemas
- Multicast Vlan Feature:** Enabled (checkbox checked)
- Broadcast SSID:** Enabled (checkbox checked)
- NAS-ID:** none

WPA2 AES, es el modo de encriptación más seguro disponible, la autenticación será Pre-Shared Key PSK donde se establece previamente una clave para toda la WLAN

**General Security QoS Policy-Mapping Advanced**

**Layer 2 Layer 3 AAA Servers**

Layer 2 Security: WPA+WPA2  
MAC Filtering:

**Fast Transition**  
Fast Transition: Adaptive  
Over the DS:   
Reassociation Timeout: 20 Seconds

**Protected Management Frame**  
PMF: Disabled

**WPA+WPA2 Parameters**  
WPA Policy:   
WPA2 Policy:   
WPA2 Encryption:  AES  TKIP  CCMP256  GCMP128  GCMP256  
OSEN Policy:

**Authentication Key Management**  
802.1X:  Enable  
CCKM:  Enable  
PSK:  Enable  
FT 802.1X:  Enable  
FT PSK:  Enable  
PSK Format: ASCII  passwordwifi

WLANS > Edit 'perfil de sistemas'

**General Security QoS Policy-Mapping Advanced**

Allow AAA Override:  Enabled  
Coverage Hole Detection:  Enabled  
Enable Session Timeout:  36000 Session timeout (secs)  
Aironet IE:  Enabled  
Diagnostic Channel:  Enabled  
Override Interface ACL: IPv4: None  IPv6: None   
Layer2 Adi: None   
URL ACL: None   
P2P Blocking Action: Disabled   
Client Exclusion:  Enabled 180 Timeout Value (secs)  
Maximum Allowed Clients: 0

DHCP  
DHCP Server:  Override  
DHCP Addr. Assignment:  Required  
OEAP  
Split Tunnel:  Enabled

Management Frame Protection (MFP)  
MFP Client Protection:  Optional   
DTIM Period (in beacon intervals):  
802.11a/n (1 - 255): 1  
802.11b/g/n (1 - 255): 1  
NAC  
NAC State: None   
Load Balancing and Band Select

Guardar los cambios

## WLANS

Current Filter: None [Change Filter] [Clear Filter] Create New ▾ Go

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	1	WLAN	perfil de sistemas	wifi-sistemas	Enabled	[WPA2][Auth(PSK)]	<input checked="" type="checkbox"/>

Verificar si los radios están habilitados tanto 802.11a/b

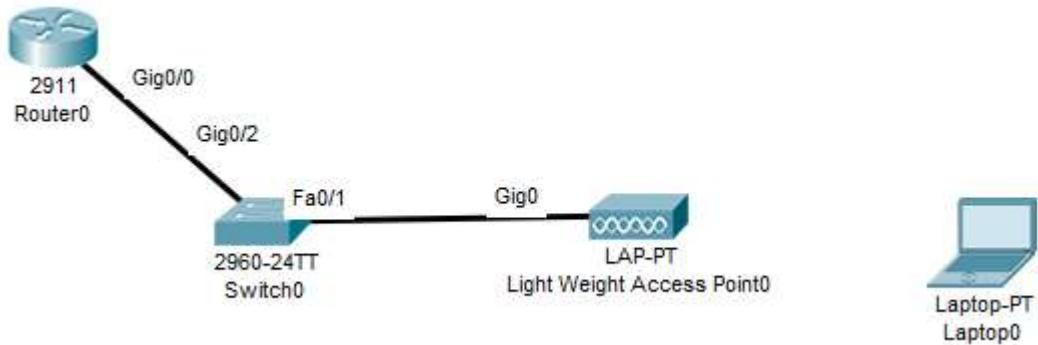
Data Rate	Status
1 Mbps	Mandatory
2 Mbps	Mandatory
5.5 Mbps	Mandatory
6 Mbps	Supported
9 Mbps	Supported
11 Mbps	Mandatory
12 Mbps	Supported
18 Mbps	Supported

Probar con un cliente y verificar se se unió correctamente

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name
f4:60:e2:bf:5a:ac	192.168.1.101	AP-3702

### 7.1.2. Arquitectura autónoma

Cada AP independiente, es una extensión de una red switchada que conecta los SSID a las VLAN en la capa de acceso. En este caso no hay CAPWAP y las VLANs deben ser troncalizadas en la conexión entre el AP y el switch.



### Ejemplo AIR CAP 2621 A K9

Asignar una dirección IP a la interfaz de administración

```

Ap (conf) # interface BVI1
Ap (conf-if) # ip address 192.168.1.34 255.255.255.0
  
```

Configuración de las interfaces de radio, Radio 0 equivale la banda de 2.4G y Radio 1 a 5G

```

Ap (conf) # interface Dot11Radio0
Ap (conf-if) # encryption mode ciphers aes-ccm
Ap (conf-if) # ssid SISTEMAS
Ap (conf-if) # no shutdown
Ap (conf-if) # exit

Ap (conf) # interface Dot11Radio1
Ap (conf-if) # encryption mode ciphers aes-ccm
Ap (conf-if) # ssid SISTEMAS
Ap (conf-if) # no shutdown
Ap (conf-if) # exit
  
```

Configurar SSID

```

Ap (conf) # dot11 ssid SISTEMAS
Ap (conf-if) # band-select
Ap (conf-if) # authentication open
  
```

Habilitar el protocolo de seguridad wpa versión 2

```

Ap (conf-if) # authentication key-management wpa version 2
Nota.- previa configuración de ciphers aes-ccm
  
```

Permitir visibilidad de ssid

```

Ap (conf-if) # guest-mode
  
```

Habilitar PSK, Se tiene 0 y 7 para la contraseña, el cero nos permite la configuración en texto claro, y el 7 una contraseña encriptada

```

Ap (conf-if) # wpa-psk ascii 0 "contraseña de ssid"
  
```

Configuración de DHCP

```

Ap (conf) # ip dhcp excluded-address 192.168.1.1 192.168.1.10
Ap (conf) # ip dhcp pool POOL
Ap (conf-if) # network 192.168.1.0 255.255.255.0
Ap (conf-if) # default-router 192.168.1.1
Ap (conf-if) # dns-server 8.8.8.8
  
```

## 8.1. REDES WAN

Es una red de área geográfica amplia comunica ciudades, continentes países, se considera la internet como una red WAN, el ancho de banda de una red WAN es mucho menor al de una LAN, existen dos tipos de WAN:

- **WAN pública:** la internet, todos pueden acceder al mismo no es confiable, no me permite una transferencia confiable (Bancos).
- **WAN privada:** Servicios dedicado Punto Punto (PPP), HDLC, Frame Relay (No utilizado actualmente), MPLS.

La WAN depende de un proveedor de servicios (Entel, axs,Tigo, Viva), el ancho de banda dentro de la WAN se cobra. Los servicios de WAN se encuentran dentro de la capa 1 física y 2 enlace de datos del modelo OSI. Capa 2 debido a que usa ATM, HDLC, Frame Relay y debido a que realiza encapsulación y capa 1 debido a que ve las funcionalidades físicas métodos guiados (fibra, coaxial) y no guiados (inalámbrico, satelital).

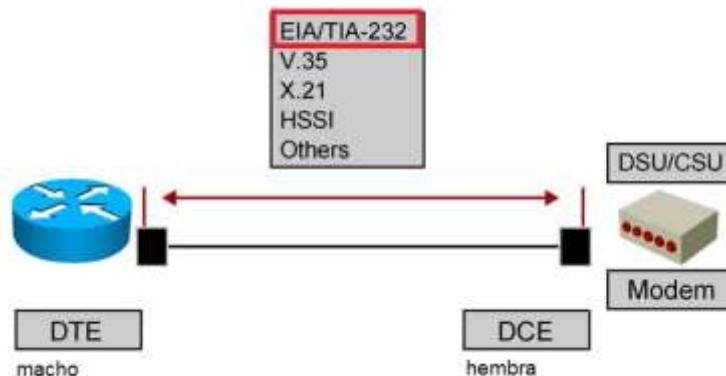
Su topología puede ser:

- **Point to Point:** de un lugar a otro directamente.
- **Hub and Spoke:** sitio central en el cual se concentran los demás enlaces)
- **Full Mesh:** todos con todos

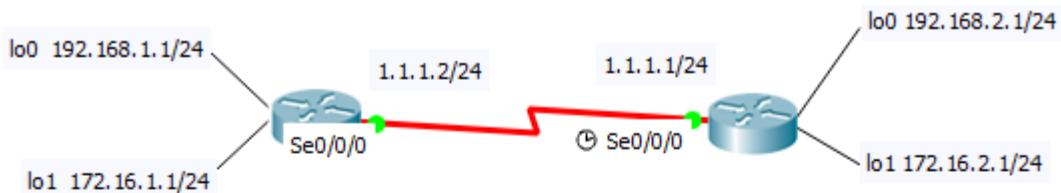
Términos wan:

- **CPE (Customer Premises Equipment):** Se contrata un servicio y nos dan un moden/router dentro de la oficina
- **Punto de Demarcación:** nos indica que desde el modem hacia la wan es responsabilidad del proveedor.
- **Local loop:** desde el modem hasta la oficina del proveedor de servicio
- **Central Office:** el proveedor de servicio

Los protocolos que más sobresalen son PPP punto a punto, MPLS (Multiprotocol label switching). En las redes WAN se tiene una comunicación serial RS-232 como DTE (termina la comunicación, pc) al router y DCE modem (inicia la comunicación), el DTE es macho y el DCE es hembra.



**Nota.-** Los router tienen un comando llamado “clock rate”, que solo simula esta velocidad.



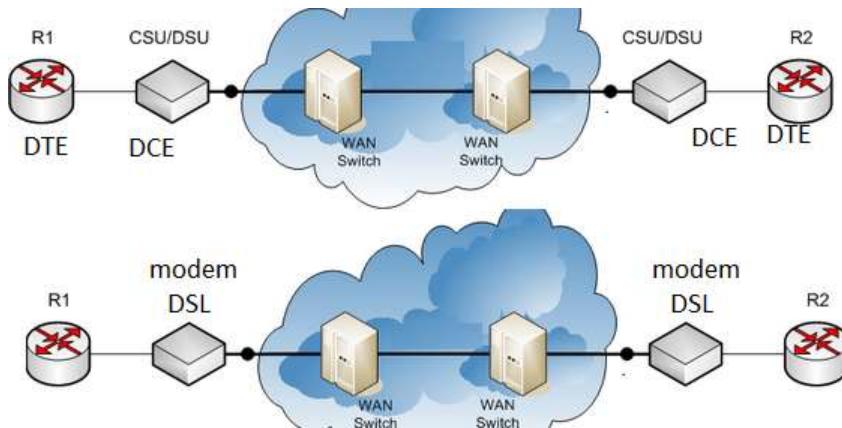
```
R2#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 9600
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:

R2#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 1.1.1.2/24
MTU 1500 bytes, BW 1000 Kbit DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC loopback not set, keepalive set (10 sec)
-----
```

```
R2#show ip route
1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Serial0/0/0
172.16.0.0/24 is subnetted, 2 subnets
D       172.16.1.0 [90/3200000] via 1.1.1.2, 00:03:42, Serial0/0/0
C       172.16.2.0 is directly connected, Loopback1
D       192.168.1.0/24 [90/3200000] via 1.1.1.2, 00:03:42, Serial0/0/0
C       192.168.2.0/24 is directly connected, Loopback0
```

Nota.- por defecto la encapsulación por defecto es HDLC

## 8.2. Dispositivos WAN



Una csu/dsu (chanel service unit/data service unit) convierte la señal digital de un router a una línea dedicada E1/T1. Termina un bucle local digital

Un modem convierte la señal digital de un router a una línea telefónica. Termina un bucle local analógico

## 7.3. VPN administrado por el proveedor MPLS

Comutación de paquetes en base a etiquetas no IP.

- A nivel capa 2, VPS y VPWS
- A nivel capa 3 MPLS VPN

#### 8.4. WAN privada

Se divide en dedicada (PPP) y conmutada (comutación de circuitos, comutación de celda y comutación de paquetes), de los cuales solo sigue vigente la comutación de paquetes (Frame relay (obsoleta), coaxial, DSL, MPLS).

##### 8.4.1. PPP punto a punto

Principal desventaja es su costo, método muy confiable para WAN, existe punto a punto sobre Ethernet PPPoE y punto a punto sobre ATM, es un protocolo de capa 2, establece una comunicación confiable entre dispositivos, tiene dos protocolos:

- NCP (Network Control Protocol).- Envío de paquetes sobre la encapsulación TCP.
- LCP (Link Control Protocol).- Establece la comunicación entre dispositivos.

##### 8.4.2. Establecer la sesión en PPP.-

- Se levanta la fase de conexión a nivel de capa 2 (acceso al medio)
- Fase de autentificación PAD (texto plano) y CHAP (encriptado) que es opcional
- La fase de establecimiento o comunicación de red

###### 8.4.2.1. PPP autentificación.-

- PAD (establece dos caminos de comunicación, envía el password y usuario y el otro extremo acepta inmediatamente “texto plano”)
- CHAD (tres vías de comunicación, envía un mensaje Challenge, responde y acepta la comunicación, utiliza encriptación MD5).

```
RouterX(config-if)# encapsulation ppp
```

- Enables PPP encapsulation

```
RouterX(config)# hostname name
```

- Assigns a hostname to your router

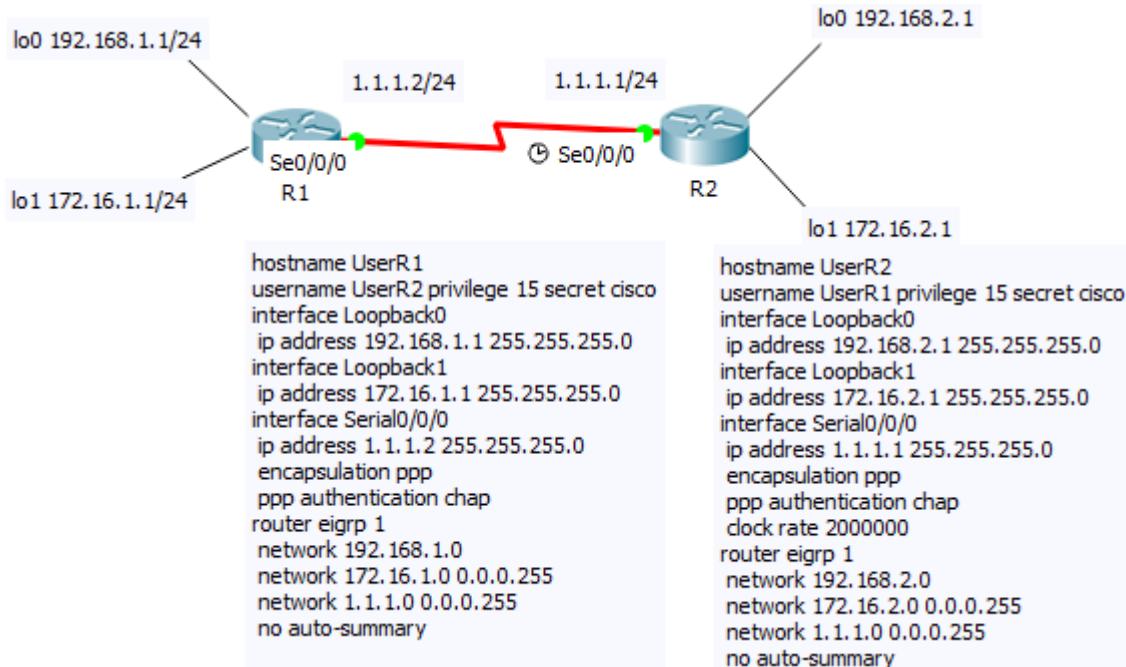
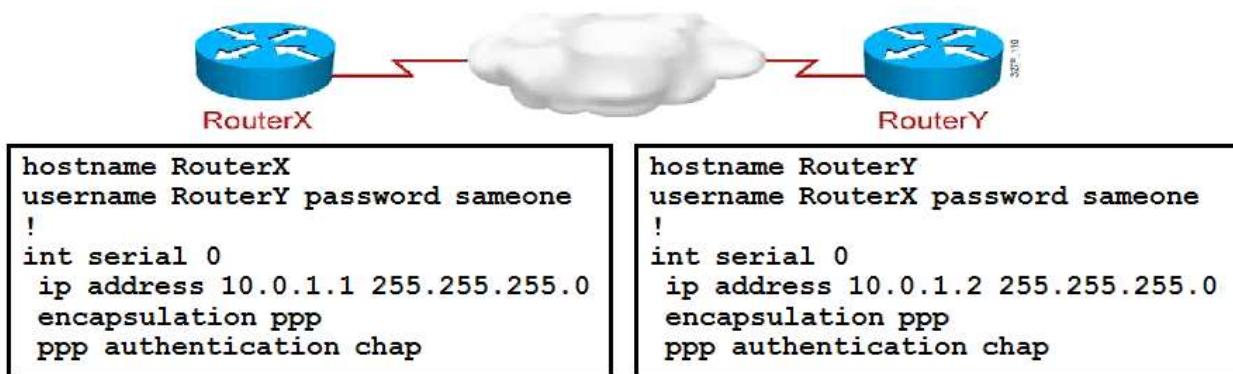
```
RouterX(config)# username name password password
```

- Identifies the username and password of remote router

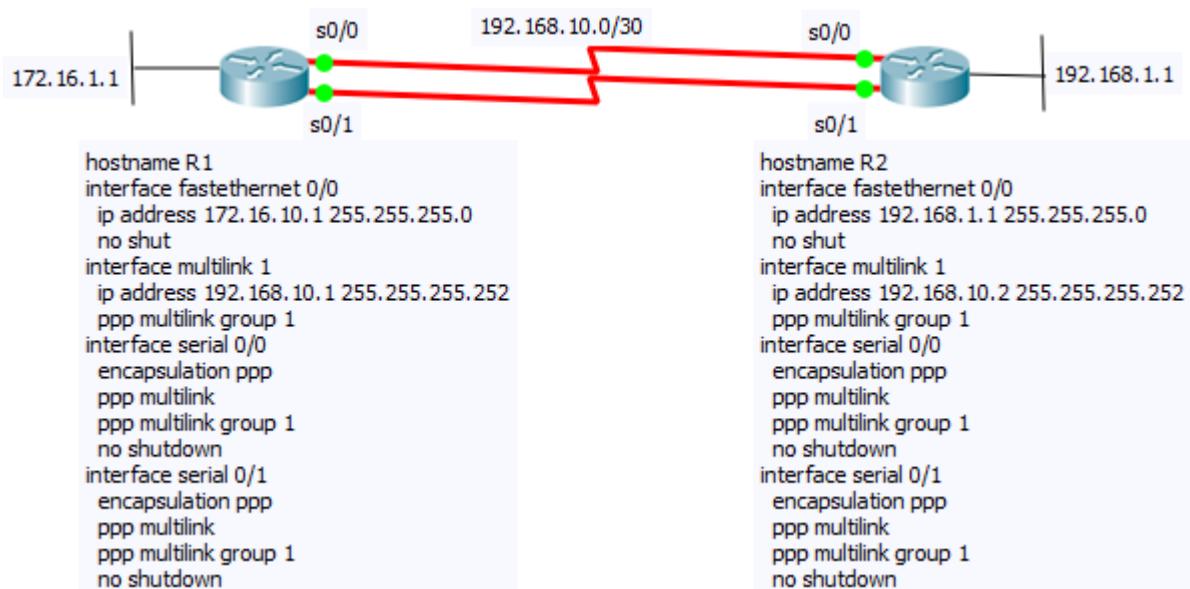
```
RouterX(config-if)# ppp authentication
{chap | chap pap | pap chap | pap}
```

- Enables PAP or CHAP authentication

Si en un lado es CHAP en otro lado debe ser CHAP, si es PAP en el otro extremo debe ser PAP, otra manera semi automática es colocando chap pap



## Multilink



```
R2(config-if)#no shutdown
R2(config-if)#do show ip int br
*Mar 1 00:45:59.267: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up
R2(config-if)#do show ip int br
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.1.1    YES manual up        up
Serial0/0          unassigned     YES TFTP  up        up
FastEthernet0/1    unassigned     YES unset administratively down down
Serial0/1          unassigned     YES TFTP  up        up
Multilink1         192.168.10.2   YES manual up        up
R2(config-if)#
*Mar 1 00:46:00.335: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, chan
up
```

```
R1#show interfaces multilink 1 stat
Multilink1
      Switching path      Pkts In    Chars In      Pkts Out    Chars Out
      Processor           39       4182          47       4494
      Route cache         22       1408          23       1610
      Total               61       5590          70       6104
```

Antes de la conexión se puede ver la siguiente información

```
RouterX# debug ppp authentication
4d20h: %LINK-3-UPDOWN: Interface Serial0, changed state to up
4d20h: Se0 PPP: Treating connection as a dedicated line
4d20h: Se0 PPP: Phase is AUTHENTICATING, by both
4d20h: Se0 CHAP: O CHALLENGE id 2 len 28 from "left"
4d20h: Se0 CHAP: I CHALLENGE id 3 len 28 from "right"          CHAD
4d20h: Se0 CHAP: O RESPONSE id 3 len 28 from "left"
4d20h: Se0 CHAP: I RESPONSE id 2 len 28 from "right"          .
4d20h: Se0 CHAP: O SUCCESS id 2 len 4
4d20h: Se0 CHAP: I SUCCESS id 3 len 4
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
```

#### 8.4.3. Comparación HDLC y PPP

##### HDLC

Funciona en la capa 2 (capa de enlace de datos)

protocolo orientado a bit

No tiene un método para detectar los errores.

Solía realizar la encapsulación de datos sin usar otros protocolos de encapsulación.

No es compatible con la autenticación, es decir, no proporciona autenticación entre dos nodos.

No verifica la calidad de un enlace establecido.

##### PPP

Funciona en la capa 2 y la capa 3 (la capa de red)

protocolo orientado a bytes

Utiliza FCS para detectar los errores mientras se transmiten los datos

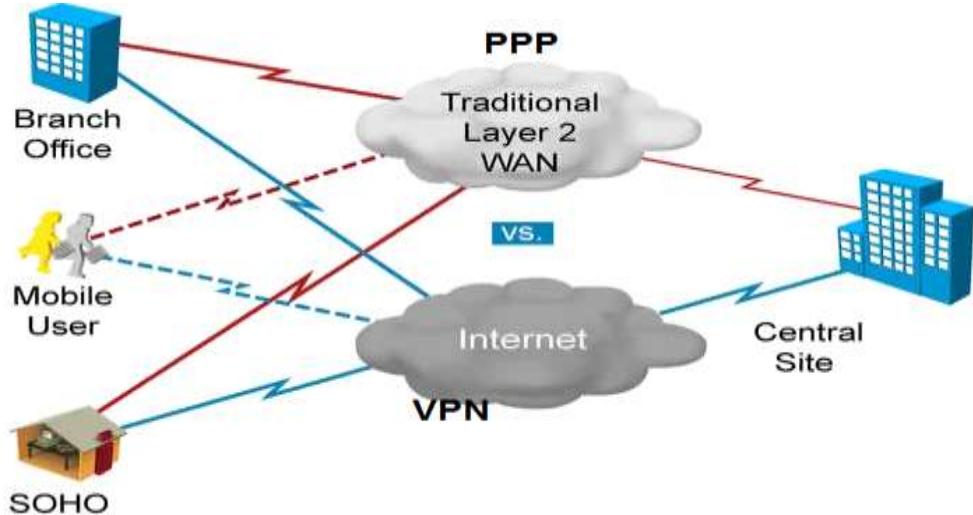
PPP no puede encapsular datos sin la ayuda de otros protocolos de encapsulación como HDLC, SDLC (control de enlace de datos síncronos)

Es compatible con la autenticación mediante protocolos como PAP y CHAP

Utiliza el protocolo de control de enlace (LCP) para verificar la calidad del enlace establecido.

### 8.5. Redes VPN (Virtual Private Network).-

La VPN es la información privada que se transporta por la red pública, se dice privado porque mantiene la confidencialidad. Las ventajas de una red VPN es el costo (a diferencia de PPP las VPN usan Internet para su transporte), seguridad (minimiza los riesgos de ataque) y escalabilidad o permeabilidad (debido a que esta para llegar a un sitio lo hace mediante Internet).

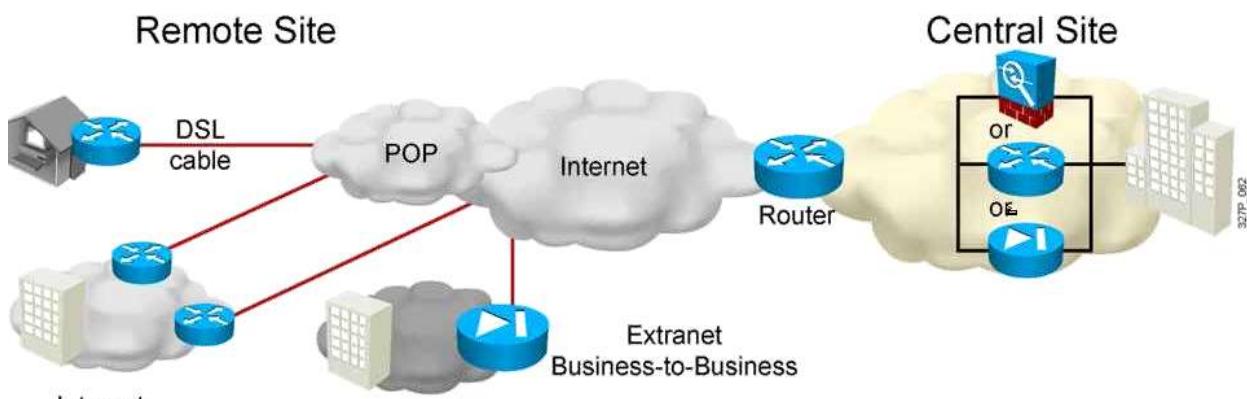


Existen dos tipos de VPN Site-to-Site y Remote Access

#### 8.5.1. VPN Sitio a Sitio

Se establece entre dos dispositivos similares (que soporten la tecnología, hardware), en cada sitio se debe tener un similar dispositivo es una extensión clásica de una WAN. Como ejemplos de VPN sitio a sitio se tiene.

- IPsec (abierta distintas tecnologías)
- GRE (solo soportan los routers).



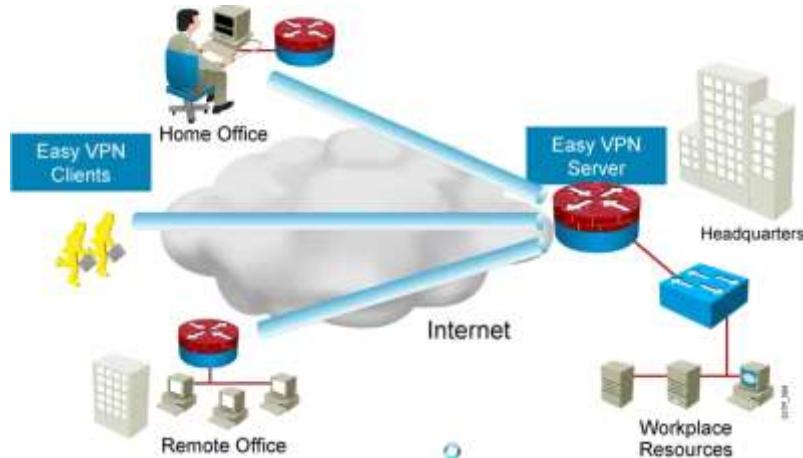
Router-router, Router-ASA, ASA-ASA

#### 8.5.2. VPN acceso remoto

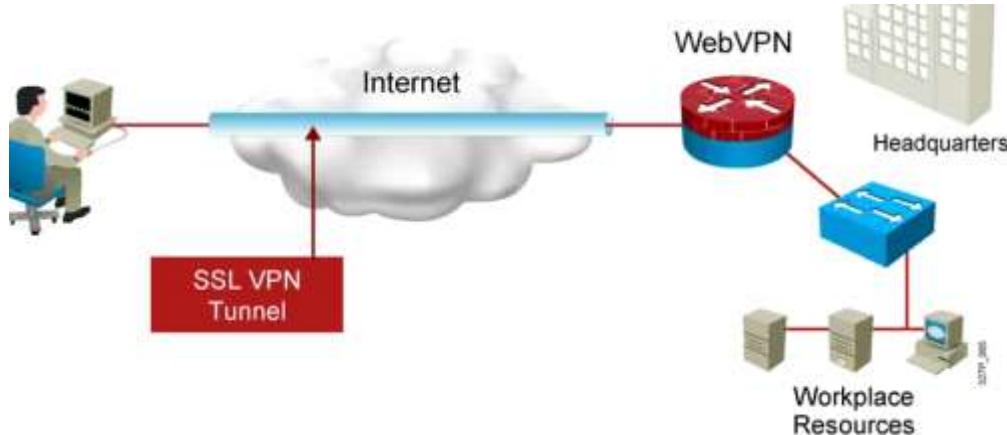
El router central actúa similar a un servidor VPN (no existe un servidor vpn) donde este arma la ruta con los routers de las sucursales, solo requiere que en un lugar soporte VPN en los otros puede ser SSL o HTTP, easy VPN, any conect.

Utiliza un browser que es un software navegador como mozilla, chrome, explore.

- Cisco Easy VPN: Del tipo acceso remoto se instala en el router central el Easy VPN Server y del lado de la sucursal el “Easy VPN Client”

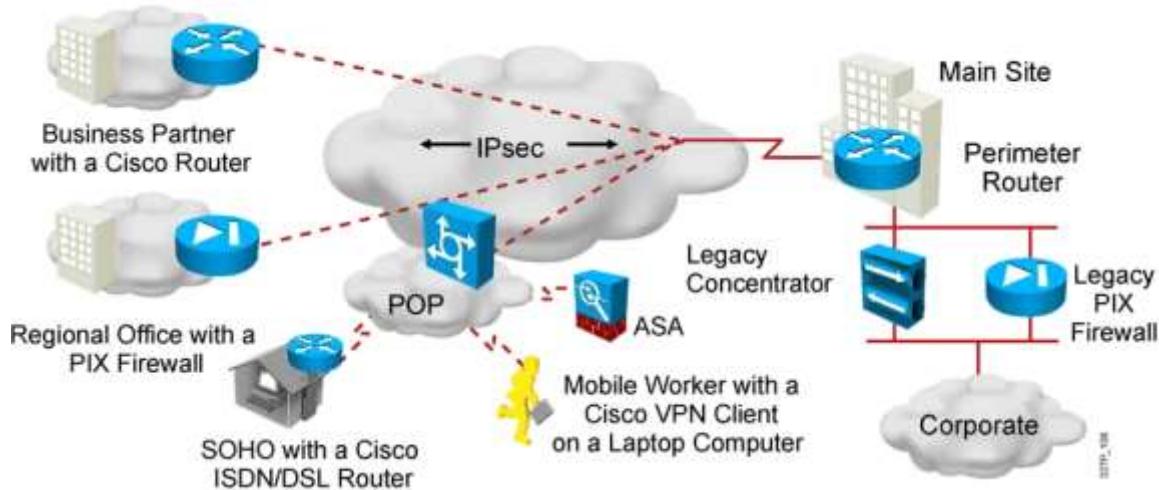


- IP sec SSL VPN (Wep VPN).- no requiere del fabricante es más estandarizado.



Nota: Cisco ASA es un dispositivo de seguridad tanto para VPN Sitio a Sitio o VPN acceso remoto.

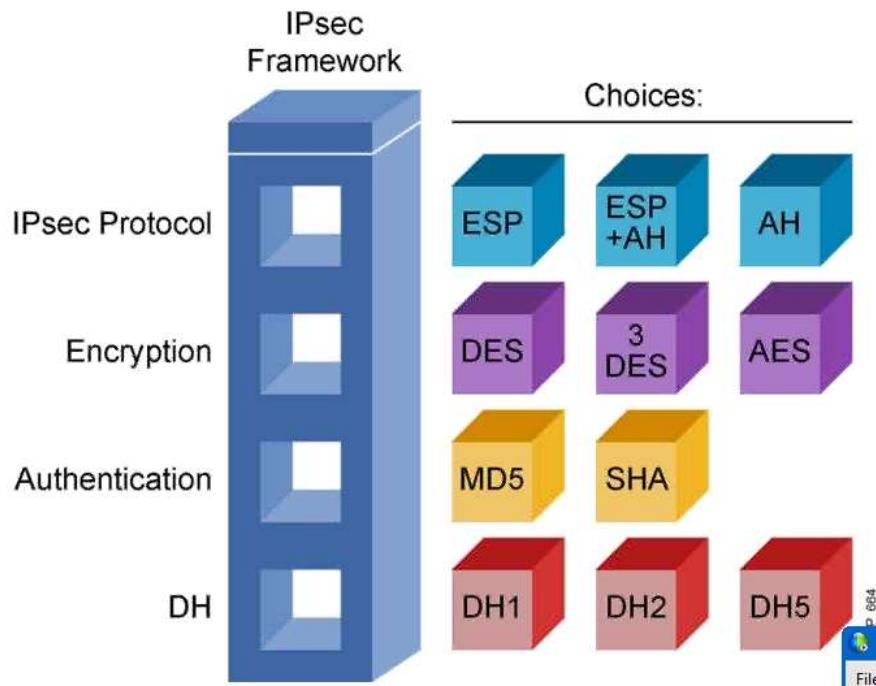
#### 8.5.3. Sitio a Sitio IPsec



Es un conjunto de algoritmos estándares o protocolos que permite dar:

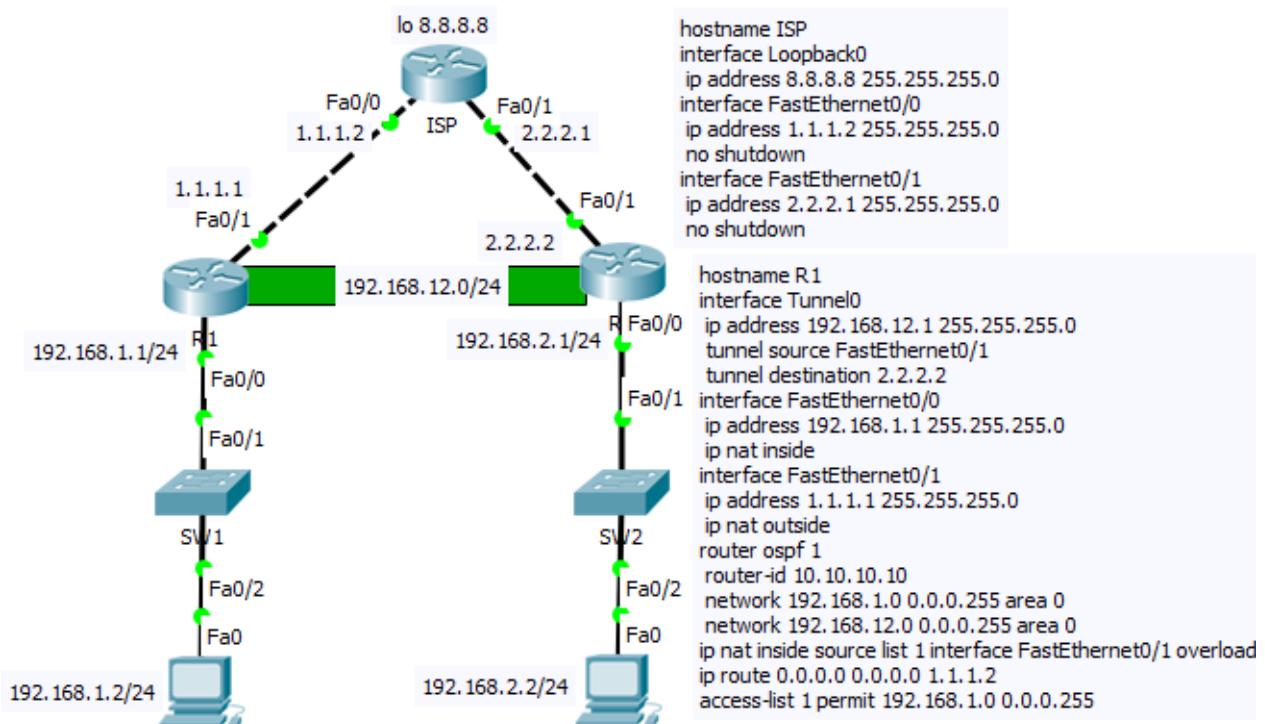
- **Confidentiality (encriptación):** los métodos de encriptación pueden ser simétricos misma llave entre origen y destino usan 255 bits de transformación (DES, AES (más seguro), 3DES) o asimétricos llaves distintas usa hasta 2048 bits de transformación (RSA).
- **Intercambio de llaves Diffi-helman,** encripta lo que ya está encriptado es asimétrico.
- **Integridad (no debe haber cambios en el trayecto).**- Se asegura que mi mensaje nunca cambie, usa los algoritmos Hashing (HMAC MD5, HMAC SHA-1, HMAC SHA-2), si el mensaje cambia en algún carácter el dato cambia de tamaño y lo descarta.
- **Autentificación (antes de levantar el túnel de comunicación verificará las credenciales).**- dos métodos PSK y RSA dos maneras de encapsulación
  - AH (authentication header) que hace autentificación e integridad.
  - ESP (encapsulation security payload) autentificación, Integridad además encripta
- **protección anti replay (no permite la copia o duplicación de datos).**

IPsec opera en la capa 3 del modelo osi.



#### 8.5.4. Sitio a Sitio Túnel GRE

Es una manera más aislada de armar túneles, realiza encapsulación de datos sobre otra red y la configuración se basa en direccionamiento IP privada. No encripta, admite encapsulación a nivel capa 3, no incluye mecanismos de control de flujo por defecto, tampoco tiene mecanismos de seguridad para proteger los datos, adiciona 24 bytes por tunelización de paquetes.



NOTA.- En este ejemplo primero garantizo la comunicación entre 1.1.1.1 y 2.2.2.2

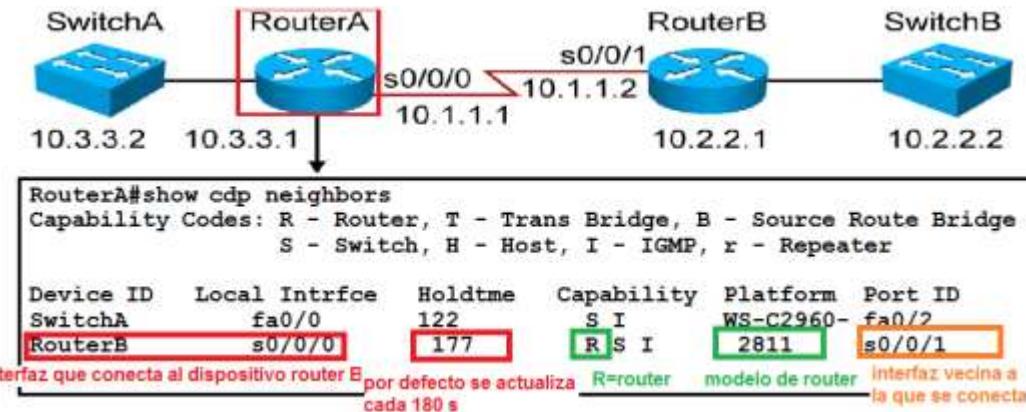
## 9.1. Administración de Routers y switch

### 9.1.1. CDP (Cisco Discovery Protocol)

Protocolo de capa 2, me permite descubrir equipos vecinos cisco desde capa 1 a capa 3, esta información incluye:

- Identifica el nombre del dispositivo
- Identifica una lista de dispositivos conectados
- Identifica los puertos local y vecino
- Identifica la plataforma (modelo del vecino)
- La capa (si es switch o router)

#Show cdp entry router “vecino”	Información específica del vecino
#Show cdp interface	Estado de los interfaces que están conectados a los vecinos
<b>#Show cdp neighbors</b>	Lista completa de los vecinos (ip vecina)
#Show cdp traffic	Estadísticas de cdp
(conf-if)#no cdp run	Deshabilita cdp en el router local
(conf-if)#interface serial 0/0/0	Deshabilitar el envío de paquetes cdp a un vecino serial 0/0/0
(conf-if)#no cdp enable	
(conf-if)# lldp run	Activa lldp neighbours
#show lldp neighbours	Ppermite descubrir vecinos de diferentes fabricantes

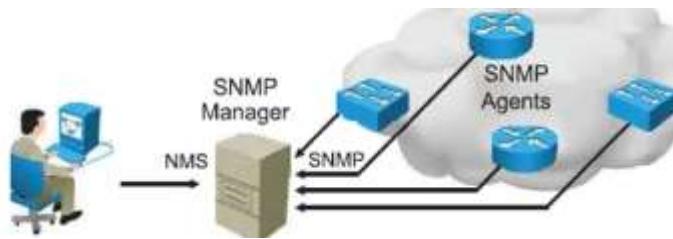


Nota.- es recomendable desactivar el cdp neighbors por temas de seguridad.

- CDP actualiza cada 180 segundos
- CDP es exclusivo de cisco, su equivalente estándar es LLDP de la IEEE

### 9.1.2. SNMP (Simple network management protocol)

Protocolo de administración de red, permite manejar reportes de forma gráfica o texto, nos muestra información del estado de los dispositivos y del tráfico que pasa por el dispositivo.

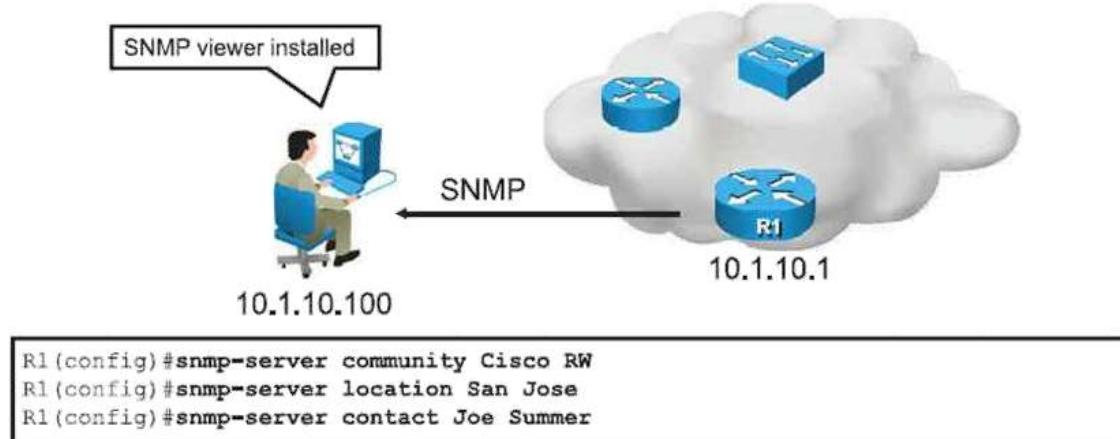


Existen tres versiones de SNMP.

- SNMPv1 y SNMPv2c, texto claro
- SNMPv3, autenticación, confidencialidad, integridad

Trabaja en base a MIB una base de datos principal basados en OIDs (identificadores de objetos) que son códigos generados representados por números.

## SNMP Configuration (Cont.)



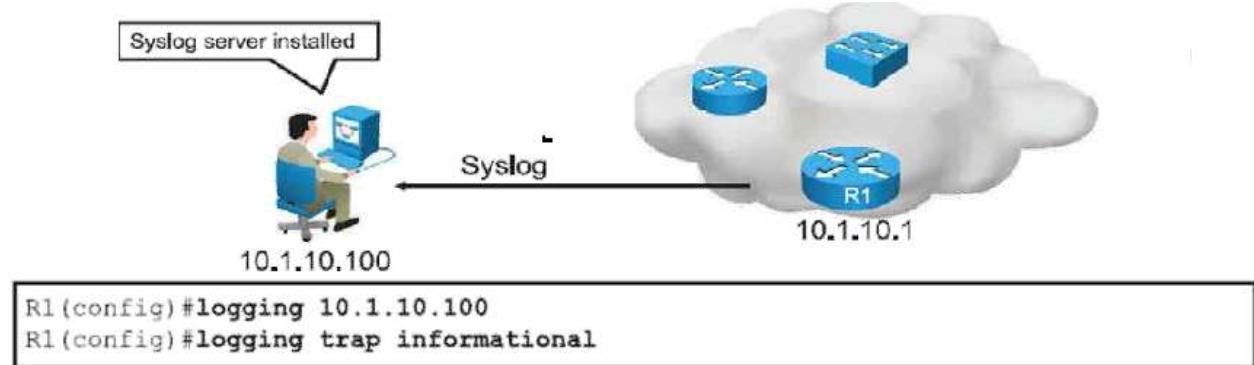
Nota: aplicativo solar wind

### 8.1.3. Protocolo de capa 7 Syslog

Mensajes de interrupción que nos permite identificar cambios en la red, (similares a los registros en Windows),

Severity Level	Explanation
Emergency (severity 0)	System is unusable
Alert (severity 1)	Immediate action needed
Critical (severity 2)	Critical condition
Error (severity 3)	Error condition
Warning (severity 4)	Warning condition
Notification (severity 5)	Normal but significant condition
Informational (severity 6)	Informational message
Debugging (severity 7)	Debugging message

Para que el servidor guarde estos mensajes se introduce el siguiente comando, con el cual mandara los mensajes del 6 (Informational) hacia arriba (hasta 0).

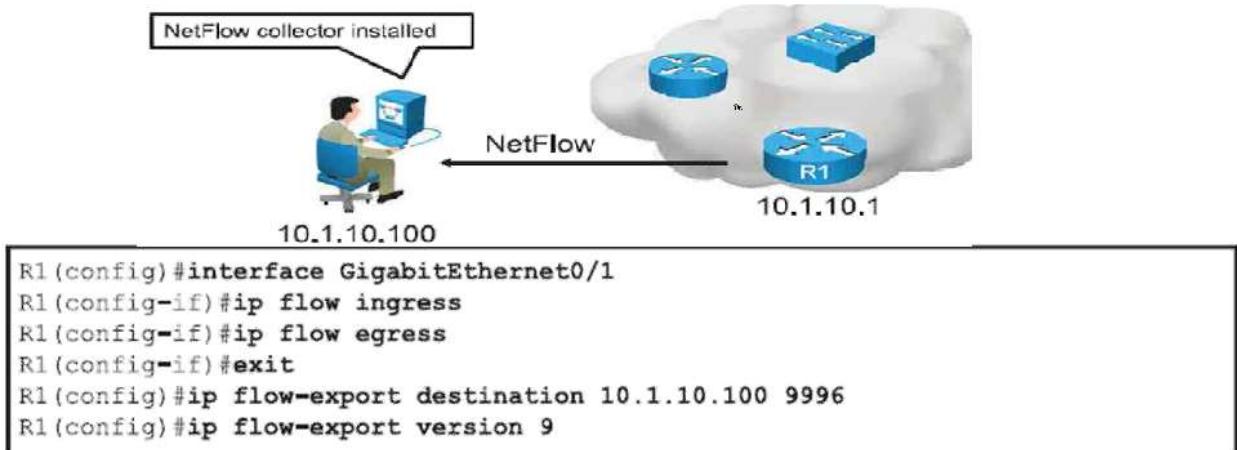


#### 9.1.4. NETFLOW

Recolecta trafico IP, habilita medidas de quien está usando recursos de red, permite identificar el tipo de tráfico que viaja por el router.

- IP origen y destino
- Puertos que se estén usando
- Protocolo de capa 3
- Tipo de servicio
- Interfaces lógicas que se estén usando

**Nota:** el router solo recolecta el dato necesita de un software para recuperar y grabar para el análisis una aplicación es el Netflow collector.



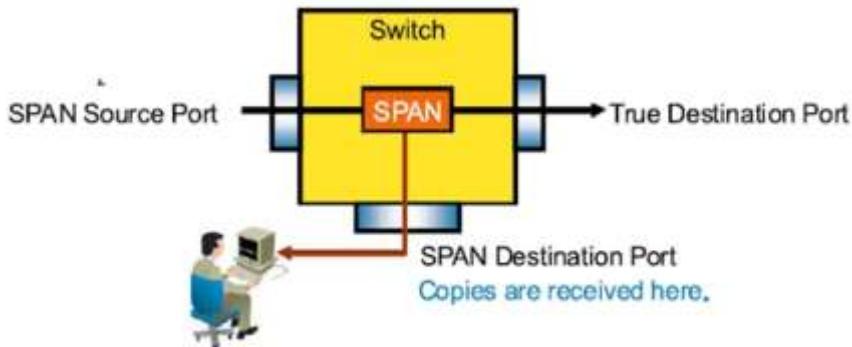
#### 8.1.5. SPAN, RSPAN, ERSPAN (Switch)

##### 8.1.5.1. SPAN

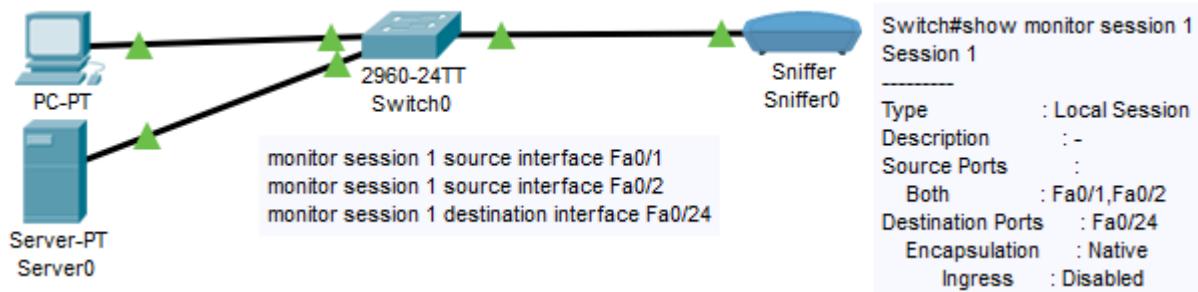
Nos permite hacer análisis de tráfico o sea que retransmite todo el tráfico de un puerto source (switch) hacia un puerto destination (router), ubicado hacia un administrador, se aplica en equipos de capa 2 y 3, envía el tráfico desde capa 2 a capa 7. Se usa para controlar el tráfico en un switch al replicarlo en otro puerto o puertos en el mismo switch

- **Ingress Traffic:** el tráfico que ingresa al switch

- **Egress Traffic:** el tráfico que sale del switch
- **Source (SPAN) port/vlan:** El puerto/puertos o VLAN que quieren ser monitoreados
- **Destination (SPAN) port:** el puerto que monitorea (tiene un sniffer instalado como wireshark).



Esta función puede usar para controlar el tráfico en un switch al replicarlo en otro puerto o puertos en el mismo switch



#### 9.1.5.2. RSPAN Remote SPAN

Se usa cuando el **source port** no está en el mismo switch otra manera de decirlo es que realiza SPAN entre switches con VLAN. Se trabaja con troncales y tiene sus propias VLANs, RSPAN no soporta BPDU ni participa en STP.

#### 9.1.6. Stackwise

Permite apilamiento de switches en una conexión de alto rendimiento (en vez de interconectarlos con ethernet). En switches 3600, 3700, 3800. Maneja Throughput (ancho de banda) 32Gbps, se apilan hasta 9 switches. El stacking permite la autoconfiguración para verse como uno solo. Se selección automática de master pudiendo usar una sola IP (tambien una sola SNMP, STP, CLI) para todo el stack, mejora el control de tráfico y proporciona redundancia



Para verificar el estado de los puertos

#Show switch stack-port

Mostrar los vecinos

#show switch neighbors

Mostrar los switch esclavos y maestros (prioridad más baja es maestro)

#Show switch

### 10.1. BGP (Border Gateway Protocol).-

Son usados por los proveedores de servicios ISP para comunicarse entre ellos su función es de conectar distintos sistemas autónomos o ISP (AS es de 16 bits de 0 – 65535, asignado por la IANA).

- BGP es multihoming (multiconexion) o sea que permite conectar 2 o más ISP
- AS, sistema autónomo colección de redes bajo una sola administración
- IGP (Interior Gateway Protocol) optimiza el enrutamiento interior-AS ospf, rip, eigrp, is-is
- EGP (exterior Gateway protocol) corre entre sistemas autónomos, habilita políticas de enrutamiento, mejora la seguridad

Se llama EBGP cuando BGP está corriendo entre routers de distinto AS, usado para redundancia y balanceo de carga, tiene una distancia administrativa de 20

Se llama IBGP cuando BGP está corriendo entre routers del mismo AS, con una distancia administrativa de 200.

- En TCP usa el puerto 179 para establecer sesión

Un sistema autónomo es un grupo de redes IP que poseen una política de rutas propia e independiente". Esta definición hace referencia a la característica fundamental de un Sistema Autónomo: realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet. Un número de AS o ASN se asigna a cada AS, el que lo identifica de manera única a sus redes dentro de Internet.

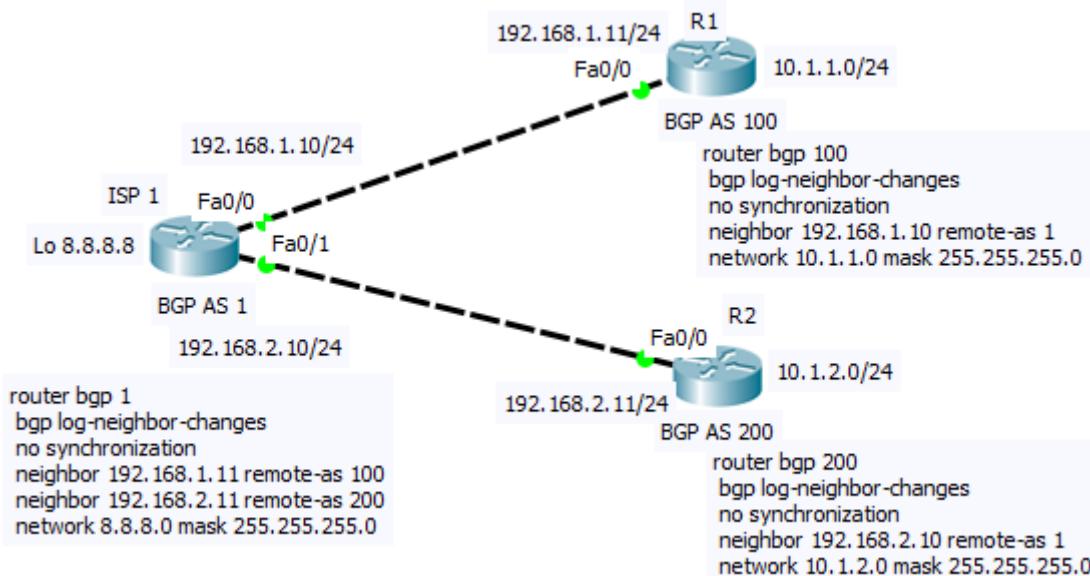
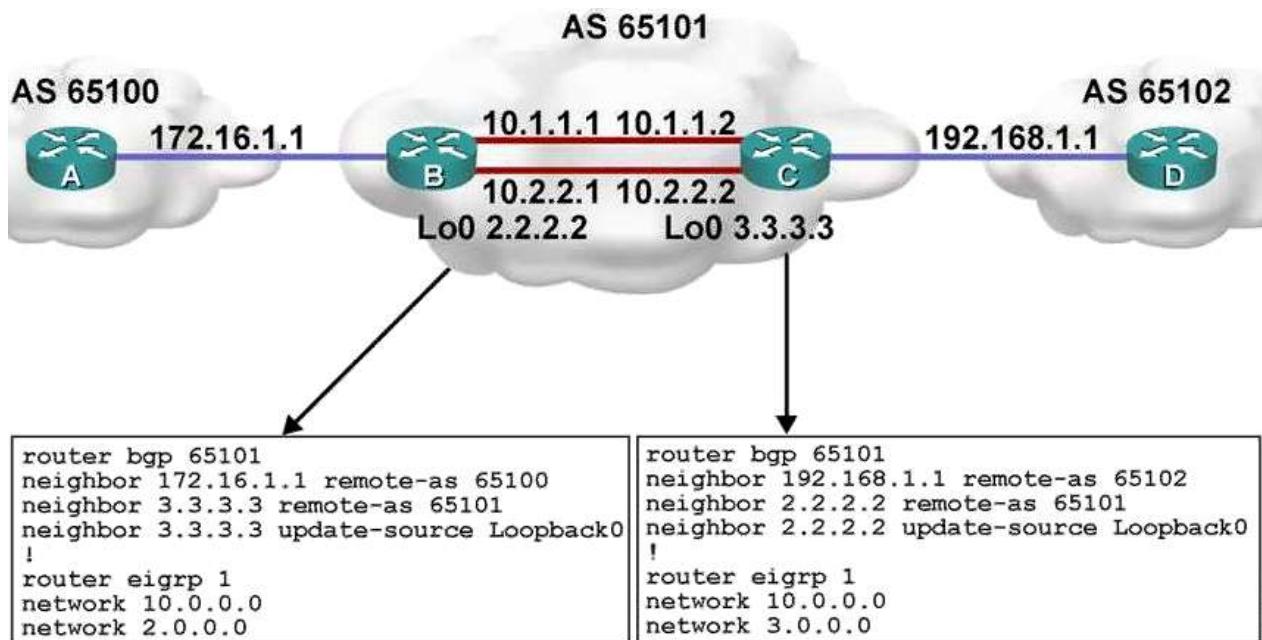
Se puede usar una ruta por defecto para salir a un ISP (solo uno) pero para diferentes ISP se debe usar BGP que trabaja con distintos AS es libre de bucles y es path-vector o distancia vector (no tiene límite de saltos).

No es apropiado para conexiones locales por el excesivo consumo de memoria y procesamiento.

Es el único que funciona bajo TCP puerto 179, se asegura hacia donde manda sus paquetes es lento comparado.

#### 10.1.1. Tablas de BGP.-

- Neighbors table. Lista de vecinos.
- BGP table. Lista de redes aprendidas, múltiples caminos y sus atributos.
- IP routing table. Table de enrutamiento.



<pre>ISP#show ip bgp summary BGP router identifier 8.8.8.8, local AS number 1 BGP table version is 4, main routing table version 6 3 network entries using 396 bytes of memory 3 path entries using 156 bytes of memory 2/2 BGP path/bestpath attribute entries using 368 bytes of memory 3 BGP AS-PATH entries using 72 bytes of memory 0 BGP route-map cache entries using 0 bytes of memory 0 BGP filter-list cache entries using 0 bytes of memory Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory BGP using 1024 total bytes of memory BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs</pre> <table border="1"> <thead> <tr> <th>Neighbor</th><th>V</th><th>AS</th><th>MsgRcvd</th><th>MsgSent</th><th>TblVer</th><th>InQ</th><th>OutQ</th><th>Up/Down</th><th>State/PfxRcd</th></tr> </thead> <tbody> <tr> <td>192.168.1.11</td><td>4</td><td>100</td><td>53</td><td>52</td><td>4</td><td>0</td><td>0</td><td>00:50:34</td><td>4</td></tr> <tr> <td>192.168.2.11</td><td>4</td><td>200</td><td>53</td><td>52</td><td>4</td><td>0</td><td>0</td><td>00:50:24</td><td>4</td></tr> </tbody> </table> <pre>ISP#show ip bgp neighbors BGP neighbor is 192.168.1.11, remote AS 100, external link   BGP version 4, remote router ID 10.1.1.1   BGP state = Established, up for 00:53:03   Last read 00:53:03, last write 00:53:03, hold time is 180, keepalive interval is 60 seconds   Neighbor capabilities:     Route refresh: advertised and received(new)     Address family IPv4 Unicast: advertised and received   Message statistics:     InQ depth is 0     OutQ depth is 0</pre>	Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd	192.168.1.11	4	100	53	52	4	0	0	00:50:34	4	192.168.2.11	4	200	53	52	4	0	0	00:50:24	4	<pre>ISP# show ip route Gateway of last resort is not set    8.0.0.0/24 is subnetted, 1 subnets C     8.8.8.0 is directly connected, Loopback0   10.0.0.0/24 is subnetted, 2 subnets B       10.1.1.0 [20/0] via 192.168.1.11, 00:00:00 B       10.1.2.0 [20/0] via 192.168.2.11, 00:00:00 C     192.168.1.0/24 is directly connected, FastEthernet0/0 C     192.168.2.0/24 is directly connected, FastEthernet0/1</pre>
Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd																						
192.168.1.11	4	100	53	52	4	0	0	00:50:34	4																						
192.168.2.11	4	200	53	52	4	0	0	00:50:24	4																						

## 11.1 Software defined network SDN

La automatización de la administración de las redes, es un acercamiento centralizados para aprovisionar administrar y programar redes. Elimina las tareas repetitivas, no es necesario configurar equipo por equipo, upgrade masivos, reducción del tiempo de troubleshooting.

**Redes basados en controladoras:** controla todos los dispositivos tal como ICY o DNA center, permite administrar o programarlo de manera centralizada.

### 11.1.1. Overlay y Underlay y Fabric

Una red **Underlay** es una infraestructura Fisica-logica sobre la cual la red Overlay esta construida. Es la red subyacente responsable de la entrega de paquetes a través de las redes. Una red **Overlay** es una red Virtual construida sobre la red Underlay. **Fabric** es el conjunto de estos elementos mas el APIC.

Parameter	Underlay Network	Overlay Network
<b>Philosophy</b>	Underlay Network is physical infrastructure above which overlay network is built.	An Overlay network is a virtual network that is built on top of an underlying Network infrastructure/Network layer (the underlay).
<b>Related protocols</b>	Ethernet Switching, VLAN , Routing etc.	VXLAN , OTV , VPLS
<b>Scalability</b>	Less Scalable due to technology limitation	Designed to provide more scalability than underlay network. For e.g. – VLAN (underlay Network) provides 4096 Vlan support while VXLAN (Overlay Network) provides upto 16 million identifiers.
<b>Packet control</b>	Hardware orchestrated	Software orchestrated
<b>Packet delivery</b>	Responsible for delivery of packets	Offloaded from delivery of packets
<b>Packet encapsulation and overhead</b>	Packet delivery and reliability occurs at layer 3 and Layer 4	Needs to encapsulate packets across source and destination, hence incurs additional overhead.
<b>Managing multitenancy</b>	NAT or VRF based segregation required which may face challenge in big environments	Ability to manage overlapping IP addresses between multiple tenants.
<b>Multipath forwarding</b>	Less scalable options of multipath forwarding. Infact using multiple paths can have associated overhead and complexity.	Support for multi-path forwarding within virtual networks.
<b>Deployment time</b>	Less scalable and time consuming activity to setup new services and functions	Ability to rapidly and incrementally deploy new functions through edge-centric innovations
<b>Traffic flow</b>	Transmits packets which traverse over network devices like Switches and Routers.	Transmits packets only along the virtual links between the overlay nodes.