

Contenido

CISCO CCNA 200-301	4
002 Conceptos basicos de redes	4
003 Que es un switch.....	7
004 Que es un Router	8
005 Firewalls de nueva generación (NGF) e IPS.....	11
006 Endpoints o dispositivos finales	13
007 Puntos de Acceso o Access Points.....	15
008 Redes SOHO.....	18
009 Servicios en Sitio o en la nube	19
010 Principios de WiFi.....	20
011 Conceptos básicos de cableado	23
012 Tabla de direcciones MAC	26
03 Fundamentos Topologias y Arquitecturas	28
013 Introducion a Wide Area Network (WAN).....	28
014 Topologias de Red 2 Niveles y 3 Niveles.....	30
04 Fundamentos de Redes Introduccion al Laboratorio y equipo Cisco.....	31
017 Introduccion a Cisco IOS.....	31
018 Secuencia de inicio de los equipos	32
019 Sistema de Archivos de los equipos	33
05 Fundamentos Direccionamiento IPv4	36
020 IPv4Introduccion	36
021 IPv4Mascara y subredes	38
022 IPv4 VLSM Parte 1	43
023 IPv4 VLSM Parte 2	49
06 Fundamentos Direccionamiento IPv6	53
024 IPv6Introduccion a direcciones IPv6	53
025 IPv6 Tipos de Direcciones.....	57
027 IPv6 Configuracion basica de direcciones IPV6	59
034 LLDP.....	60

035 Introduccion a Etherchannel.....	60
037 Introduccion a Spanning Tree Protocol – STP	61
039 STP Portfast	62
040 Configuracion de SPAN.....	63
041 StackWise.....	65
042 DTP.....	66
08 Conectividad IP	66
043 Introducion a routing.....	67
044 Rutas Estaticas.....	68
045 Enrutamiento Dinamico	70
046 OSPF Conceptos basicos	75
047 OSPF Configuracion basica de OSPF area 0	77
048 OSPF Router ID	78
049 OSPF Areas	78
051 OSPF Metrica	82
052 OSPF Tipos de paquetes	85
053 OSPF Tipos de SLAs	89
055 First Hop Redundancy Protocol Introduccion a HSRP y VRRP	93
056 OSPF v3	97
09 Servicios IP	99
057 DHCP	99
058 NAT Introduccion a NAT y PAT	101
063 Acceso remoto por SSH	109
10 Seguridad	110
065 Conceptos basicos de seguridad	110
066 Elementos de un programa de seguridad	112
067 Elementos de las politicas de seguridad sobre claves	114
068 ACLs Introduccion a listas de acceso	116
069 ACLs Listas de acceso Standard	120
070 ACLs Listas de acceso Extendidas	123
071 AAA Tacacs y Radius	125
072 Seguridad de Capa 2 Port Security	128

073 Control de acceso Asegurando la consola del equipo	129
074 Seguridad de Capa2 DHCP Snooping	130
11 Automatizacion y Programacion orientado a Redes.....	130
075 SDN Automatizando la administracion de las redes	130
076 Redes tradicionales versus redes basadas en controladoras	132
077 Conceptos de Overlay Underlay y Fabric.....	133

CISCO CCNA 200-301

002 Conceptos basicos de redes

QUE ES UNA RED

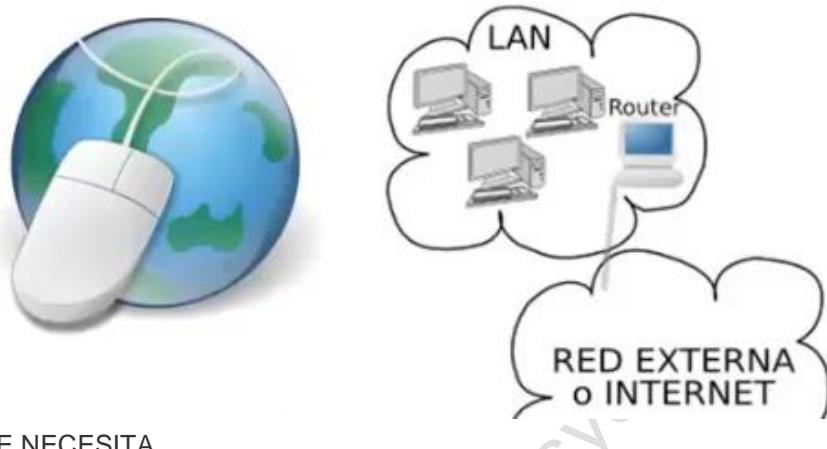
- Cuando hablamos de una red en informática nos referimos a dos o mas computadoras conectadas para compartir información.



POR QUE NECESITAMOS UNA RED?

https://bloginfo...

- Necesidad de comunicarnos
 - Email, navegación web, llamadas telefónicas por ip, transferencia de documentos, socializar etc
 - Nivel personal y empresarial



QUE SE NECESA

- Hosts: PCs, Notebooks, impresoras, Tablets, Teléfonos Inteligentes, etc
- Cable o wireless
- Dispositivo para concentrar conexiones: hub o switch? y/o punto de acceso inalámbrico
- Enrutador o router para acceso a “otras” redes



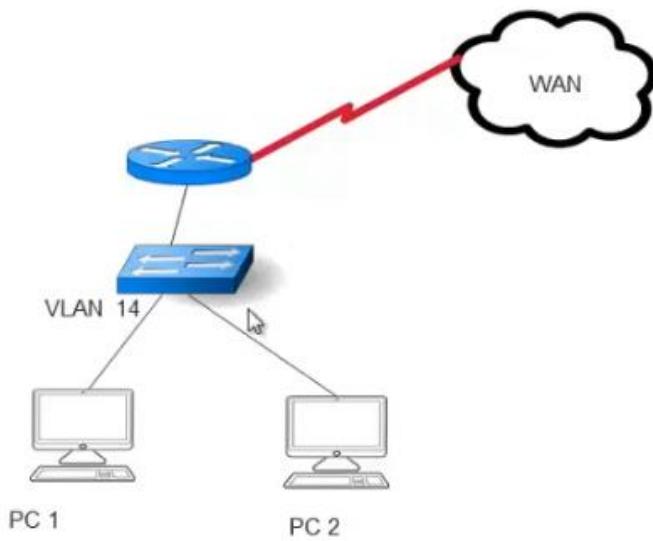
SIMBOLOGIA E ICONOS



TOPOLOGIA LOGICA

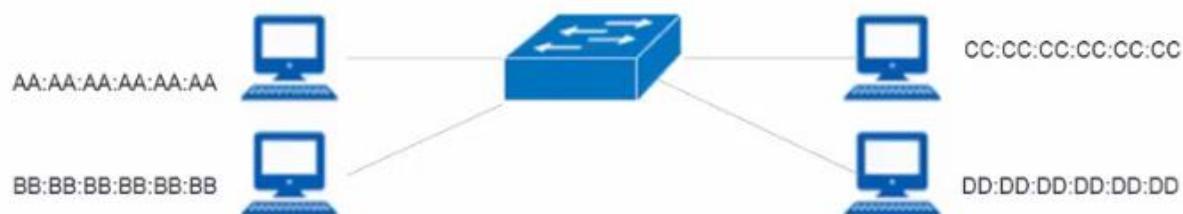
https://bloginformatico.com

Representación grafica de como se conectan los componentes de la red



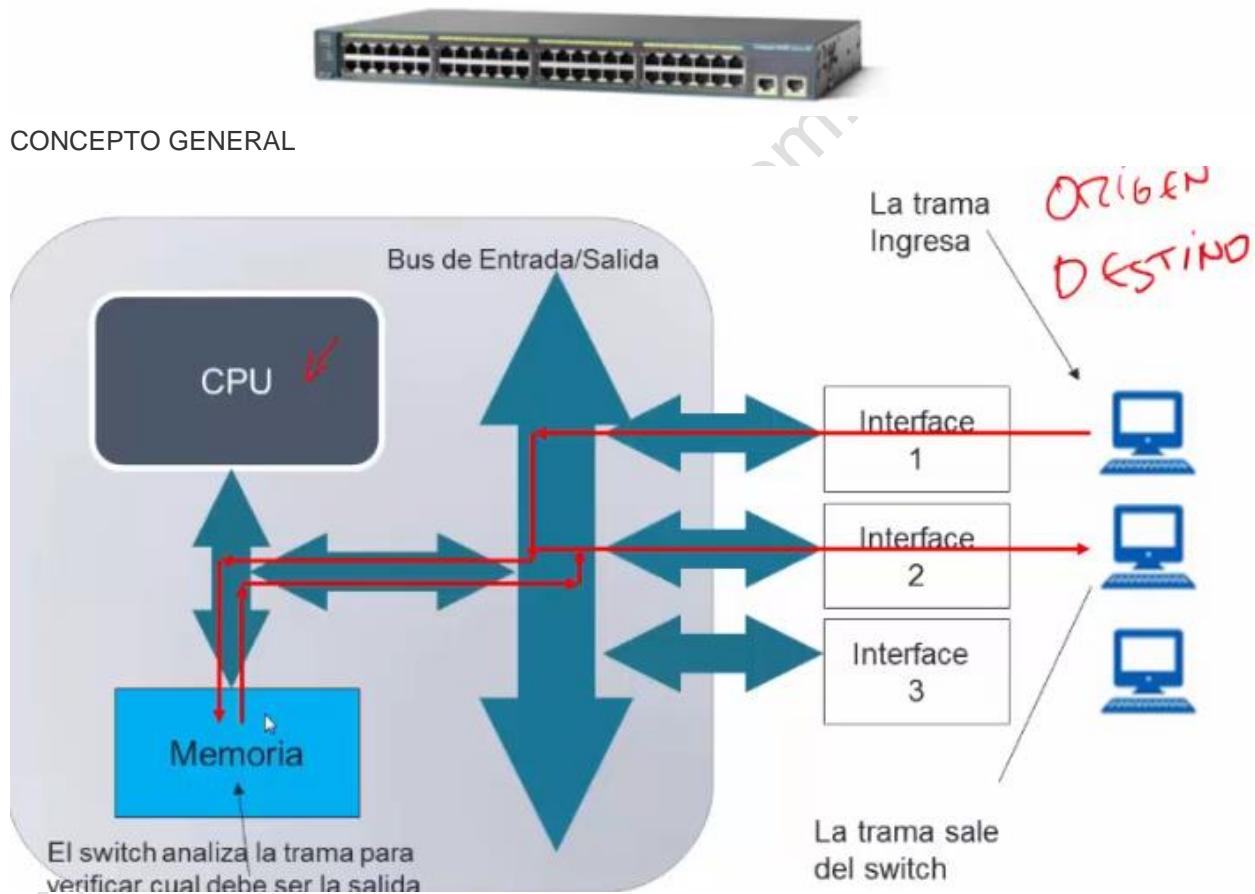
003 Que es un switch

- Compuestos por Hardware (CPU, Memoria, ASICs) y Software = IOS
- Ejecuta la conmutación basado en la dirección MAC de los dispositivos.
- Conecta los dispositivos finales a la red
- Opera en la Capa 2 del Modelo de Referencia OSI
- Construye una tabla de direcciones MAC (MAC Address Table)



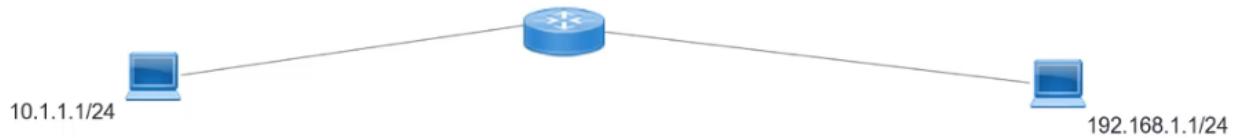
CARACTERISTICAS

- Es un Bridge multipuerto.
- Densidad de puertos
- Soportan diferentes tipos de velocidades (10Mbps, 100Mbps, 1000Mbps, 10Gbps, 40Gbps)
- Soportan VLANs (Virtual LANs)
- Separa cada puerto en un dominio de colisión (24 puertos = 24 dominios de colisión)



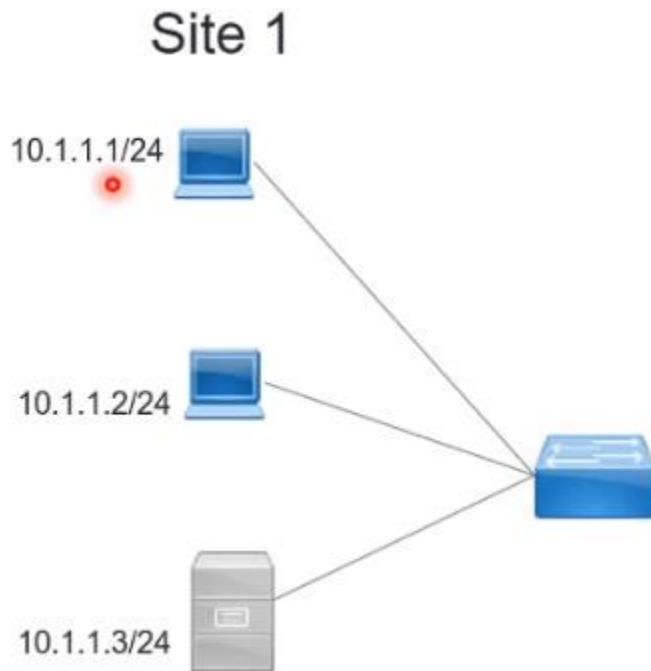
004 Que es un Router

Un router lo que nos permite basicamente es comunicar dos redes diferentes

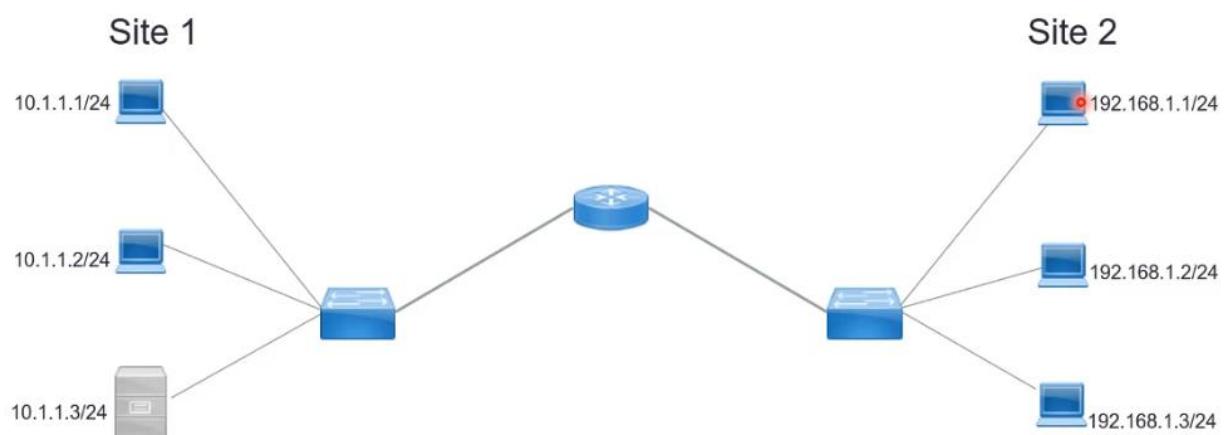


Su función básica y principal es la de comunicar dos redes completamente diferentes.

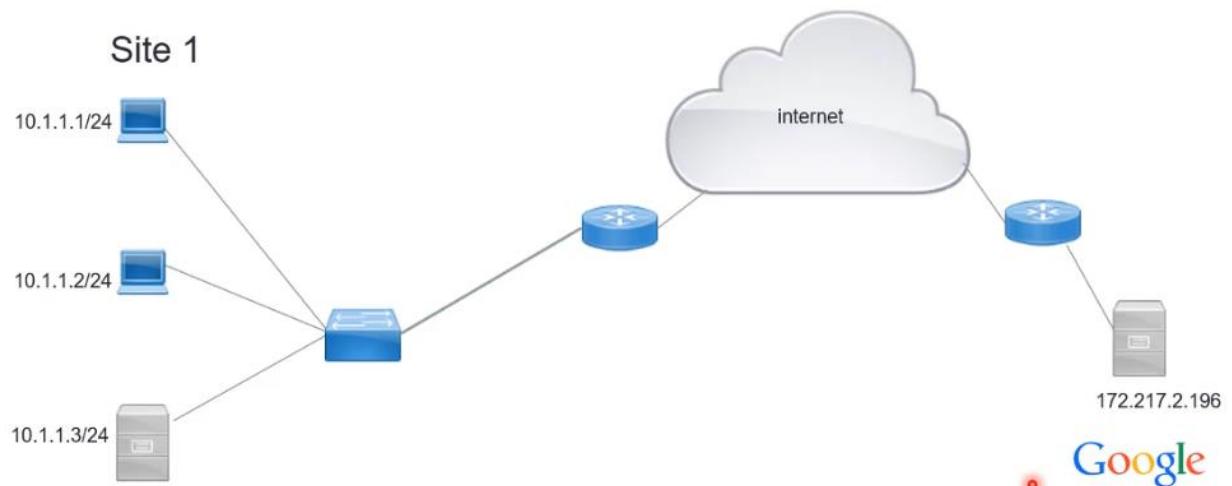
Entonces cuando tengamos una comunicación LAN básica no necesitamos un router



Pero en este caso si vamos a tener la necesidad de un enrutador



También necesitaremos de un router en el siguiente caso

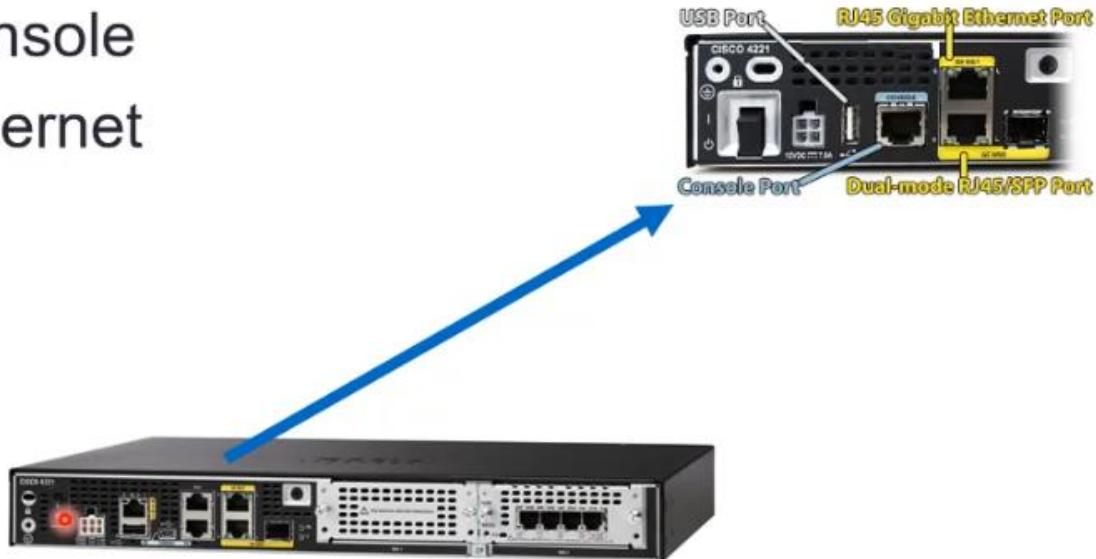


Para comunicación entre redes diferentes
 Nos referiremos a enruteadores empresariales
 Vemos como es físicamente el enruteador



Puertos básicos del enruteador

- USB
- Console
- Ethernet



Modulos e interfaces del router

- Gran Variedad
- Ethernet
- Voz
- Wireless
- Serial/Async
- Broadband/ADSL



005 Firewalls de nueva generación (NGF) e IPS

Básicamente un firewall es un dispositivo que va a monitorear el tráfico que ingresa o sale de nuestra red

- Cisco ASA
- Cisco Firepower



Que es un IPS

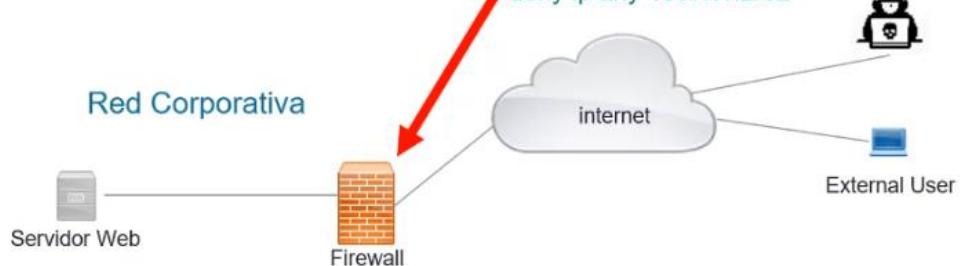
- Sistema de Prevención de Intrusos = Intrusion Prevention System
- Examina el trafico para determinar patrones de ataques
- Se basa en “firmas” de ataques conocidos
- DEBE estar actualizado constantemente
- Utiliza Deep Packet Inspection

Tipos de firewall

- Basados en la inspección de dirección IP, Puerto y/o protocolo
- Header o Encabezado del Paquete
- Utilizan listas de acceso (ACLs)
- State Less
- Capa 3-4

ACL:

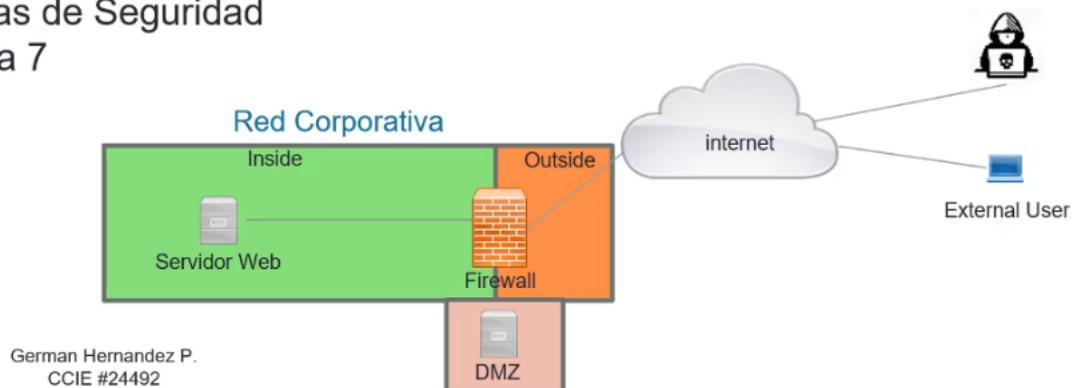
```
permit ip any 155.1.1.1/32
permit tcp any 156.1.12/32 eq 80
deny ip any 155.1.1.2/32
```



Stateful

Tipos de firewall: Stateful FW

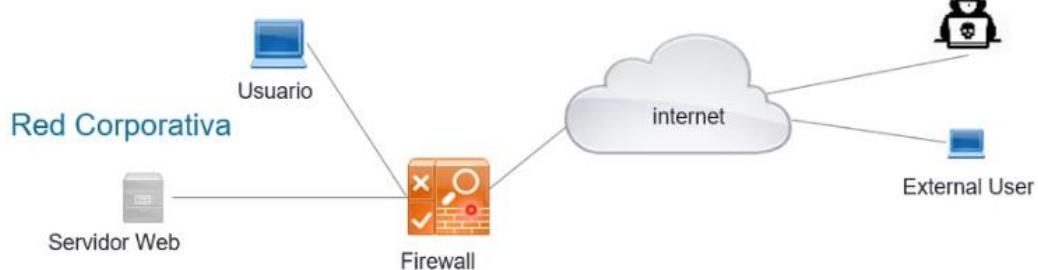
- Conocidos como los Firewall Tradicionales
- Stateful = Revisa conexiones
- SPI (State Packet Inspection)
- Tabla de estados
- Zonas de Seguridad
- Capa 7



Next generation

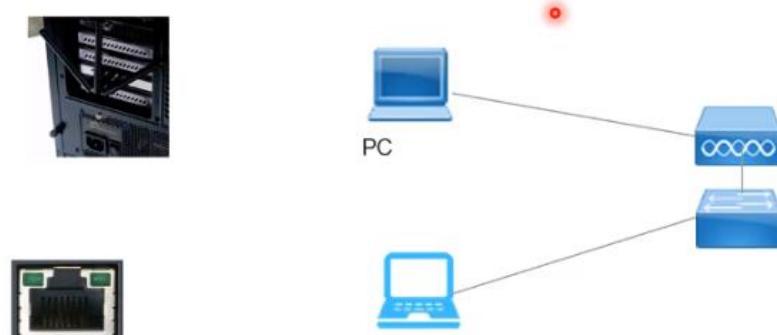
Next Generation FW

- Stateful
- Visibilidad y control de aplicaciones
- IPS (Intrusion Prevention System)
- Advanced Malware Protection (AMP)
- Filtro de URL
- VPN



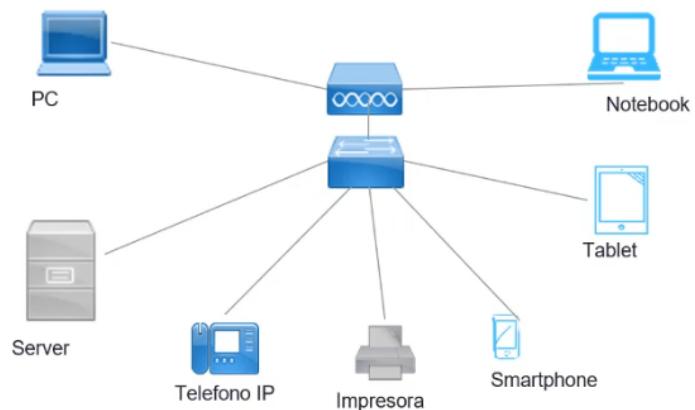
006 Endpoints o dispositivos finales

- Conocido como host
- Cualquier dispositivo que requiera acceso a la red.
- Debe tener Tarjeta de Red y un protocolo de red (Ej. Dirección IP)



Cuales serian una endpoints

- PC
- Portátiles
- Servidores
- Tablets
- Smartphones
- Impresoras
- Teléfonos IP
- Estaciones de trabajo



Otros tipos de endpoints

- POS
- PLC
- Basureros inteligentes
- Parquimetros
- Autos con WiFi
- Controladores de dispositivos en casa
- Alexa/Google Home



German Hernandez P.

007 Puntos de Acceso o Access Points

Que es un Access Point?



- Dispositivo que interconecta hosts de forma inalámbrica para formar una red inalámbrica o wireless LAN (WLAN).
- Conocido también como AP (access point) o WAP (Wireless AP)

Características

- **Protocolo 802.11**

- 802.11g = 54 Mbps
- 802.11n = 600 Mbps
- 802.11ac = 1.3 Gbps

- **Bandas**

- 2.4 Ghz
- 5.0 Ghz

- **SSID (Service Set IDentifier)** identificador de paquetes de servicio

Categorías de acces point

- **Autónomos**

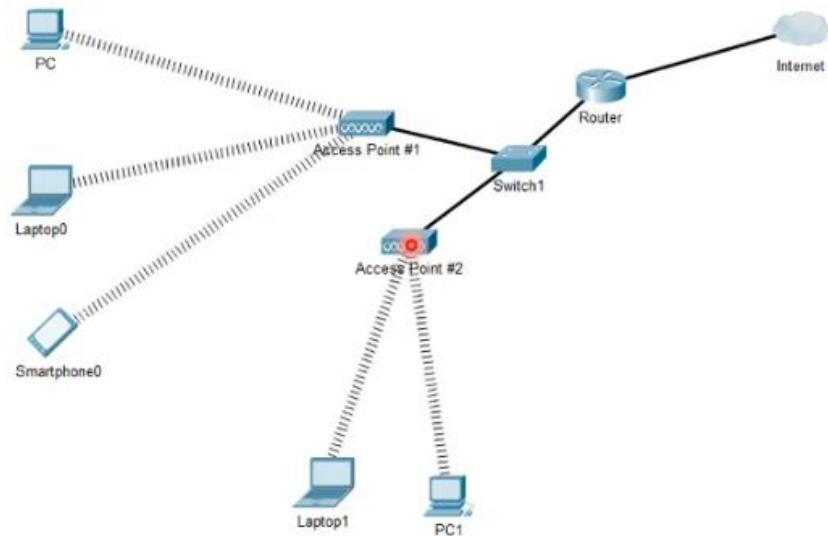
- Administrados individualmente

- **Lightweight**

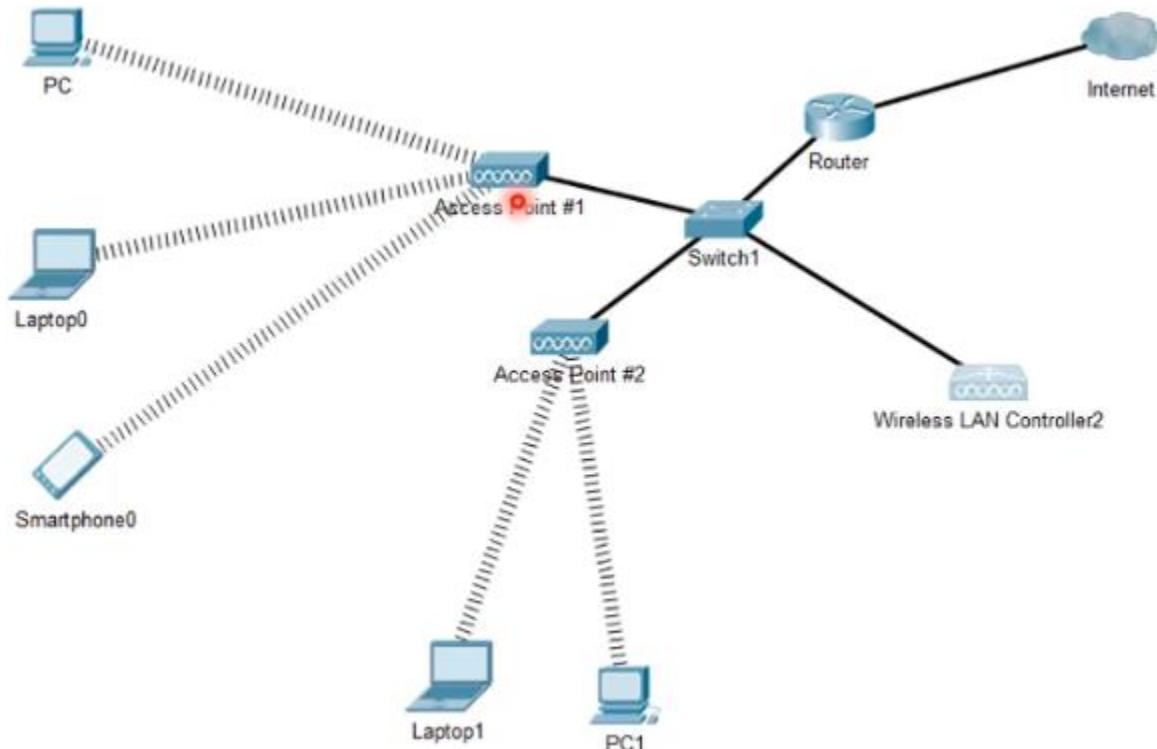
- Requieren una controladora:
 - Wireless Lan Controller
 - La WLAN Cambia Dinámicamente
 - Mas usados en la redes empresariales

Acces point autónomo

- Administrado de forma individual



Acces point administrado por controladora



Tipos de Access point

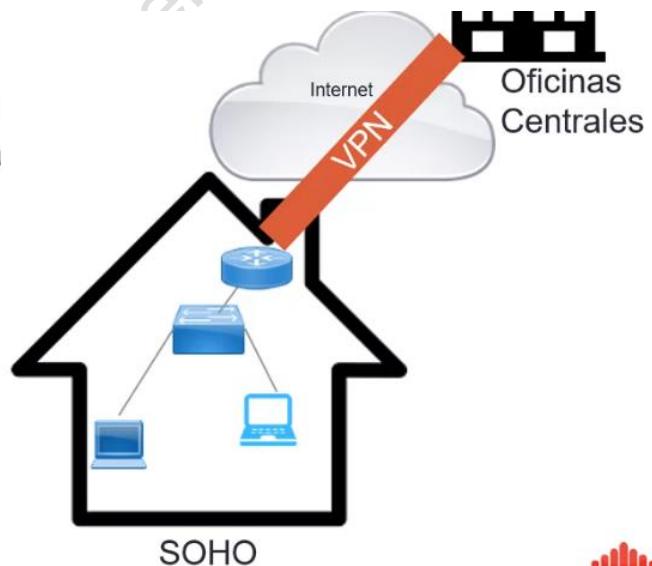
- Interiores (Indoor)
- Exteriores (Outdoor)



008 Redes SOHO

Que es una red SOHO

- Oficinas pequeñas o usuarios que necesitan conectarse al sitio central
- Generalmente utilizan internet y una Red Virtual Privada (VPN)
- Generalmente de 1 a 10 usuarios



German Hernandez P.
CCIE #24492

Características

- Usan conexiones de Banda Ancha

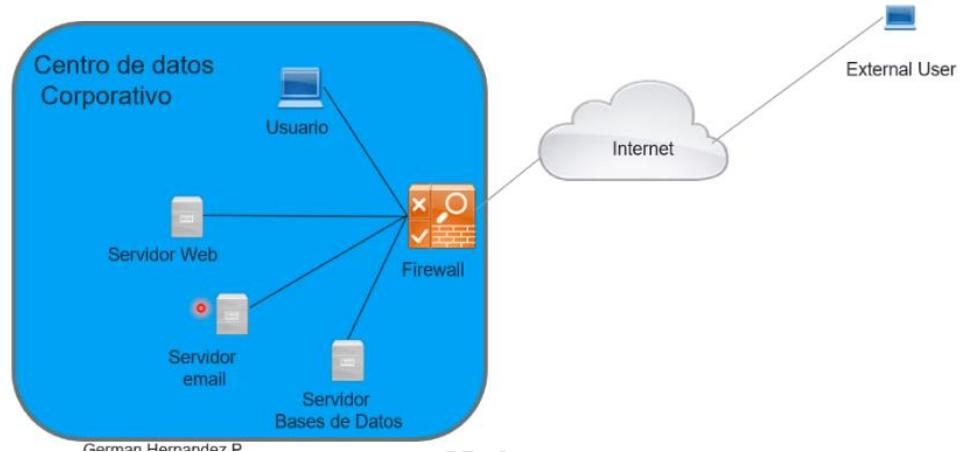
- Cable Modem
- ADSL
- FTTH (Fibra Optica)

- Pocos usuarios

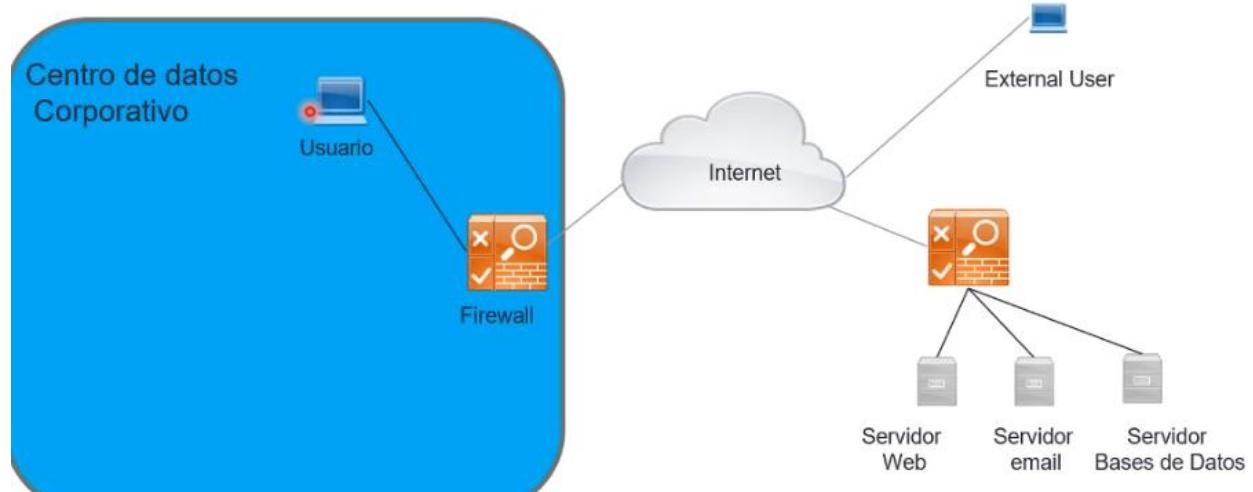
- Cableadas o Wifi

009 Servicios en Sitio o en la nube

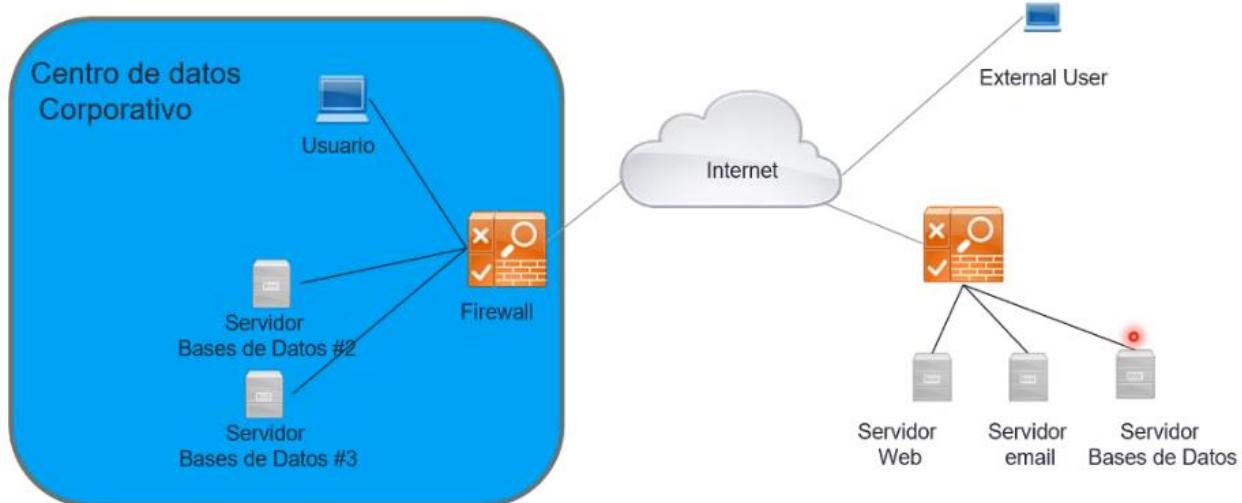
SITIO



En la nube



Mixto sitio y nube



Nube publica o nube privada

Nube Pública:

- Amazon Web Services
- Google Cloud
- Microsoft Azure

Nube Privada

- Hosting
- Colocation



010 Principios de WiFi

Wifi estándar 802.11

802.11

- Desarrollado por IEEE (Institute of Electrical and Electronics Engineers)
- Sub estandares
 - 802.11b (11 Mbps usando spectro 2.4 GHz)
 - 802.11a (54 Mbps usando spectro 5 GHz)
 - 802.11g (54 Mbps usando spectro 2.4 GHz spectrum)
 - 802.11n (300 Mbps usando spectro 2.4 GHz y 5 GHz o ambos).



Tabla frecuencia que operan

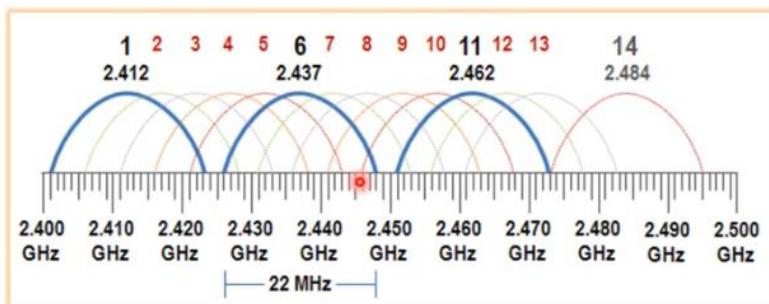
Estandar	Frecuencia	Velocidad Maxima	Compatibilidad	Estado actual
802.11b	2.4 GHz	11 Mbps	802.11g	Obsoleto
802.11a	5 GHz	54 Mbps	802.11n (5 GHz)	Obsoleto
802.11g	2.4GHz	54 Mbps	802.11b (11 Mbps)	Actual
802.11n	2.4 GHz o 5 GHz	300 Mbps	802.11g (a 54 Mbps) 802.11b (a 11 Mbps) 802.11a (a 54 Mbps a 5 GHz)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

Frecuencia 2.4

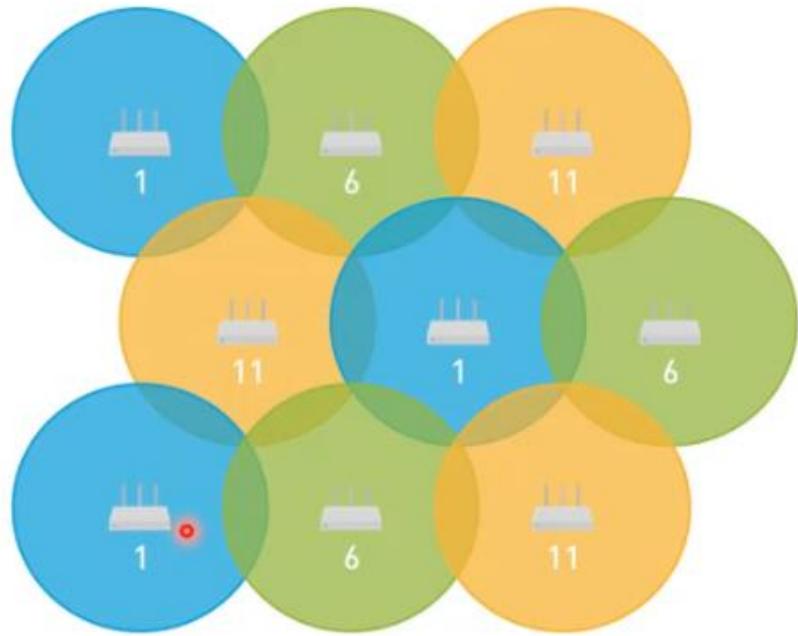
Frecuencias 2.4Ghz non-overlapping

- 2.4Ghz

- Se divide en 14 frecuencias de las cuales se usan 11
- Canales 1, 6 y 11 se recomiendan para evitar “overlapping”



Ejemplo:



Frecuencia 5.0

Frecuencias 5.0 Ghz non-overlapping

- 5.0Ghz

2.4 GHz (802.11b/g/n)



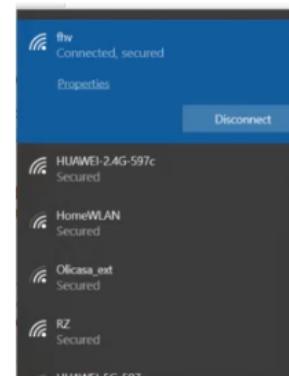
5 GHz (802.11a/n/ac)



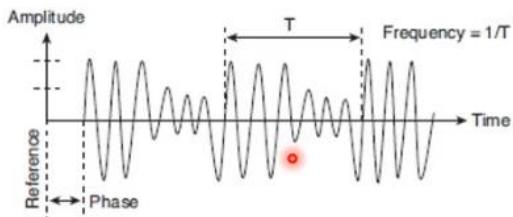
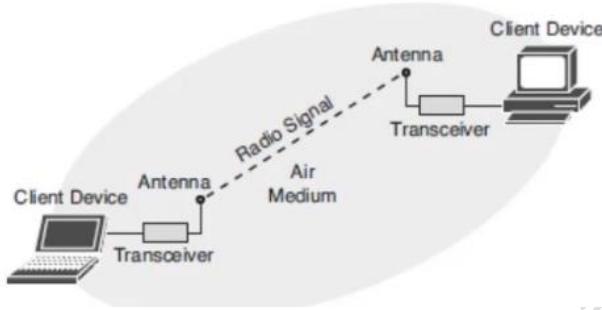
SSID

https://brandonmiller.com

- Service Set Identifier o identificador de paquetes de servicio
- Identifica la red Wireless
- 32 caracteres ASCII



Radio frecuencia



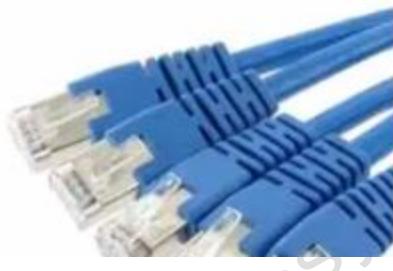
Encriptacion

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)
WPA/WPA2-PSK (TKIP / AES)	Permite WPA y WPA2 con TKIP y AES.

011 Conceptos básicos de cableado

Cables de cobre

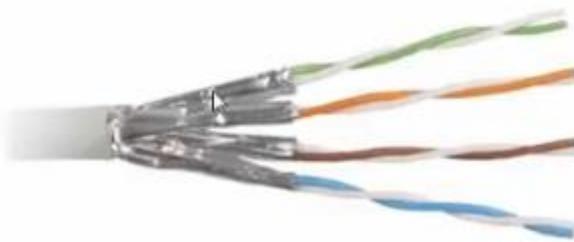
- Capa 1 del modelo de referencia OSI
- Coaxial
- Twisted Pair
 - UTP: Unshielded Twisted Pair
 - STP: Shielded Twisted Pair



- UTP

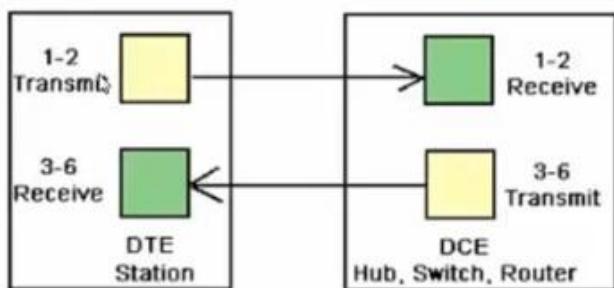


- STP



Transmisión de datos usando cables de par trenzado

- Se envían datos por un cable de cobre
- Se usan impulsos eléctricos
- Se convierte los impulsos eléctricos en unos (1s) y ceros (0s)
- El par trenzado ayudan a cancelar el ruido electrico



Fibra óptica

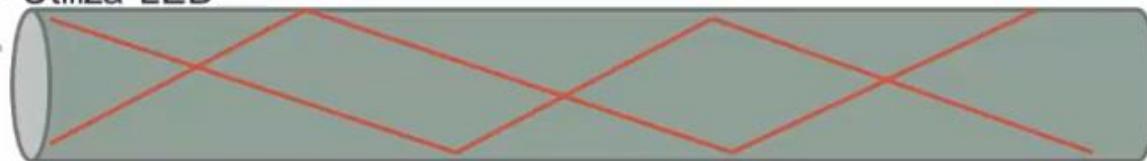
• Monomodo (SMF=Single Mode Fiber)

- Utiliza laser
- Largas Distancias
- – No le afecta el "ruido" eléctrico



• Multimodo (MultiModeFiber=MMF)

- Utiliza LED



Tipos de conectores de fibra

GBICs y SFP Ethernet

Gigabit Interface Converter
GBIC



Small Form Factor Pluggables
SFP

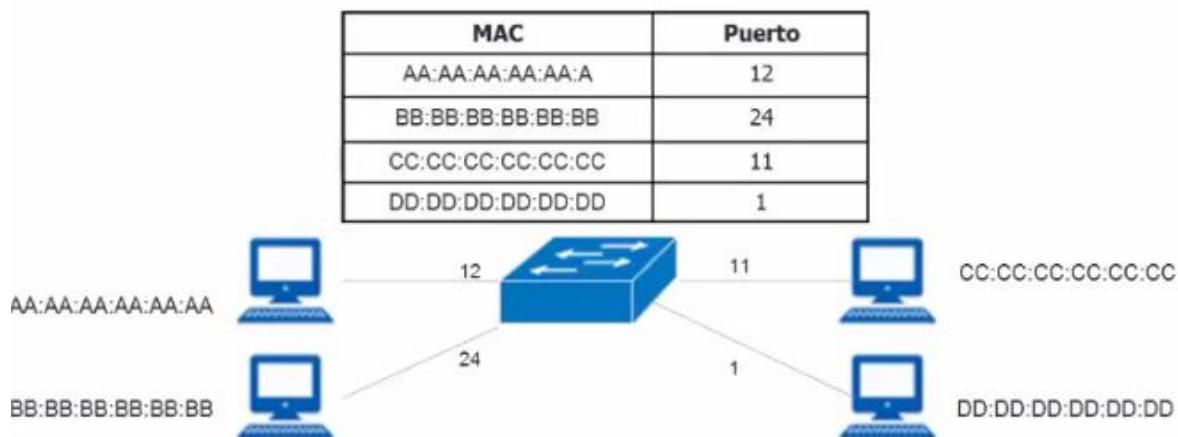


012 Tabla de direcciones MAC

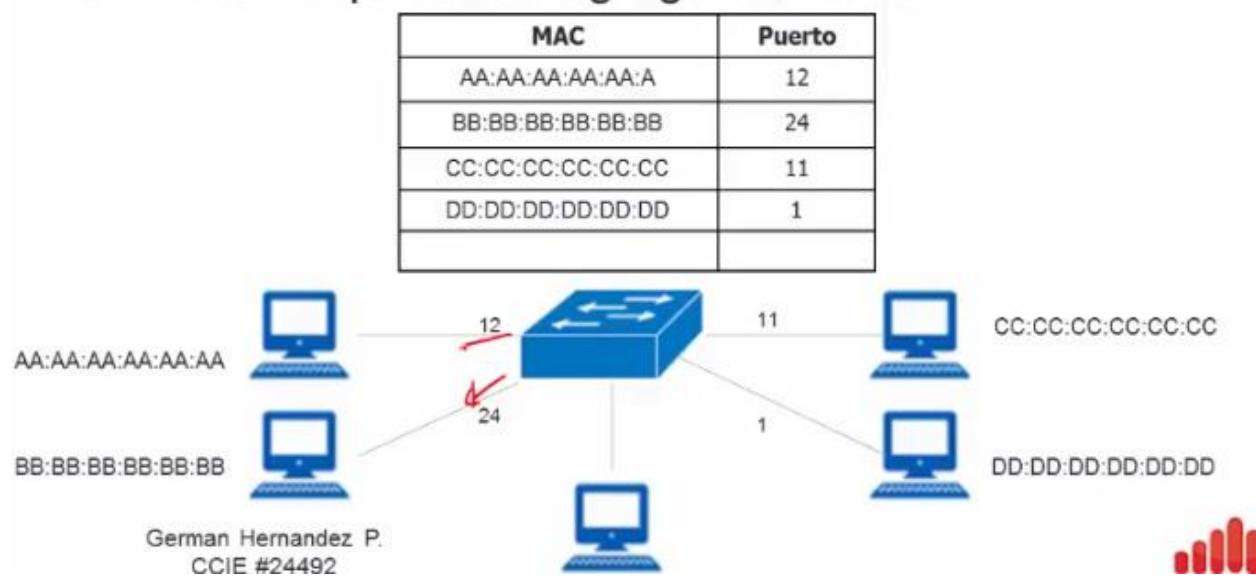
https://bloginformaticasy

MAC ADDRESS TABLE

- Inicialmente la **CAM** (Content Addressable Memory) esta vacía
- El switch va llenando dicha memoria analizando el MAC origen de las tramas que llegan a cada puerto



- Que sucede si llega una trama para una dirección MAC que no esta en la tabla?
- Se envía a todos los puertos
- Si el host responde se agrega a la tabla



- Las entradas al switch que no tienen actividad se eliminan
- Este temporizador es de 300 segundos
- Cuando el switch coloca una entrada en la CAM este temporizador se inicia
- La eliminación se conoce como descarte por antigüedad

03 Fundamentos Topologias y Arquitecturas

013 Introducion a Wide Area Network (WAN)

Wide Area Network o Redes de Area Ancha o extensa



Característica

Opera mas allá del alcance de una LAN
Se usa para interconectar un sitio central por ejemplo con sus sucursales o sitios remotos
También usado para empleados remotos
Le pertenecen a un Proveedor de Servicios
La empresa debe pagar por el servicio



Topología

Punto a punto (point to point)
Hub and Spoke
Full Mesh

Términos wan

CPE (Customer Premises Equipment)

Punto de Demarcación

Local Loop

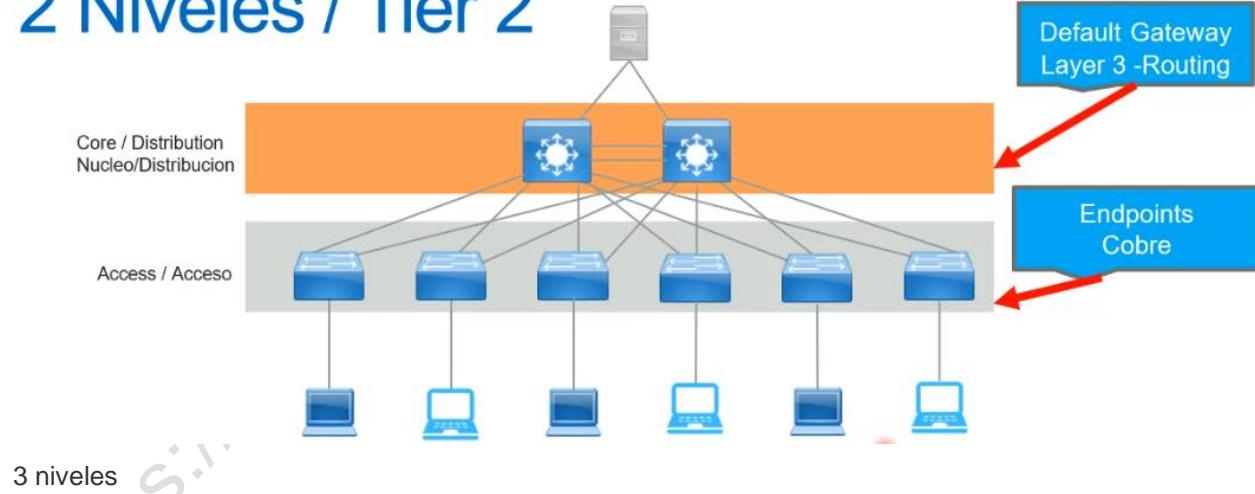
Central Office



014 Topologías de Red 2 Niveles y 3 Niveles

2 niveles

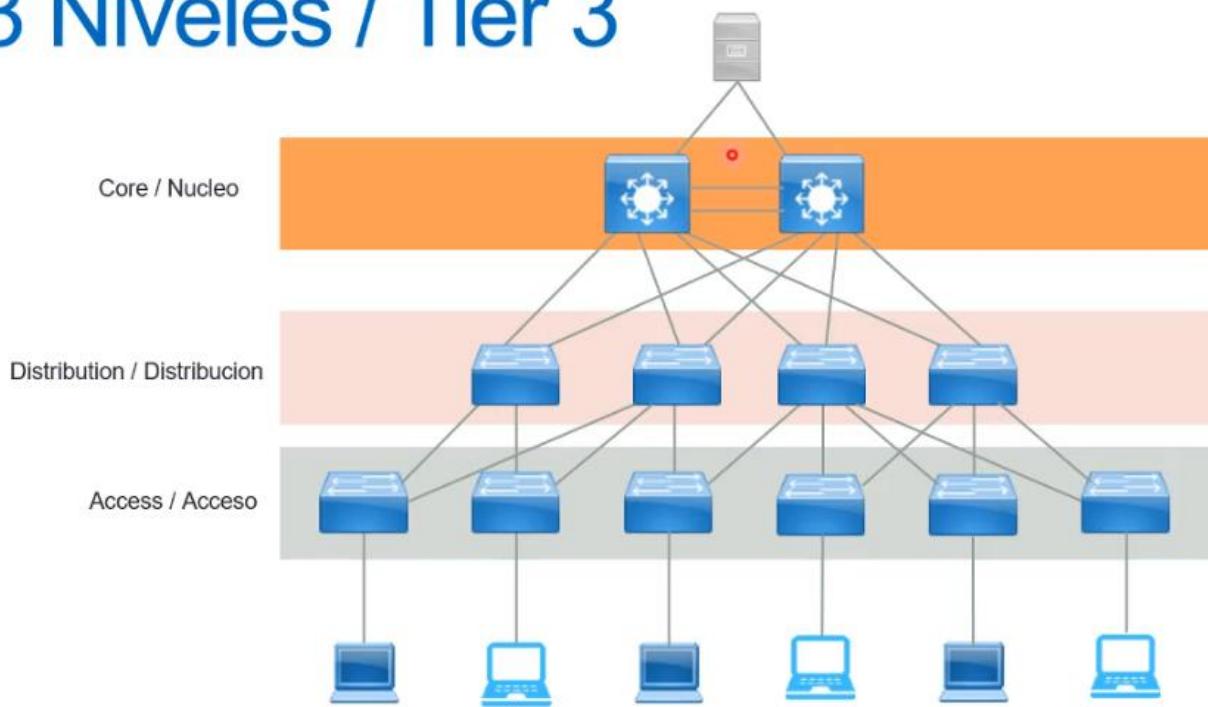
2 Niveles / Tier 2



3 niveles

https://

3 Niveles / Tier 3



04 Fundamentos de Redes Introducción al Laboratorio y equipo

Cisco

017 Introducción a Cisco IOS

Que es IOS?

- Cisco le llama a su Sistema Operativo **Internetwork Operating System** o Cisco **IOS**.
- Es el sistema operativo nativo de la mayoría de routers y switches Cisco.
- Utiliza una línea de comandos CLI (Command Line Interface) para su configuración
- Permite que el administrador verifique el estado del equipo y lo configure.



Características

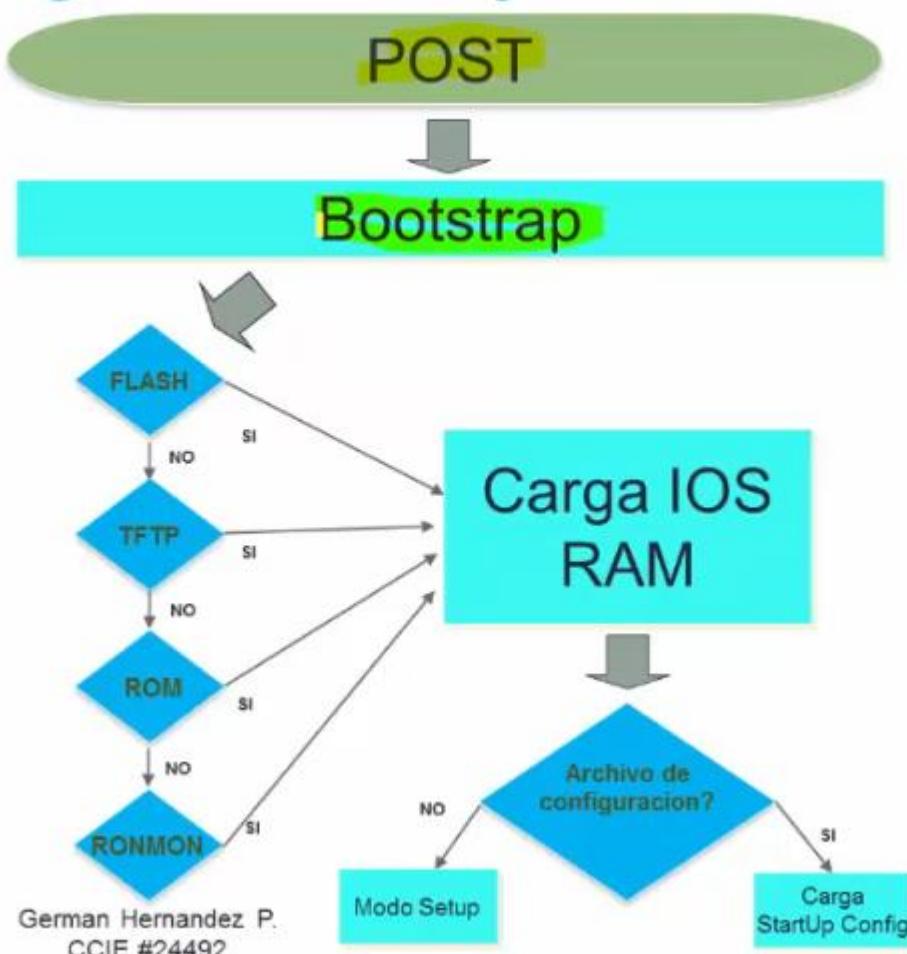
- Se divide en paquetes o features
 - IP Data (INCLUIDO)
 - IP SLAs, IPX, L2TPv3, Mobile IP, MPLS,etc
 - Security (OPCIONAL)
 - VPN, Firewall, IP SLAs, NAC
 - Unified Communications (OPCIONAL)
 - CallManager Express, Gatekeeper, H.323, IP SLAs, MGCP, SIP, VoIP

Secuencia de Arranque

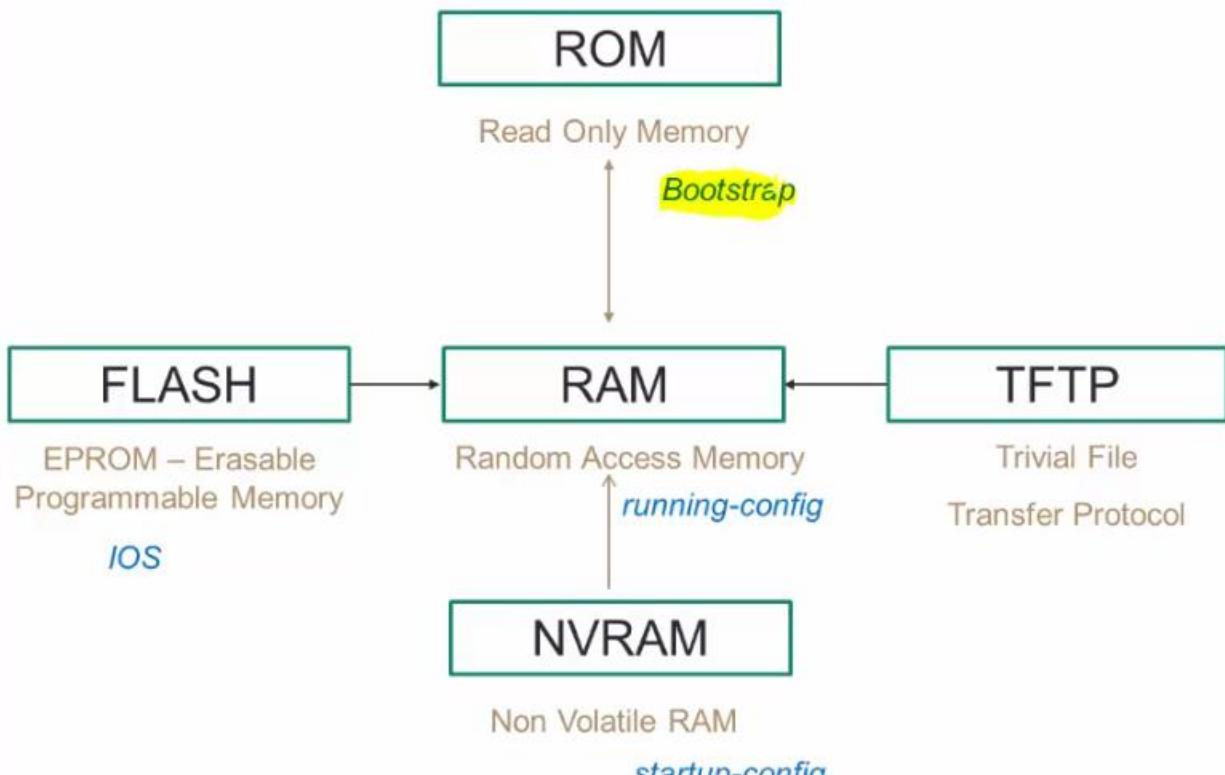
1. Ejecuta el Power On Self Test (POST).
2. Carga el programa de bootstrap.
3. Carga un IOS.
4. Carga un archivo de configuración.

```
System Bootstrap, Versi  
Technical Support: http:  
Copyright (c) 2010 by c  
Total memory size = 512  
cisco2901/K9 platform v  
Main memory is configur  
Readonly ROMMON initial  
program load complete,  
program load complete,
```

Diagrama de flujo del Proceso



German Hernandez P.
CCIE #24492



ROM

- Contiene el **POST (Power On Self Test)**
- Carga el programa de bootstrap (carga el Cisco IOS)
- Sistema Operativo mínimo.
- No se pierde su contenido al reiniciar.

FLASH

https://blc

- EEPROM (Electronically Erasable Programmable Read-Only Memory)
- Almacena el IOS (Internetworking Operating System)
- Se pueden tener múltiples versiones de IOS
- No pierde su contenido al reiniciar



RAM



- Almacena de forma temporal tanto la configuración como el sistema operativo del equipo
- Su contenido se pierde al reiniciarlo o apagarlo.
- También almacena:
 - Tablas de enrutamiento
 - Cache de ARP
 - Buffers de Chache
 - Buffers de switching
 - Y otros...



- Al archivo de configuración lleva el nombre de:
running-config

NVRAM

- Memoria RAM no volátil (Non-volatile RAM)
- Almacena la configuración y archivos de backup
- Su contenido no se pierde al reiniciar
- Al archivo de configuración lleva el nombre de:
startup-config

05 Fundamentos Direccionamiento IPv4

020 IPv4Introducción

Direcciones IPv4

- Dirección IP = Identificador = Único
- Máscara de Red
- Capa 3
- Decimal 0.0.0.0 – 255.255.255.255
- Cada dirección tiene una porción de HOST y una de RED



10.1.1.1
255.255.255.0



10.1.1.2
255.255.255.0

Origen BINARIO de 32 bits

00001010000000010000000100000001

Se separa en Octetos

00001010.00000001.00000001.00000001

Notación decimal con puntos:

10.1.1.1

Clases

Clase	Rango
Clase A	0.0.0.0 hasta 126.255.255.255
Clase B	128.0.0.0 hasta 191.255.255.255
Clase C	192.0.0.0 hasta 223.255.255.255
Clase D (Multicast)	224.0.0.0 hasta 239.255.255.255
Clase E (Experimental)	240.0.0.0 hasta 255.255.255.255

Ya no se usa el concepto de clases

169.254.0.0/16: Automatic Private IP Address (APIPA) Non Ruteable

El rango de 127 se utiliza para direcciones Loopback

CIDR (Classless Inter-Domain Routing) utiliza los bits de la parte de red para determinar como rutear el tráfico

Reservadas para IP privadas

Reservadas para IP PRIVADAS

RFC 1918

Rango

10.0.0.0

172.16.0.0 – 172.31.0.0

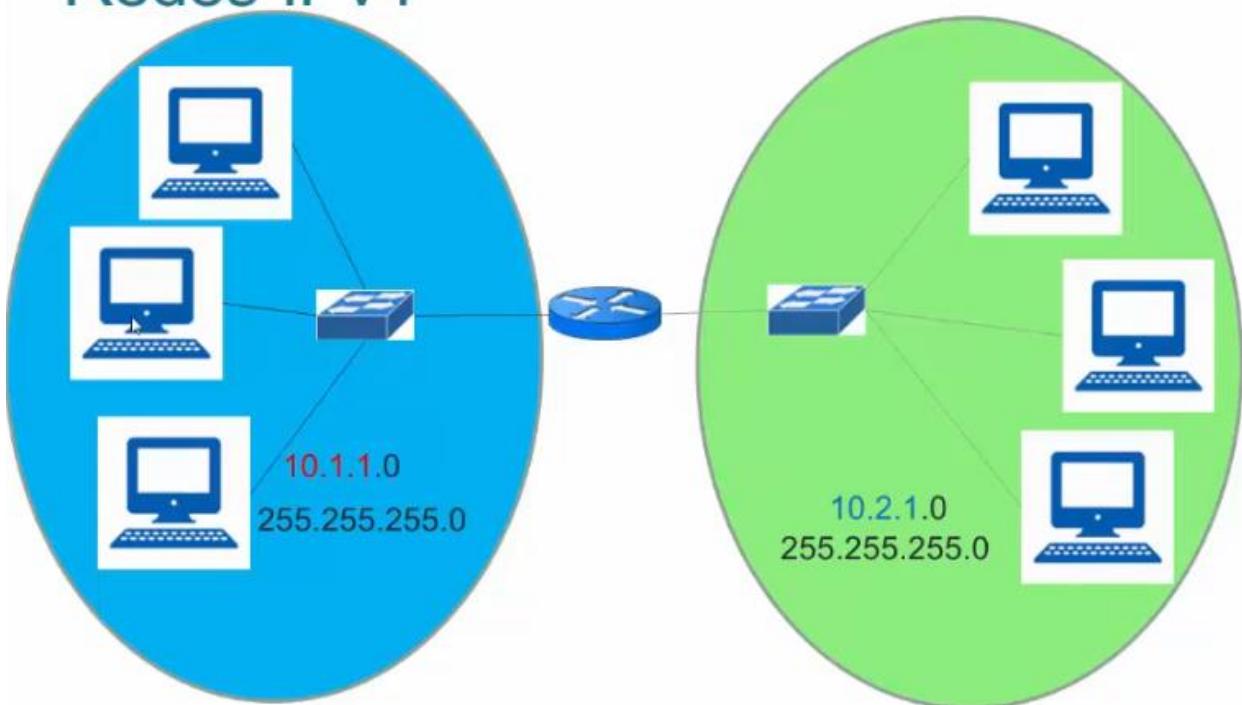
192.168.0.0 - 192.168.255.0

Uso Libre

No ruteadas en internet

021 IPv4 Mascara y subredes

Redes IPv4



Mascara de red

Clase	Mascara	Hosts
Clase A	255.0.0.0	16.777.216
Clase B	255.255.0.0	65536
Clase C	255.255.255.0	256

RED

10.1.1.0
255.255.255.0
256 hosts - 2

Sub red

10.1.1.0	10.1.1.128
255.255.255.128	255.255.255.128
128 hosts -2	128 hosts -2

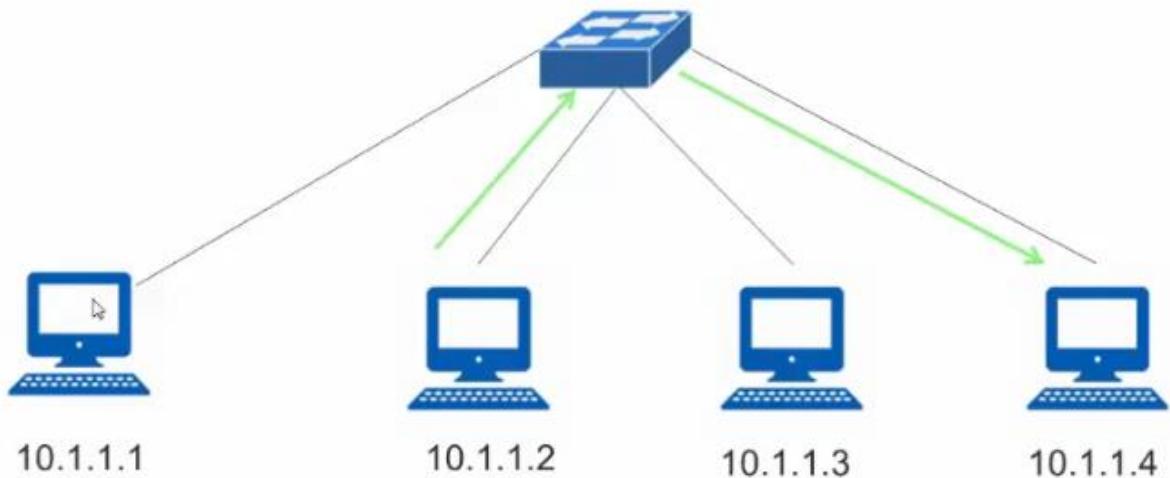
Dirección de red y broadcast

Dirección IPv4	10	1	1	1
Mascara de Red	255	255	255	0
Red	10	1	1	0
Broadcast	10	1	1	255

Clase	Mascara	Hosts
Clase A	255.0.0.0	16.777.216-2 = 16.777.214
Clase B	255.255.0.0	65536-2 = 65534
Clase C	255.255.255.0	256-2 = 254

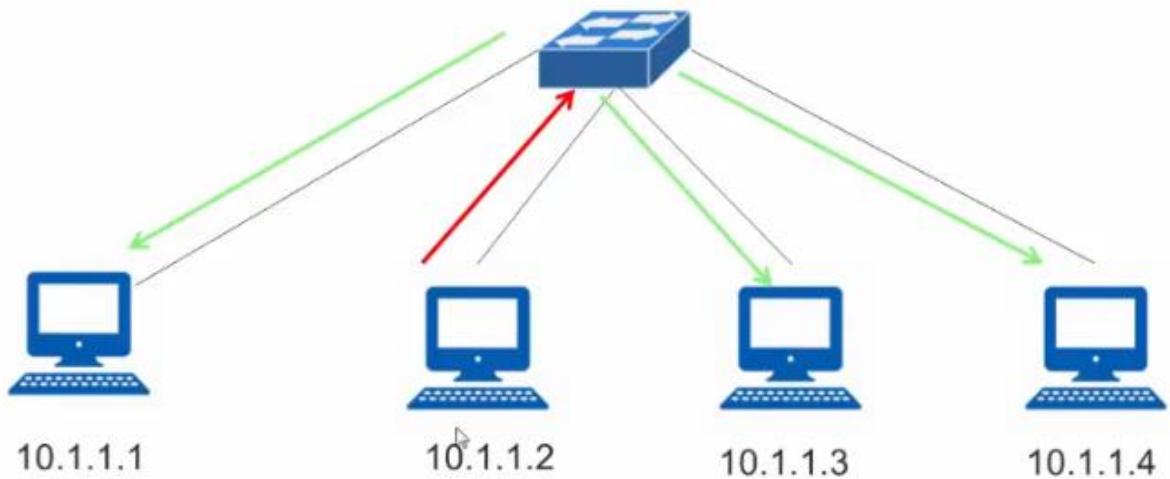
Unicast

Se envía un paquete de host a host
Origen 10.1.1.2 destino 10.1.1.4



Broadcast

Se envía un paquete de un host a TODOS los de esa red
Origen 10.1.1.2 destino 10.1.1.255



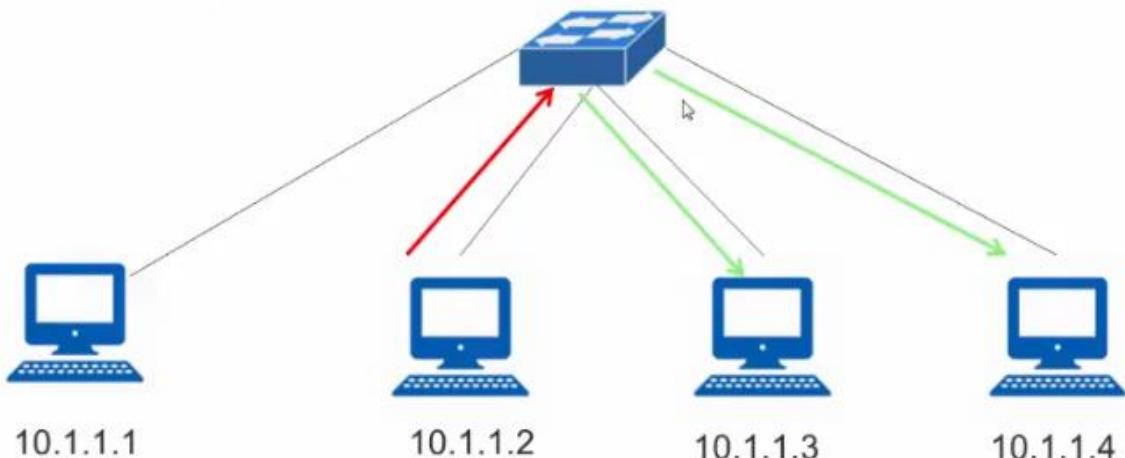
Multicast

Se envía un paquete de un host a un grupo de hosts

Origen 10.1.1.2 destino 224.0.0.0

Mecanismo eficiente para transmitir los mismos datos a múltiples receptores. Ahorra ancho de banda.

Algunos protocolos de enrutamiento lo utilizan



Dirección IP y mascara de red

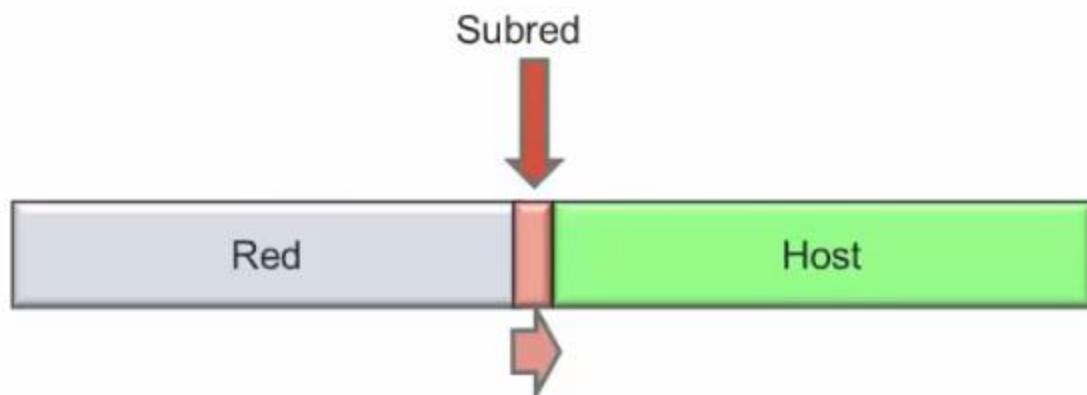
Dirección IPv4	10	1	1	0
Mascara de Red	255	255	255	0
Binario	11111111	11111111	11111111	00000000



Subred

http://

Mascara de Red			
255	255	255	128
11111111	11111111	11111111	10000000



Valores de la mascara decimal

	Valor del BIT								
	128	64	32	16	8	4	2	1	
255	1	1	1	1	1	1	1	1	
254	1	1	1	1	1	1	1	0	
252	1	1	1	1	1	1	0	0	
248	1	1	1	1	1	0	0	0	
240	1	1	1	1	0	0	0	0	
224	1	1	1	0	0	0	0	0	
192	1	1	0	0	0	0	0	0	
128	1	0	0	0	0	0	0	0	
0	0	0	0	0	0	0	0	0	

Valores de la mascara prefijo



Prefijo	Decimal	Valor del BIT							
		128	64	32	16	8	4	2	1
/32	255	1	1	1	1	1	1	1	1
/31	254	1	1	1	1	1	1	1	0
/30	252	1	1	1	1	1	1	0	0
/29	248	1	1	1	1	1	0	0	0
/28	240	1	1	1	1	0	0	0	0
/27	224	1	1	1	0	0	0	0	0
/26	192	1	1	0	0	0	0	0	0
/25	128	1	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0

Como saber cual es la red? Operación AND

$$1 \text{ AND } 1 = 1$$

$$1 \text{ AND } 0 = 0$$

$$0 \text{ AND } 1 = 0$$

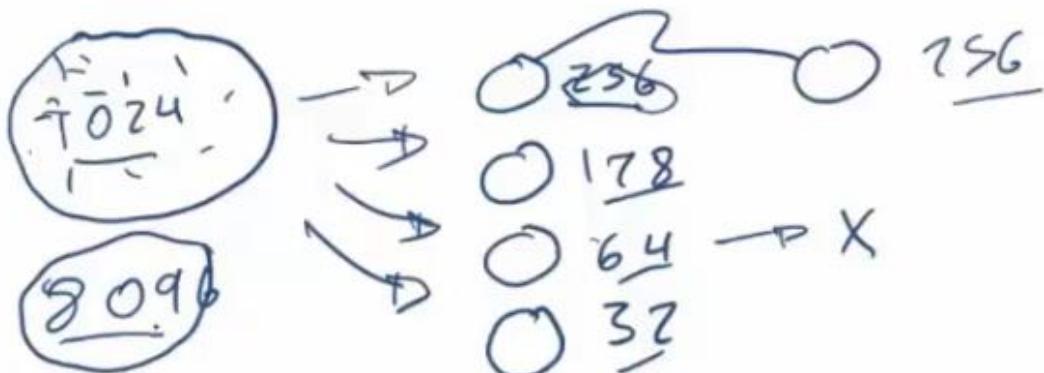
$$0 \text{ AND } 0 = 0$$

0 0 0 0 0 1 0 1 0	0 0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0 1
1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1
0 0 0 0 0 1 0 1 0	0 0 0 0 0 1 0 1 0	0 0 0 0 0 1 0 1 0	0 0 0 0 0 0 0 0 0

Dirección	10	1	1	1
Binario	00001010	00000001	00000001	00000001
Mascara	255	255	255	0
Binario	11111111	11111111	11111111	00000000
Resultado de AND	00001010	00000001	00000001	00000000
Dirección de Red	10	1	1	0

Beneficios de hacer subredes

- Se reduce el tráfico de la red ✓
- Se optimiza el rendimiento ✓
- Administración simplificada ✓
- Facilidad de gestión en redes muy grandes ✓



Classless Interdomain Routing (CIDR)

- Se introdujo en 1993 por le IETF RFC 1517
- Uso mas eficiente del espacio de direcciones IPv4
- Se agrega el prefijo (ej. $255.255.255.0 = /24$), lo que reduce el tamaño de las tablas de enrutamiento

CIDR

<https://>

Mascara	CIDR	Mascara	CIDR	Mascara	CIDR
255.0.0.0	/8 ✓	255.255.0.0	/16	255.255.255.0	/24 ✓
255.128.0.0	/9 ✓	255.255.128.0	/17 ✓	255.255.255.128	/25 ✓
255.192.0.0	/10 ✓	255.255.192.0	/18 ✓	255.255.255.192	/26
255.224.0.0	/11 ✓	255.255.224.0	/19 ✓	255.255.255.224	/27
255.240.0.0	/12 ✓	255.255.240.0	/20 ✓	255.255.255.240	/28
255.248.0.0	/13 ✓	255.255.248.0	/21 ✓	255.255.255.248	/29
255.252.0.0	/14 ✓	255.255.252.0	/22	255.255.255.252	/30
255.254.0.0	/15	255.255.254.0	/23	255.255.255.254	/31

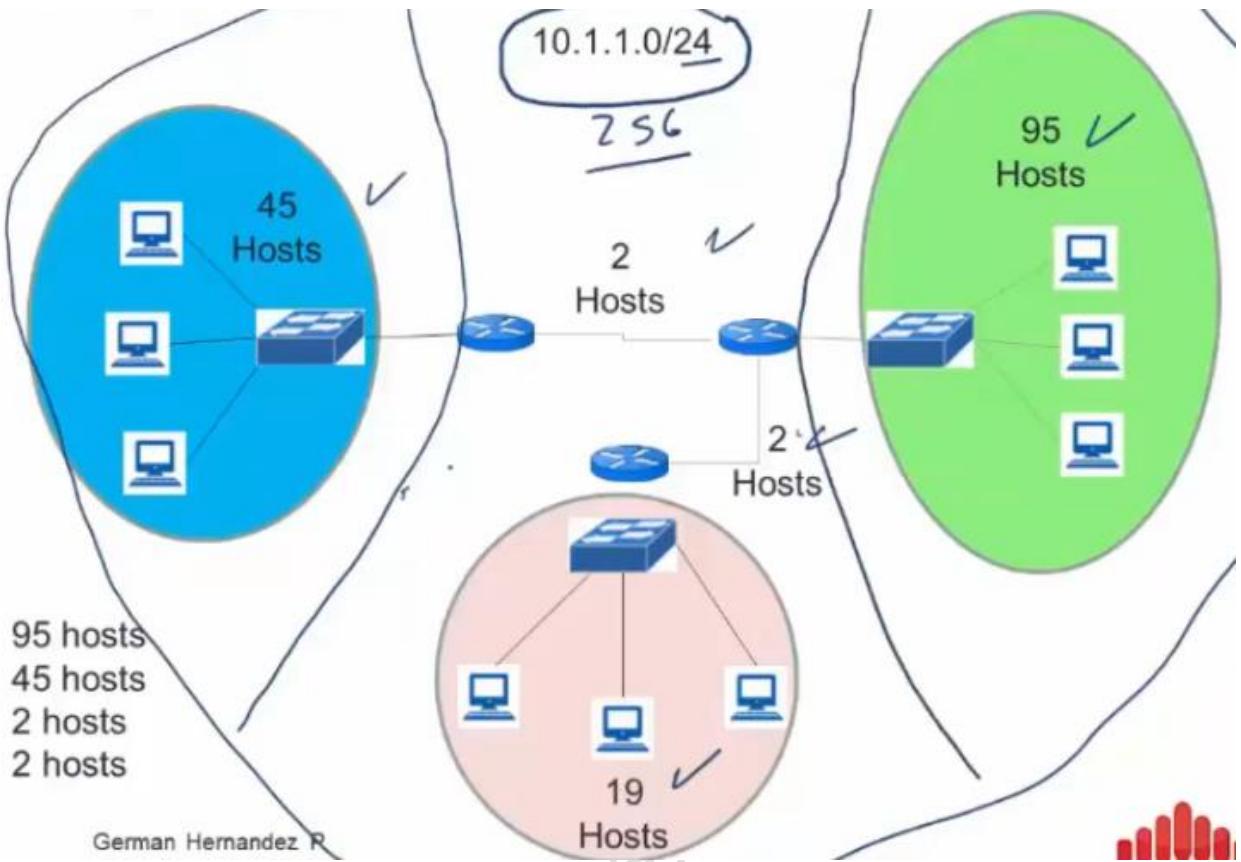
Clase C

8 bits para hosts = 256-2

Los bits de subnet van de izquierda a derecha sin saltarse bits, osea todos en 1 (24 bits = 11111111.11111111.11111111.00000000)

Mascara	CIDR	Ultimo Octeto en binario
255.255.255.0	/24	00000000
255.255.255.128	/25	10000000
255.255.255.192	/26	11000000
255.255.255.224	/27	11100000
255.255.255.240	/28	11110000
255.255.255.248	/29	11111000
255.255.255.252	/30	11111100
255.255.255.254	/31	11111110

VLSM



Haciendo subnets de una subnet con Clase C

- Cuantas subredes se obtienen de la mascara?
- Cuantos hosts validos por subred? ✓
- Cuales son esas redes? ✓
- Cual es la dirección de broadcast? ✓
- Cuales son los hosts validos? ✓

Cuantas sub redes?

Formula:

2^x = números de subredes.

- X es el numero de bits "enmascarados" o de red osea los unos (1s)
- Ejemplo:
 - 1100 0000
 - $2^2 = 4$
 - 4 subredes

1100 0000

Cuantos host por subred?

Formula:

2^{y-2} = numero de hosts por subred

Y es el numero de bits sin enmascarar o disponibles para Hosts osea los ceros (0s)

Ejemplo:

11000000

$$2^6 - 2 = \underline{64} - 2 = 62 \checkmark$$

Ósea 62 hosts por subred

11000000

$$\begin{array}{r} 64 - 2 = 62 \\ \hline 11000000 \end{array}$$

Cuales son las subredes

Formula:

256 – mascara de red = tamaño del bloque

Ejemplo:

$$256 - 192 = 64$$

Osea se debe sumar de 64 en 64 4 veces:

	RED	10.1.1.0
.0	10.1.1.0 .	
.64	10.1.1.64	
.128	10.1.1.128	
.192	10.1.1.192	

Cuales son las direcciones de broadcast?



Serian todos los bits en unos ✓

Precisamente el numero que precede a la siguiente dirección de red

RED	BROADCAST
10.1.1.0	10.1.1.63
10.1.1.64	10.1.1.127
10.1.1.128	10.1.1.191
10.1.1.192	10.1.1.255

Cuales son las direcciones de host validas?

Son los números entre redes, exceptuando la dirección de red y la dirección de broadcast:

RED	BROADCAST	HOSTS
10.1.1.0	10.1.1.63	10.1.1.1-10.1.1.662
10.1.1.64	10.1.1.127	10.1.1.65-10.1.1.126
10.1.1.128	10.1.1.191	10.1.1.129-10.1.1.190
10.1.1.192	10.1.1.255	10.1.1.193-10.1.1.254

023 IPv4 VLSM Parte 2

Método abreviado

	/25	/26	/27	/28	/29	/30	/31
	.128	.192	.224	.240	.248	.252	.254
Redes	2	4	8	16	32	64	128
Hosts	128	64	32	16	8	4	4

10.1.1.0

10.1.1.0

255.255.255.128

255.255.255.192

2 redes de 128 hosts -2

4 redes de 64 hosts -2

Red= 10.1.1.0

Red= 10.1.1.0

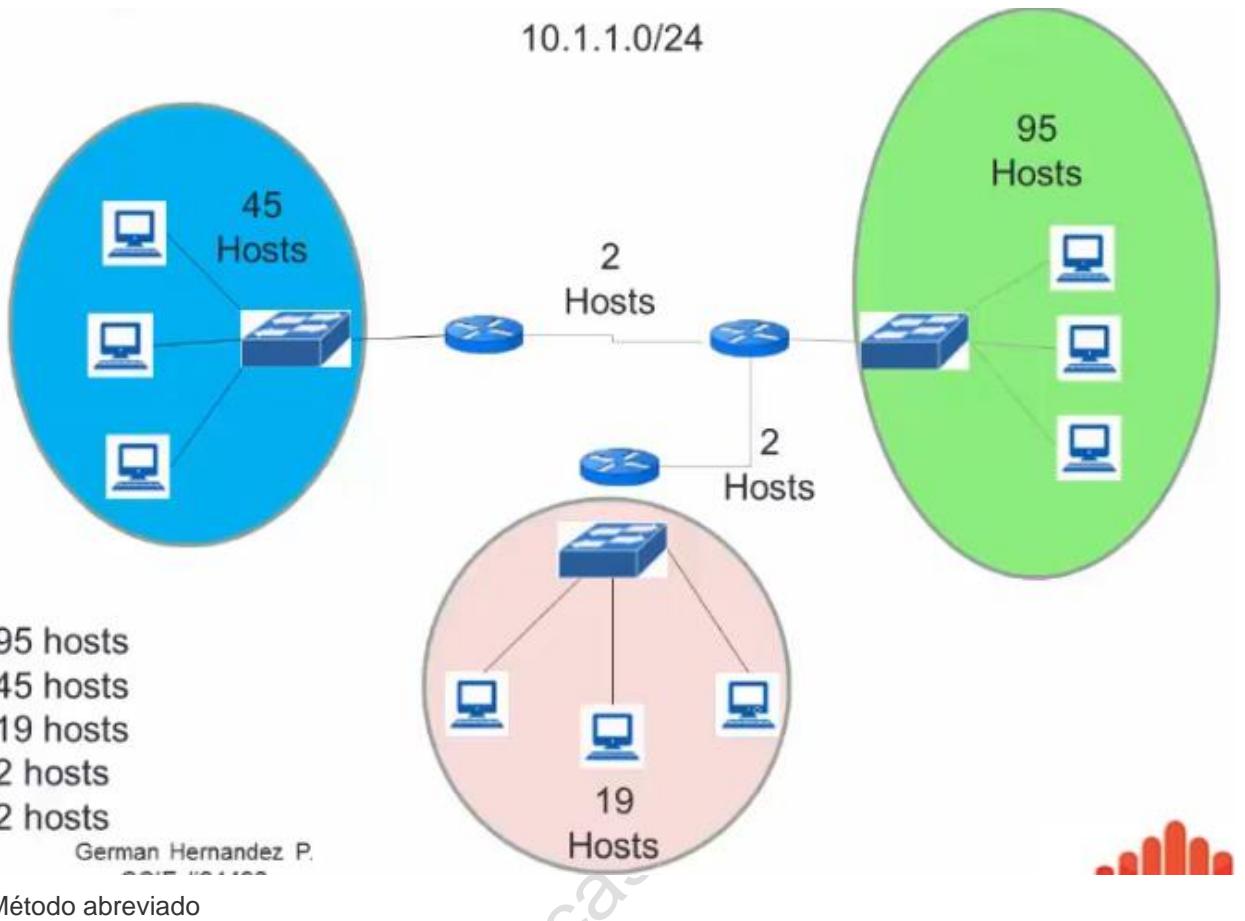
Red= 10.1.1.128

Red= 10.1.1.64

VLSM

Red= 10.1.1.128

Red= 10.1.1.192



	/25	/26	/27	/28	/29	/30	/31
	.128	.192	.224	.240	.248	.252	.254
Redes	2	4	8	16	32	64	128
Hosts	128	64	32	16	8	4	2

Requerimiento:

10.1.1.0

255.255.255.0

2 redes de 128 hosts -2

95 hosts ✓

45 hosts

19 hosts

2 hosts

2 hosts

Red= 10.1.1.0

Hosts= 10.1.1.1-10.1.1.126

Broadcast: 10.1.1.127

Red= 10.1.1.128

	/25	/26	/27	/28	/29	/30	/31
	.128	.192	.224	.240	.248	.252	.254
Redes	2	4	8	16	32	64	128
Hosts	128	64	32	16	8	4	2

Requerimiento:

Red= 10.1.1.0

Hosts= 10.1.1.1-10.1.1.126

Broadcast: 10.1.1.127

95 hosts

45 hosts

19 hosts

2 hosts

2 hosts

Red= 10.1.1.128/26

Hosts: 10.1.1.129-10.1.1.190

Broadcast: 10.1.1.191

	/25	/26	/27	/28	/29	/30	/31
	.128	.192	.224	.240	.248	.252	.254
Redes	2	4	8	16	32	64	128
Hosts	128	64	32	16	8	4	2

Requerimiento: Red= 10.1.1.0
 Hosts= 10.1.1.1-10.1.1.126
 Broadcast: 10.1.1.127

95 hosts ✓
 45 hosts
 19 hosts ✓ Red= 10.1.1.128/26
 2 hosts Hosts: 10.1.1.129-10.1.1.190
 2 hosts Broadcast: 10.1.1.191

Red= 10.1.1.192/27 ✓
 Hosts: 10.1.1.193-10.1.1.222
 Broadcast: 10.1.1.223

(12) 10.1.1.192 → 192
 (12) 10.1.1.223 + 32
 224

	/25	/26	/27	/28	/29	/30	/31
	.128	.192	.224	.240	.248	.252	.254
Redes	2	4	8	16	32	64	128
Hosts	128	64	32	16	8	4	2

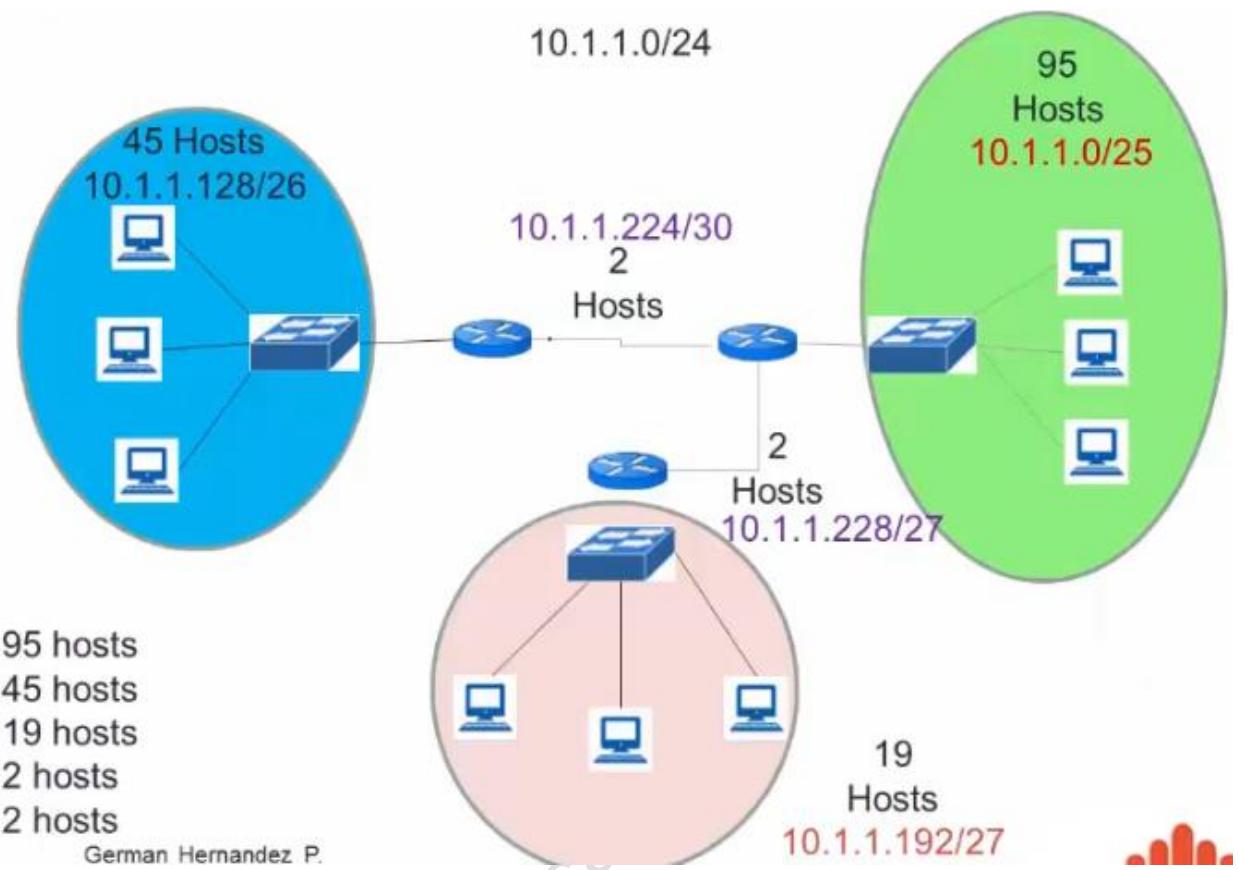
Requerimiento: Red= 10.1.1.0 ✓
 Hosts= 10.1.1.1-10.1.1.126
 Broadcast: 10.1.1.127 ✓

95 hosts ✓
 45 hosts ✓
 19 hosts ✓ Red= 10.1.1.128/26 ✓
 2 hosts ✓ Hosts: 10.1.1.129-10.1.1.190
 2 hosts ✓ Broadcast: 10.1.1.191

Red= 10.1.1.192/27
 Hosts: 10.1.1.193-10.1.1.222
 Broadcast: 10.1.1.223

Red= 10.1.1.224/30 Hosts:
 10.1.1.225-10.1.1.226 ✓
 Broadcast: 10.1.1.227 ✓

Red= 10.1.1.228/27 → ①
 Hosts: 10.1.1.229-10.1.1.230
 Broadcast: 10.1.1.231



06 Fundamentos Direccionamiento IPv6

024 IPv6 Introducción a direcciones IPv6

Necesidad de IPv6

La IPv6 fue pensada para las sustitución de IPv4.

Debido al agotamiento de dirección IPv4 y la falta de planificación o provisión en la asignación inicial.

El crecimiento acelerado del uso de internet hasta el punto del "Internet de las cosas".

IPv6 tiene mejoras significativas de acuerdo a la experiencia con IPv4.

IPv6 comparada con IPv4

IPv4

32 bits o 4 bytes de longitud.

4200000000 direcciones. Lo que seria
aproximadamente 4 mil doscientos millones de direcciones

IPv6

128 bits o 16 bytes: Cuatro veces los bits de IPv4

340282366920938463374607432768211456

Lo que equivale 340 billones de billones de billones
(sextillones) de direcciones

Principales características

Mayor espacio de direccionamiento

Seguridad

- IPv6 incluye IPSEC: autenticación y encripción.

Autoconfiguración

- Usa mensajes MULTICAST de descubrimiento de routers de ICMPv6.

Movilidad

- Permite moverse de proveedor a proveedor (ISP) conservando la misma dirección (roaming de IP)

Mecanismos de traducción de IPv6 a IPv4

Calidad de Servicio (QoS) y Clase de Servicio (CoS)

Representación de direcciones IPv6

- 128 bits de largo
- Expresado en hexadecimal en vez de decimal
- Los dos puntos ":" se usan para separar un grupo de 4 caracteres hexadecimales.

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Se representa así:

x:x:x:x:x:x:x:x

En donde "x" es un valor hexadecimal de 16 bits para 128 en total.

Ejemplo:

1080:AFD0:3FC0:4CD0:3FC8:C800:200C:417A

- En IPv6, 4 bits representan un único dígito hexadecimal, 32 valores hexadecimal = dirección IPv6

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

- Hextet es el nombre usado por cada bloque de 4 valores hexadecimales
- usado para referenciar un segmento de 16 bits o cuatro hexadecimales

Regla #1: los ceros se pueden omitir

- Cualquier cero a la izquierda en cualquier sección de 16-bit o hextet puede ser omitido
 - 02AC puede ser representado como 2AC
 - 008E puede ser representado como 8E
- 02AC:0001:1C3F:8B42:9CB7:0DDF:A1EB**
2AC:0001:1C3F:8B42:9CB7:0DDF:A1EB

8B42:**008E**:2E3A:6F41:9CB7:1DDF:D1BC

8B42:**8E**:2E3A:6F41:9CB7:1DDF:D1BC

Regla #2: omitir segmentos de todos 0

- Uno o más grupos de ceros pueden ser sustituidos por un doble dos puntos (::)
- Un doble "dos puntos" (:) puede ser usado una vez dentro de una dirección de otra manera la dirección será ambigua

1080:**0000:0000:0000**:0008:0800:200C:417A

1080::8:800:200C:417A

Tipos de direcciones

Unicast

Identificar una interface de un nodo IPv6

Multicast

Identifican un grupo de interfaces.

Anycast

Sirven para identificar a un conjunto de interfaces.

Cuando **se** envía un paquete a una dirección anycast es entregado a una de estas interfaces: a la más cercana.

Nota: IPv6 no tiene dirección de broadcast.

Interface ID



025 IPv6 Tipos de Direcciones

Unicast

- **Global Unicast**

- Equivalentes a las direcciones IPv4 **publicas**
- Enrutables
- Empiezan con 2000::/3

Ejemplo:

2004:A128::32:FEDC:BA98:7865:4321/64

- **Unique Local**

- Equivalentes a las direcciones IPv4 **privadas**.
- FC00::/7

No son enrutables en Internet

Empiezan con FC o con FD

Ejemplo:

fd12:B128:e8e1:1:FEA1:BC98:8865:4421 /64

Link Local

Direccion IPv6 Default en cualquier interfaz habilitada con IPv6

No es enrutable

Formato:

El prefijo de formato ocupa 10 bits: 1111 1110 10 (**FE80::/10**).

El resto de los primeros 64bits son 0

Identificador de host (64bits)

Ejemplo:

fe80::3e71:58ff:fce9:64bb/64

Multicast

Identifican un grupo de interfaces.

FF00::/8

Ejemplo:

FF02::1:FF00:0 - FF02::1:FFFF:FFFF

Anycast

Sirven para identificar a un conjunto de interfaces.

Cuando se envía un paquete a una dirección anycast es entregado a una de estas interfaces: a la más cercana.

Un paquete enviado a una dirección anycast es entregado a la máquina más cercana desde el punto de vista del tiempo de latencia.

Otras direcciones

Dirección sin especificar: 0:0:0:0:0:0:0:0 (::)

Cuando el host no tiene ninguna dirección asignada

Dirección de loopback: 0:0:0:0:0:0:1 (::1)

Equivale a la dirección de loopback IPv4 127.0.0.1

Direcciones IPv4 codificadas:

De uso en arquitecturas que mezclan las pilas IPv4, IPv6

Formato,

::FFFF:<IPv4>

Ejemplo ::FFFF:192.02.13.123

027 IPv6 Configuracion basica de direcciones IPV6

Paso 1 habilitar IPv6

Comando:

ipv6 unicast-routing

Ejemplo:

Router(config)# ipv6 unicast-routing

Paso 2 configurar IPv6 en la interfaz

Comando:

ipv6 address ipv6-prefix/prefix-length [eui-64]

Ejemplo:

Router(config-if)# ipv6 address 2001:0DB8:1c18:1111::3/64

Comandos de verificación

Para verificar el estado de la interfaz con IPv6 configurado:
show ipv6 interface

show ipv6 interface brief

Ping ipv6 direccion ipv6

034 LLDP

- Protocolo de descubrimiento de vecinos (Neighbors)
- Protocolo Standard IEEE 802.1AB LLDP.



035 Introducción a Etherchannel

Que es etherchannel?

- Permite la agrupación de interfaces físicas en una sola interfaz lógica.
- Por ejemplo: tomar 2 interfaces físicas Fastethernet0/1 y Fastethernet0/2 y hacer que se comporten como una sola a nivel de capa 2 o capa 3.
- Permite "sumar" las velocidades. Ej :
 $100\text{Mbps} + 100\text{Mbps} = 200 \text{ Mbps}$
- Se basa en el estándar IEEE 802.3

Características

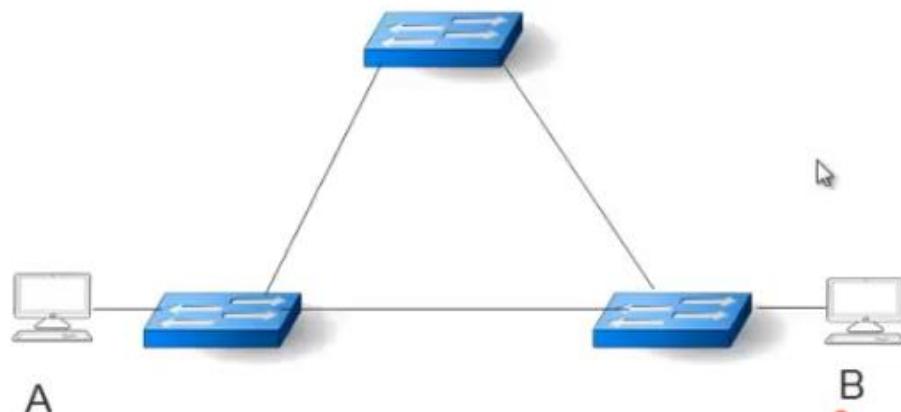


- Se pueden agrupar hasta 8 interfaces físicas
- FastEthernet, GigaEthernet, 10GigaEthernet.
- Se basa en el estándar IEEE 802.3
- Link Aggregation Control Protocol (LACP). Estandar 802.3ad
- Port Aggregation Protocol (PAgP). Propietario Cisco
- Todos los puertos deben estar en el mismo switch.
- El SpanningTree lo vera como una sola interfaz.
- También se conoce como "bundle"
- Funciona con servidores, firewalls y otro tipo de hosts.

037 Introducción a Spanning Tree Protocol – STP

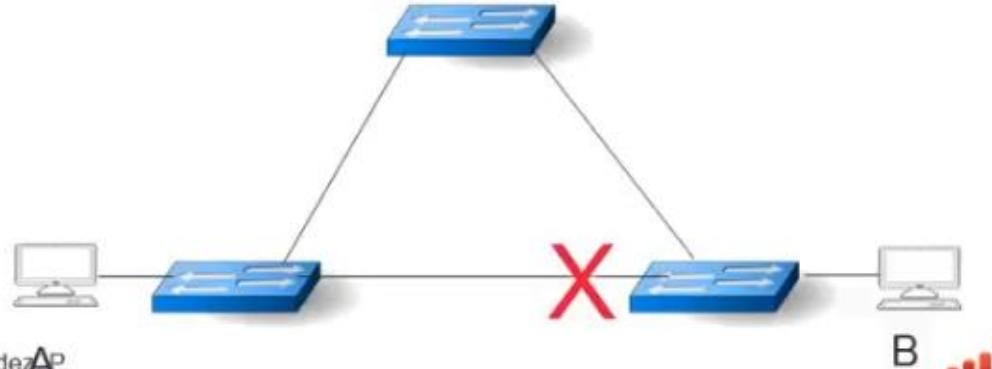
redundancia

- La redundancia en las redes LAN evita el tener un punto único de falla.
- Las redes de hoy en día usan enlaces redundantes para minimizar problemas o fallas en la red
- Pero puede crear algunos problemas como:
 - Tormentas de broadcast
 - Transmisión de tramas múltiples
 - Inestabilidad en la tabla de MACs
- Se requiere un mecanismo para evitar loops



¿Qué hace Spanning Tree?

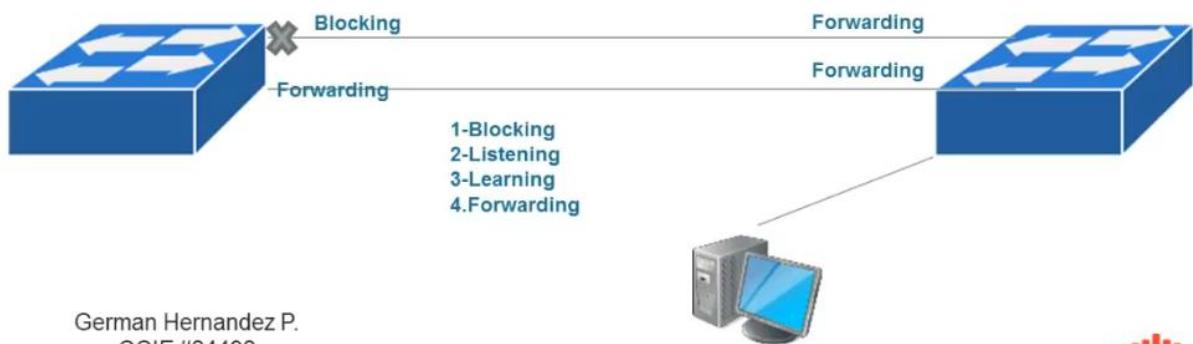
- Se habilita de forma automatica en los switches Cisco, pero podria requerir algunos ajustes.
- Se basa en el Standard IEEE 802.1d
- Provee una red libre de “loops” colocando algunos puertos en estado de “blocking”
- BPDUs, se intercambian para mantener la topologia de STP



039 STP Portfast

Que es portfast?

Se configura en los puertos de Acceso para que dicho puerto no pase por todos los estados de Spanning Tree y de una vez se coloque en el estado de FORWARDING.



German Hernandez P.
CCIE #24492

Para que?

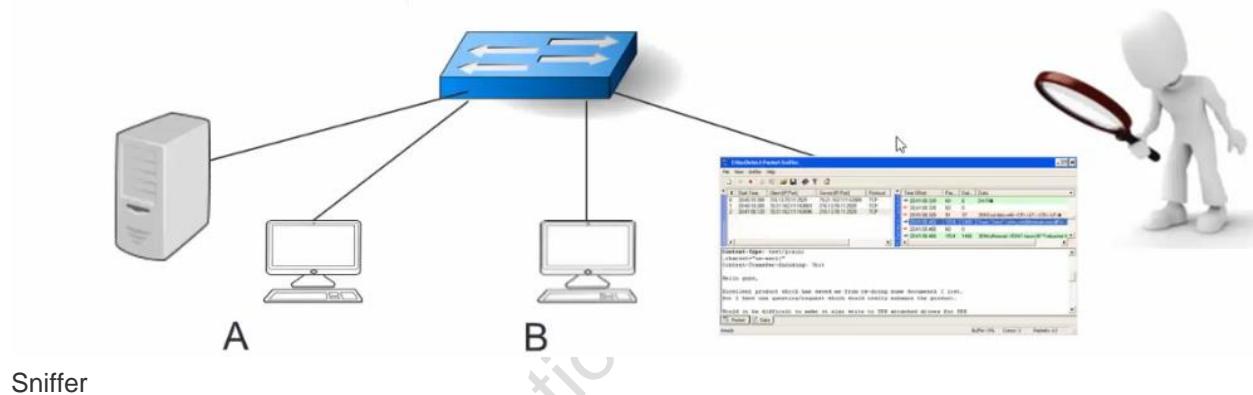
Para que los puertos conectados a PCs o Host, inicien la transmisión en cuanto se conecten.

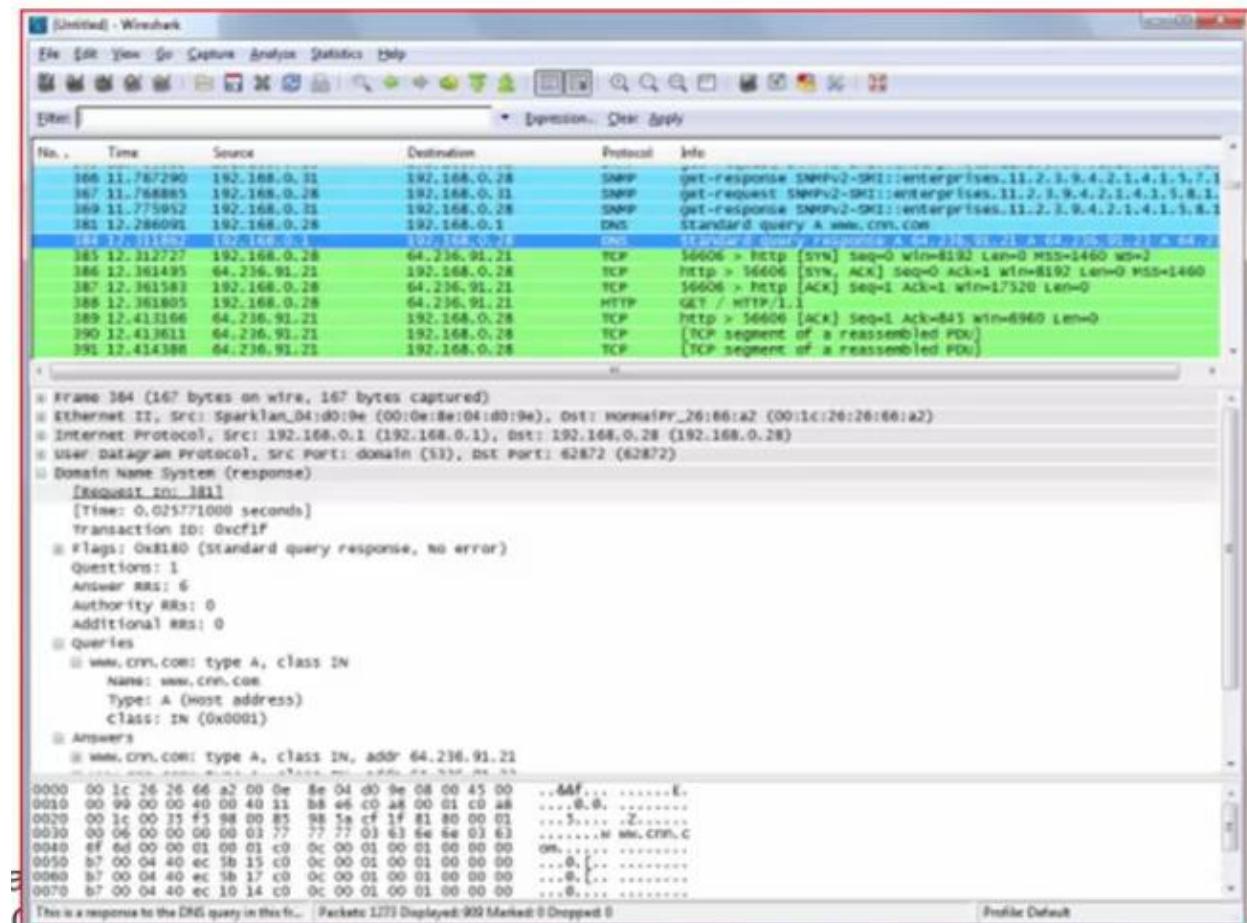
Nota: No habilitar PORTFAST en puertos en donde exista un switch. Esto ocasionaría un loop.

040 Configuración de SPAN

¿Qué es SPAN?

Tecnología que permite capturar el tráfico de los puertos de un switch para ser analizado por herramientas de software.





Terminología

Ingress Traffic: El tráfico que ingresa al switch

Egress Traffic: El tráfico que sale del switch

Source (SPAN) port: El Puerto o puertos que quieren ser monitoreados

Source (SPAN) VLAN: La VLAN a la cual se quiere monitorear (se puede hacer por puerto o por VLAN)

Destination (SPAN) port: El Puerto que monitorea los puertos "source". Acá es donde usualmente se coloca el analizador.

Remote SPAN (RSPAN): Técnica que se utiliza Cuando los **Source ports** no están en el mismo switch.

Configuración

Por ejemplo configurar el Puerto FastEthernet0/2 como Puerto SOURCE:

```
SWITCH#configure terminal  
SWITCH(config)#  
SWITCH(config)#monitor session 1 source interface fastethernet 0/2
```

Luego se configura el puerto FastEthernet0/3 como Destino:

```
SWITCH(config)#monitor session 1 destination interface fastethernet 0/3
```

Luego se verifica la configuración de SPAN:

```
SWITCH#show monitor session 1
```

041 StackWise



Disponible en switches de la serie 3600, 3700 y 3800

Característica

32 Gbps stack interconnect

Se pueden apilar hasta 9 switches

Puerto Separado de stacking

Auto-configuration

Cisco IOS ® version check/update

Cross-stack EtherChannel and QoS

Cable patentado

Funciones



Selección automática del master

Una sola instancia para servicios de red (IP, SNMP, STP, CLI)

Mejor control del tráfico

Mejor Redundancia

Comandos de verificación

S3750-Stk# show switch stack-ports

Switch #	Port 1	Port 2
1	Ok	Down
2	Ok	Ok
3	Ok	Down

042 DTP

Dynamically Trunking Protocol (DTP)

Protocolo propietario de Cisco que negocia el modo troncal entre dos switches.

Solo disponible para switches.



08 Conectividad IP

043 Introducción a routing

¿Qué es enrutamiento?

- Proceso de mover paquetes de datos de un origen a un destinoseleccionando la mejor ruta.
- De forma práctica esto sería enviar paquetes de una red a otra red.
- Usualmente lo lleva a cabo un enrutador (router)



¿Qué se necesita?

Componentes básicos que se necesitan:

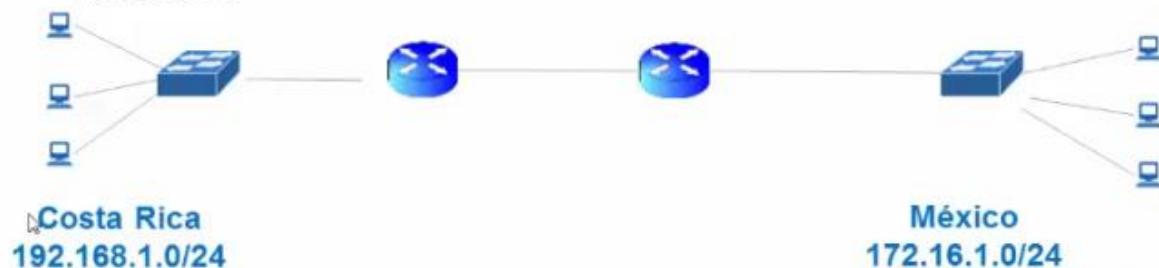
Un paquete que se enrutable (capa 3) ósea IPV4, IPV6 u otros...

Dirección de red

Máscara de red

Siguiente salto (Next Hop)

Métrica



La tabla de enrutamiento

Lista de todas las redes que el router conoce y cual seria la interfaz para alcanzarlas

Utiliza direcciones IP y mascaras de red para determinar por donde enviar el trafico



Tipos de ruta

Connected

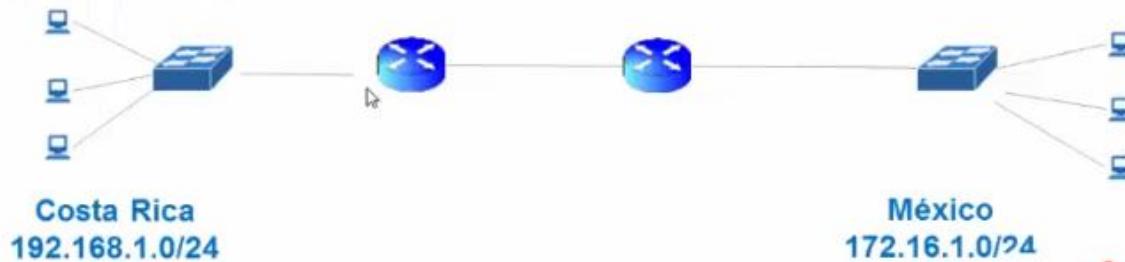
Directamente conectadas

Static

Definidas manualmente

Dynamic

Aprendidas de automáticamente por un protocolo de enrutamiento



044 Rutas Estaticas

El administrador de red introduce manualmente cada una de las rutas

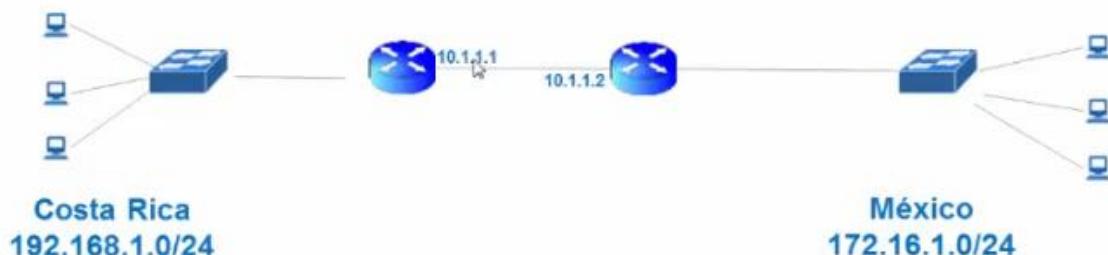
Requieren saber de antemano las redes destino y su siguiente salto (next hop)

Requieren mas administración



Configurar ruta estatica

Comando	Descripción
router(config)# ip route [red destino] [mascara de red destino] [next hop]	Se configura la red donde se quiere llegar y la IP del siguiente salto
router(config)# ip route [red destino] [mascara de red destino] [interfaz de salida]	Se configura la red donde se quiere llegar y la interfaz salida



Comandos de verificación

Comando	Descripción
router# show ip route	Muestra la tabla de enrutamiento
router# show ip route static	Muestra las rutas estáticas en la tabla de enrutamiento
router# show running-config include ip route	Muestra la configuración actual de las rutas estáticas

045 Enrutamiento Dinamico

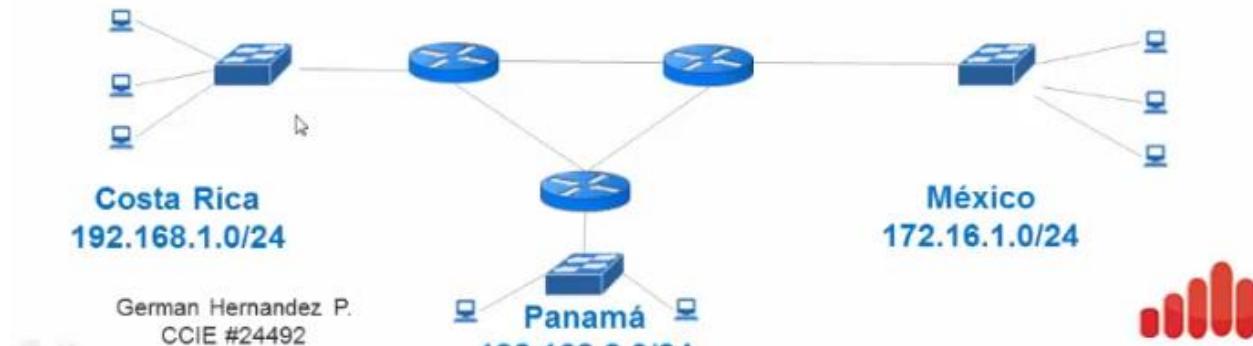
Permite actualizar las rutas automáticamente sin cambios manuales: dinámicamente.

Se realiza utilizando protocolos de enrutamiento.

Determinan la mejor ruta al destino.

Protocolo de enrutamiento: EIGRP, OSPF, BGP, etc.

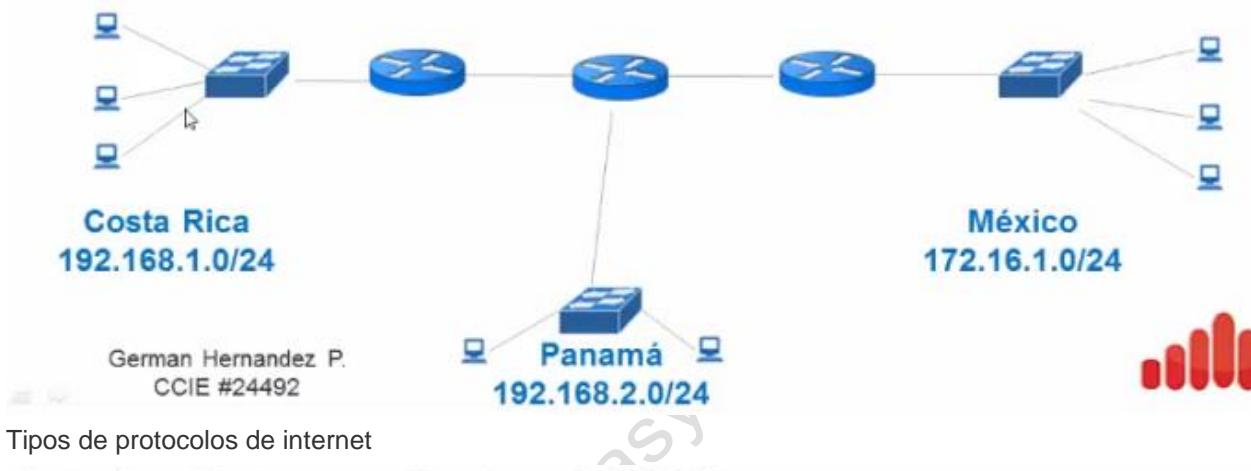
Protocolo enrutado: IPv4, IPv6, IPX, AppleTalk, etc.



Componentes

Algoritmo: Calculo matemático para determinar la mejor ruta

Mensajes: Para descubrir routers vecinos y/o interconectados, y también intercambiar tablas de enrutamiento



Interior Gateway Protocol (IGP)

Utilizan el concepto de Sistema Autónomo.

Protocolos: RIP, EIGRP, OSPF

Extended Gateway Protocol (EGP)

Intercambian enrutamiento entre redes de sistemas autonomos

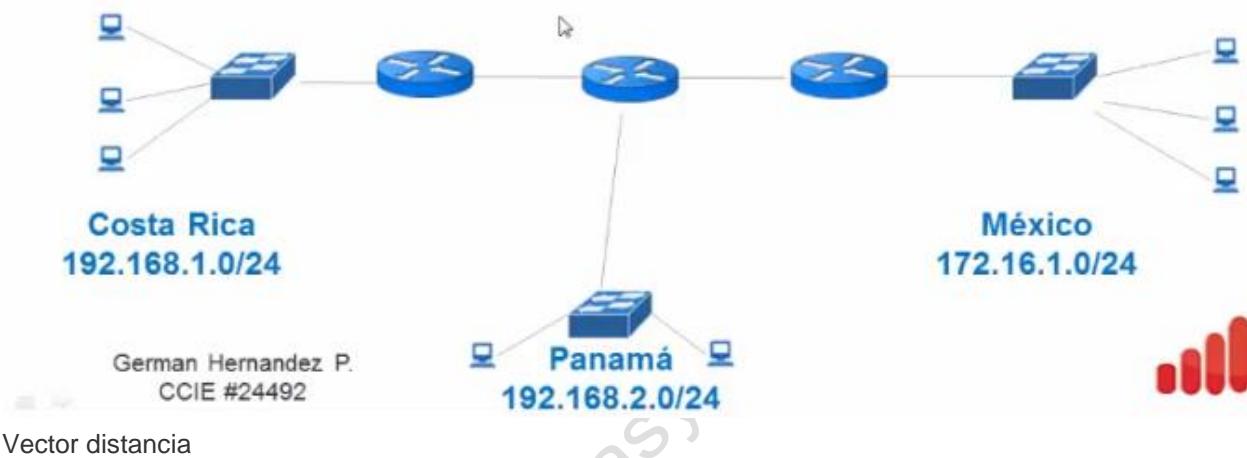
Protocolos: BGP

Clasificación

https://

Vector Distancia

Estado de Enlace



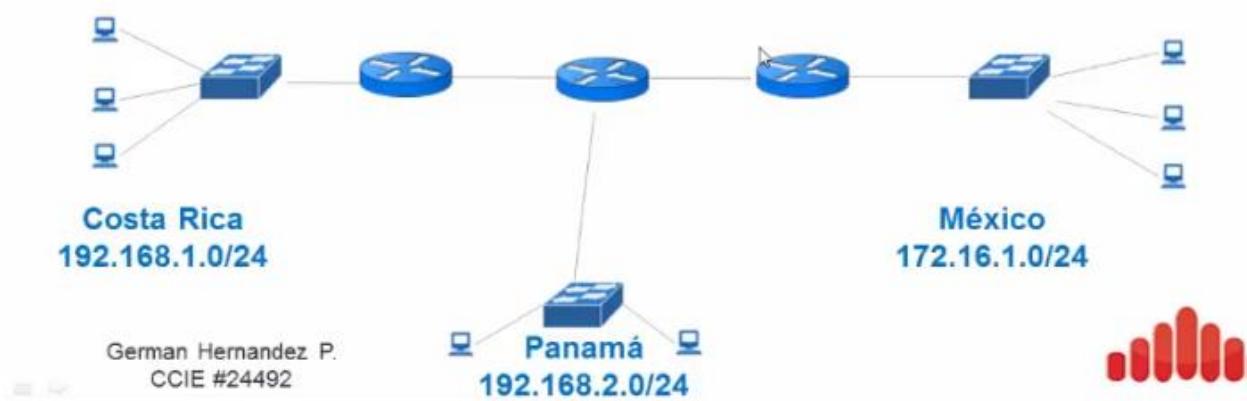
Vector distancia

Determina la dirección (vector) y la distancia a una red.

Copias periódicas de tabla de enrutamiento= actualización periódica.

Vista Parcial de la red.

Router recibe la tabla de enrutamiento de su router vecino.



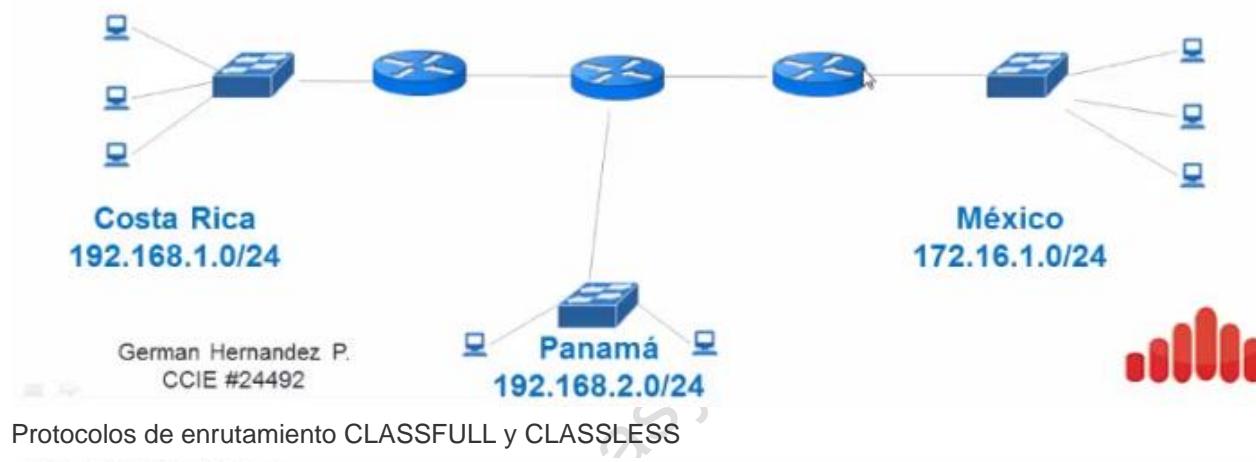
Estado de enlace

Tienen la topología exacta de la red

Actualización solo si hay cambios

Cada router tiene su propia base de datos con la topología completa

Se envían paquetes a todos los routers de la red para descubrir la red entera :LSAs (Links State Advertisement)



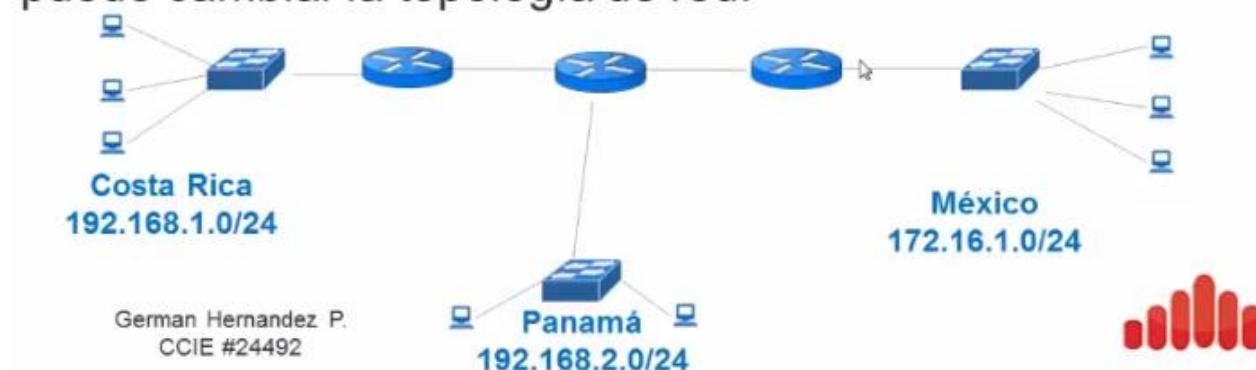
Protocolos de enrutamiento CLASSFULL y CLASSLESS

CLASSFULL

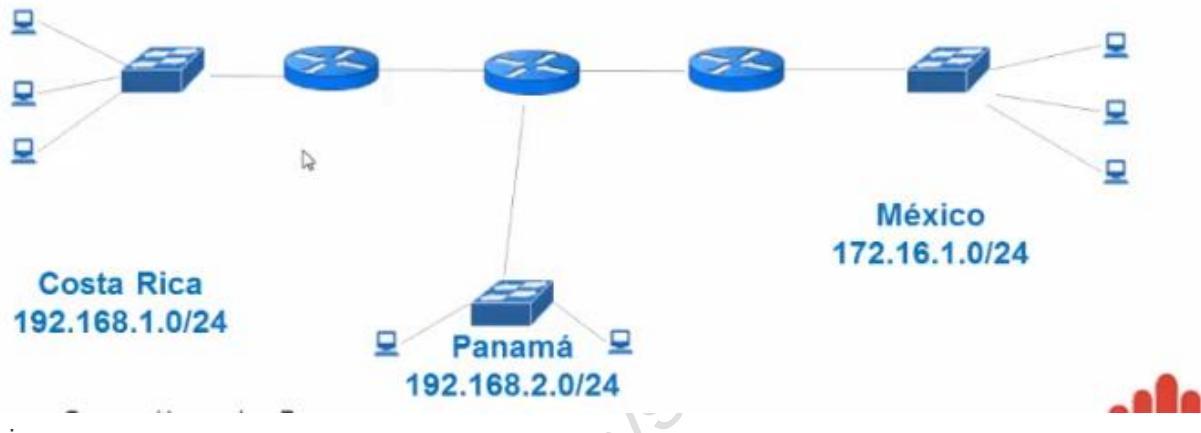
No envían la mascara de red porque asumen que no hay variaciones en las redes y la topología es la misma.

CLASSLESS

Si envían la mascara de red ya que es variable y puede cambiar la topología de red.



Existen cambios en la red, los routers cambian sus tablas de enrutamiento y finalmente todos los routers tienen la tabla de enrutamiento uniforme

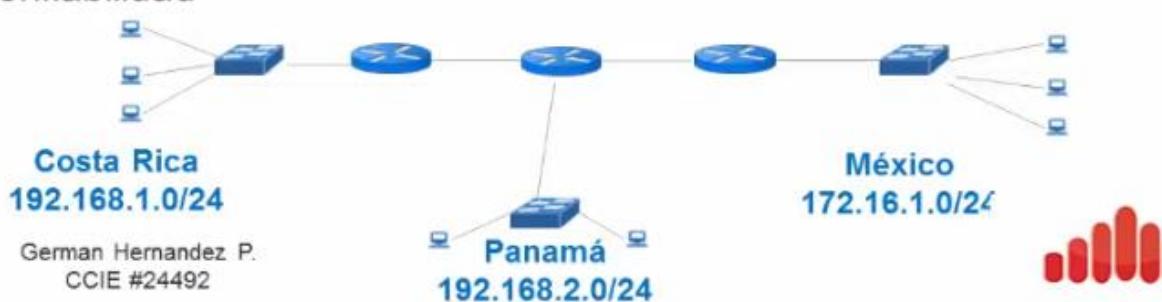


Metrica

Valor usado por los protocolos de enrutamiento para determinar la mejor ruta. Cada protocolo usa una metrica diferente tomando en cuenta diferentes factores:

- Saltos
- Ancho de banda
- Costo
- Retraso
- Carga
- Confiabilidad

Protocolo	Metrica
RIP	Saltos
EIGRP	Ancho de banda, retraso carga, confiabilidad
OSPF	Costo, Ancho de Banda



Distancia administrativa

German Hernandez P.
CCIE #24492

Los routers son multiprotocolo, así que pasa si tienen dos protocolos para llegar a una misma red?

Ejemplo: OSPF y EIGRP

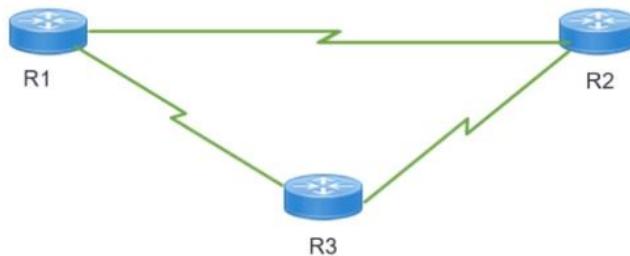
Ruta	DA
Conectado	0
Estatica	1
Ruta sumarizada EIGRP	5
BGP Externo	20
EIGRP Interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP Externo	170
BGP interno	200

046 OSPF Conceptos básicos

- Open Shortest Path First
- Tipo IGP: Interior Gateway Protocol
- Protocolo **Link State**
- Standard implementado por Cisco y una gran cantidad de fabricantes
- Basado en el algoritmo de SPF/DIJKSTRA
- Uso eficiente de las actualizaciones

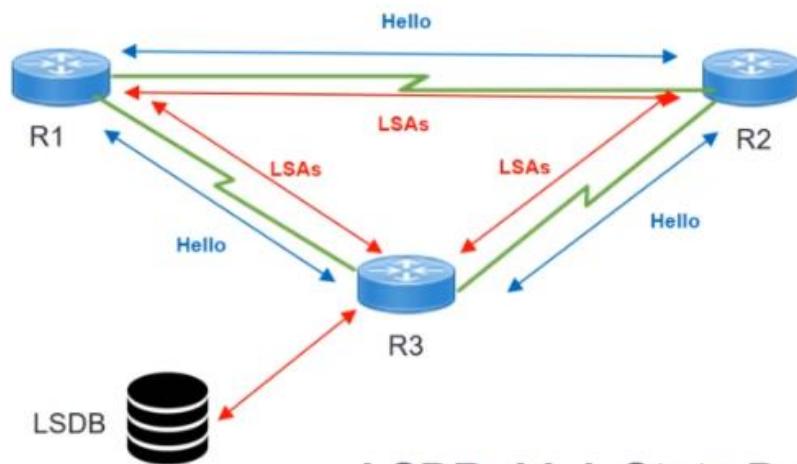
QUE SIGNIFICA LINK STATE?

- Link= Interface del router
- State: Descripción del enlace y su relación con vecinos



LINK STATE EN OSPF

Link-state advertisements (LSA)

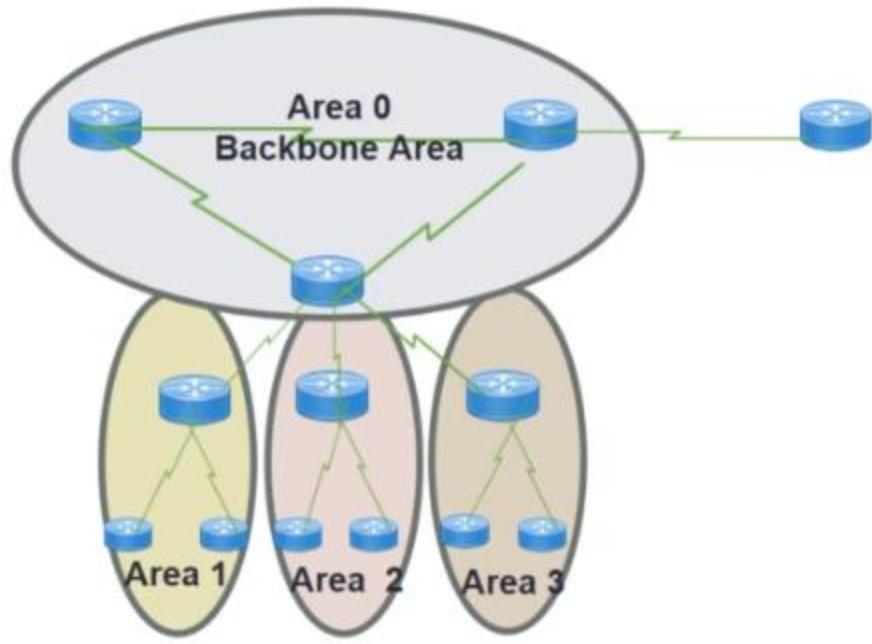


LSDB: Link State Database

OSPF

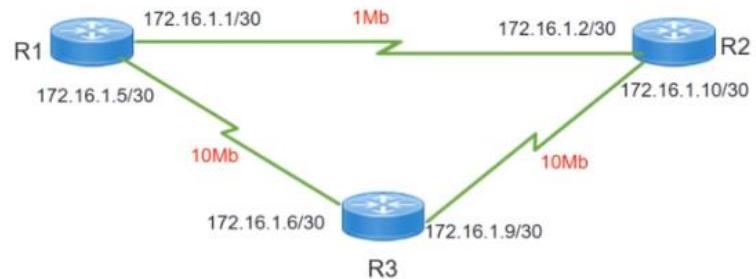
- Distancia administrativa 110
- Usa el concepto de AREAS
- Multicast: 224.0.0.5 por defecto
- Multicast: 224.0.0.6 Redes Multiacceso

AREAS EN OSPF

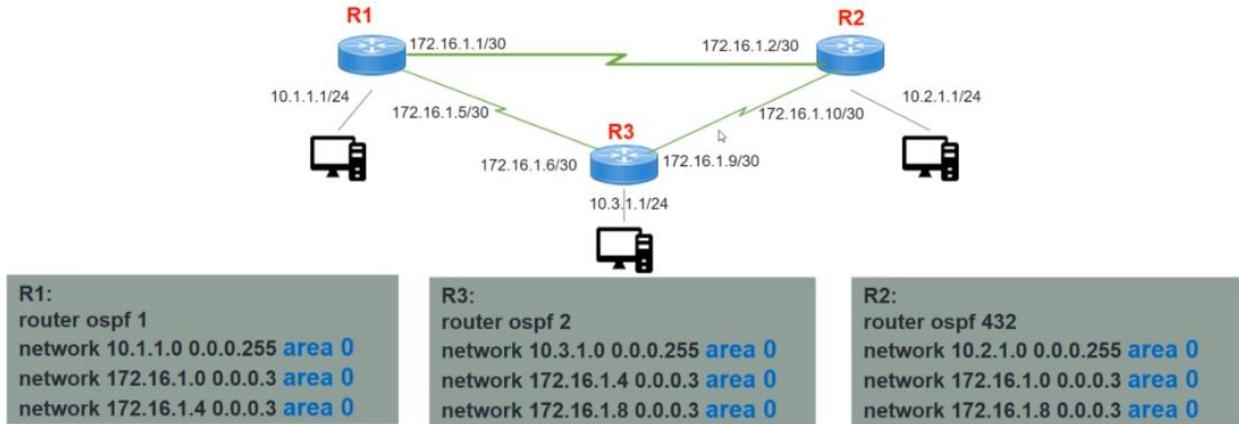


OSPF

- Metrica: Costo
- Soporta VLSM
- Rapida convergencia y escalabilidad
- Autenticacion



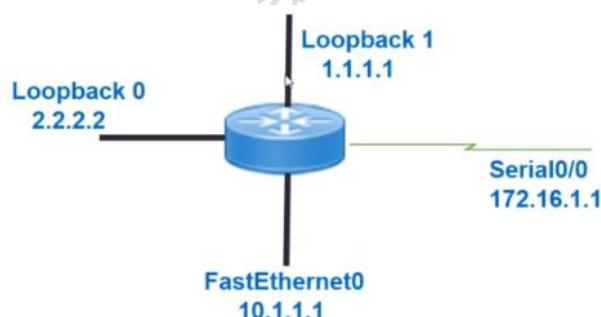
047 OSPF Configuracion basica de OSPF area 0



048 OSPF Router ID

- Cada router selecciona un ID que debe ser único
- Cada router guarda la topología de la red en su base de datos de LSDB y allí cada router debe tener un identificador único.
- 32 bit decimal puntuado (ej. 10.1.1.1)

SELECCIÓN DE ROUTER ID



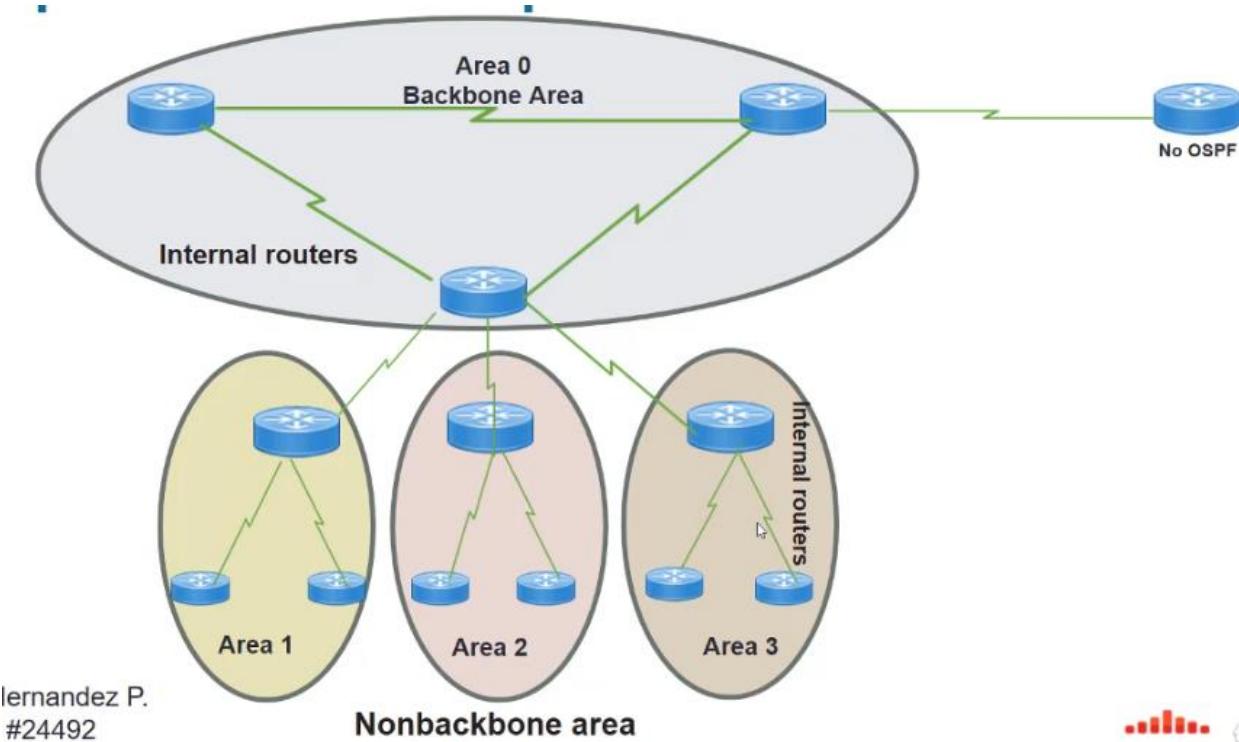
Configuración manual del router ID bajo Router OSPF.

Dirección más alta de interfaces loopback. (no shutdown)

Dirección más alta de cualquier interface que no sea loopback.

049 OSPF Areas

CONCEPTO DE JERARQUIA EN OSPF



Iernandez P.
#24492

CARACTERISTICAS DE LAS AREAS DE OSPF

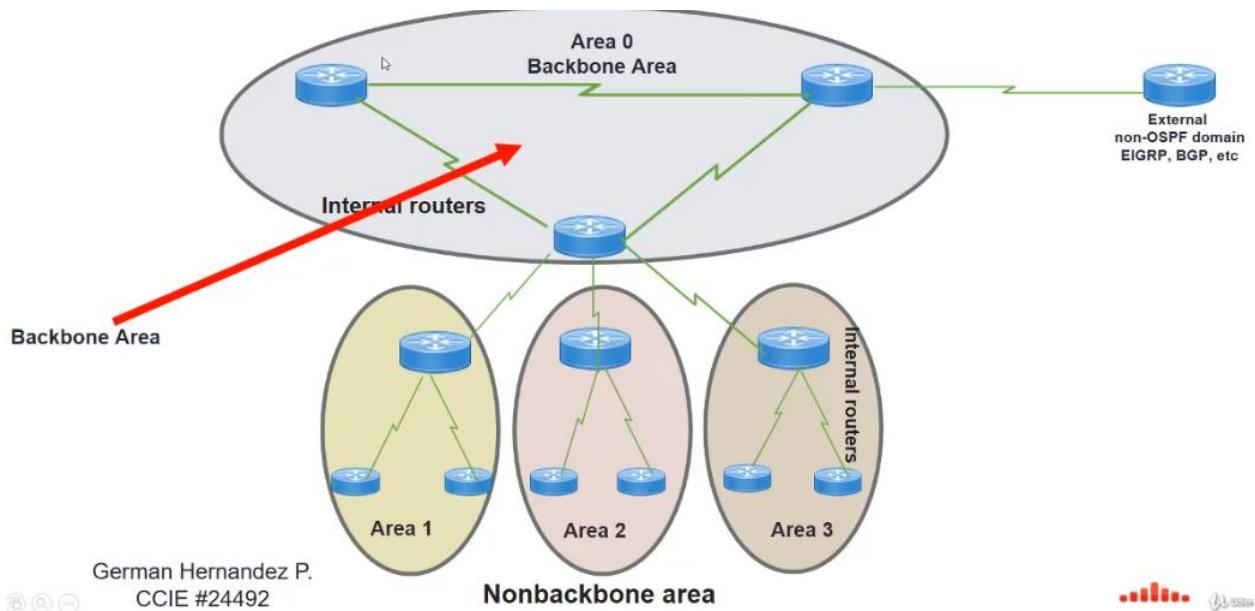
- Se configura con un numero de 32 bits
- Puede ser decimal o decimal con puntos
 - area 0** es lo mismo que **area 0.0.0.0**
 - area 1** es lo mismo que **area 0.0.0.1**

```
router ospf 11
network 10.1.1.0 0.0.0.255 area 0
```

```
interface GigabitEthernet0/0
ip address 10.1.1.1 255.255.255.0
ip ospf 11 area 0
```

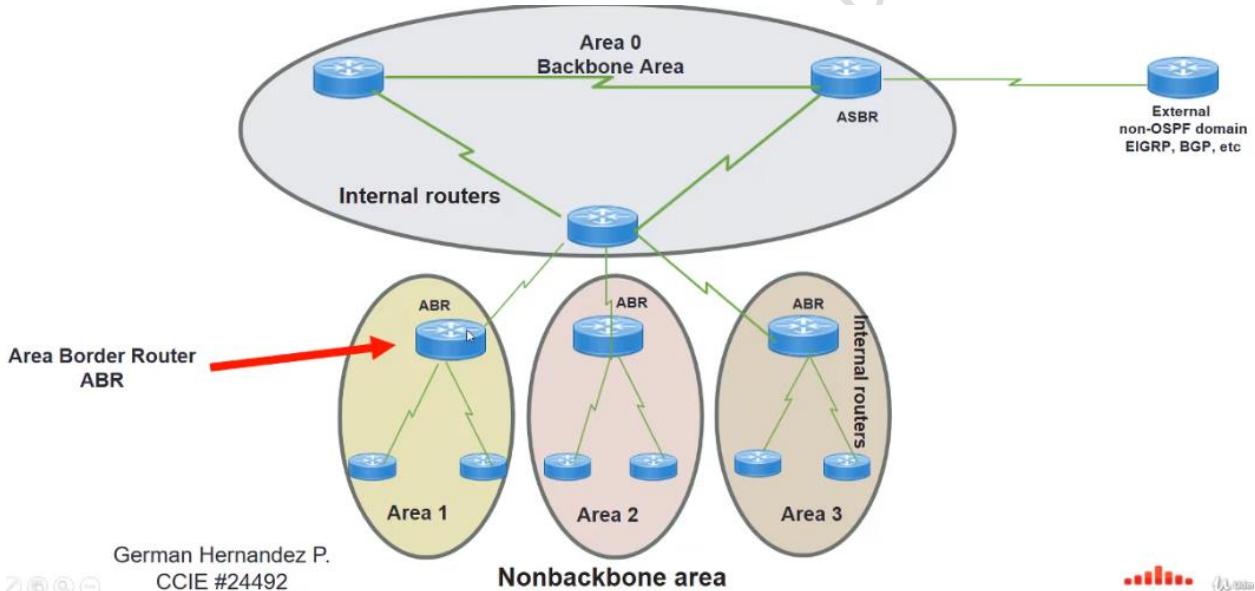
TIPOS DE ROUTERS: BACKBONE

<https://pt.wikipedia.org>



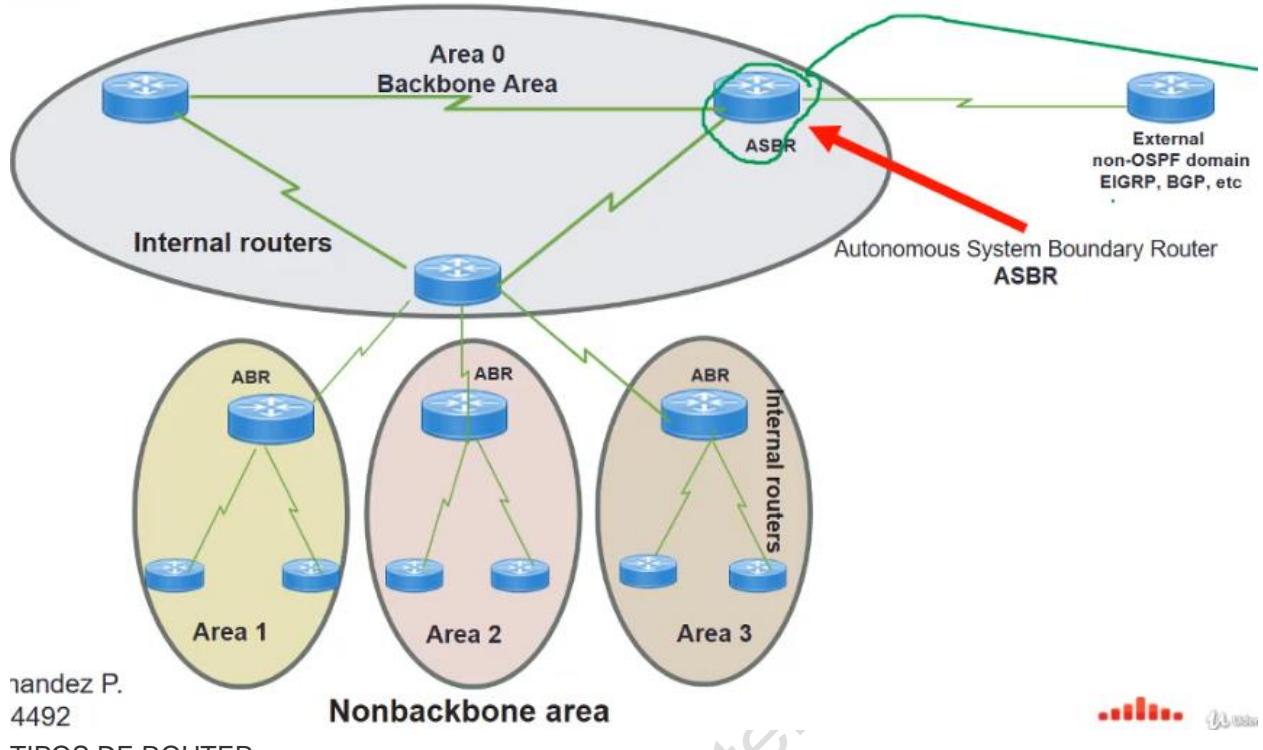
German Hernandez P.
CCIE #24492

TIPOS DE ROUTERS: ABR



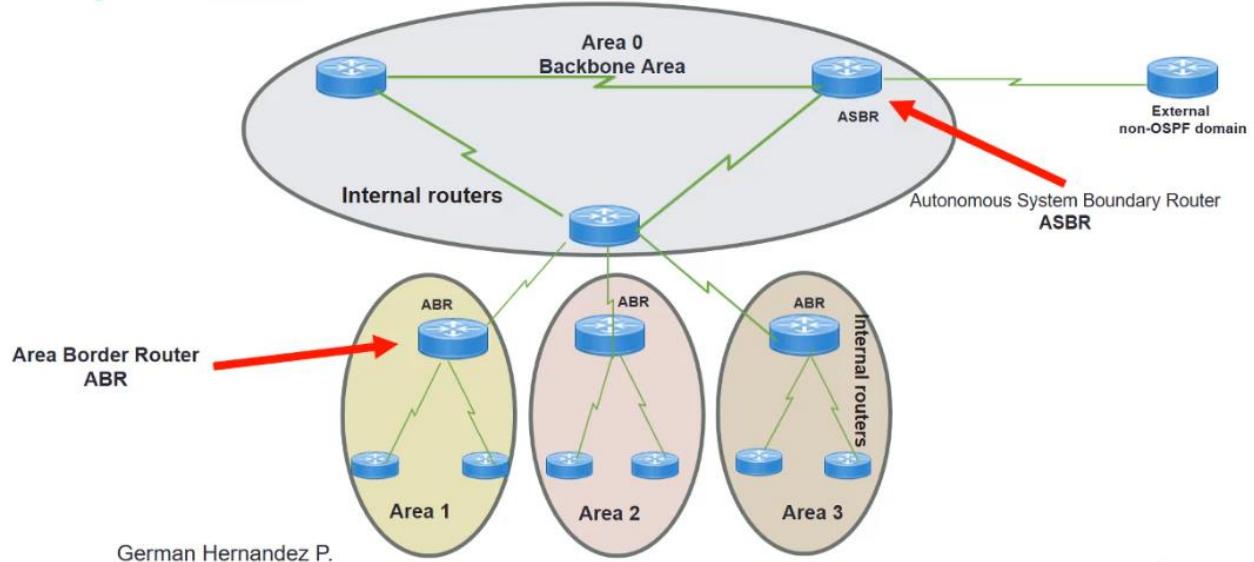
German Hernandez P.
CCIE #24492

TIPOS DE ROUTER: ASBR



Hernandez P.
4492

TIPOS DE ROUTER



Area Border Router
ABR

TIPOS DE AREAS

German Hernandez P.

Stub area: solo rutas internas y la default

Totally Stubby Area: Propietaria de Cisco. Solo rutas para su area y la default.

Not-so-stubby area (NSSA): Solo rutas internas, rutas redistribuidas de procesos OSPF conectados y la default opcionalmente.

Totally NSSA: Propietaria de Cisco. Solo rutas internas, rutas redistribuidas de procesos OSPF conectados y la default.

051 OSPF Metrica

Métrica usada es el Costo

Basado en el ancho de banda de la interfaz *

Mayor ancho de banda = Menor el Costo

Ancho de Banda referencia por default 100Mbps para ethernet

Formula:

Costo=Ancho de banda de referencia / ancho de banda de interface

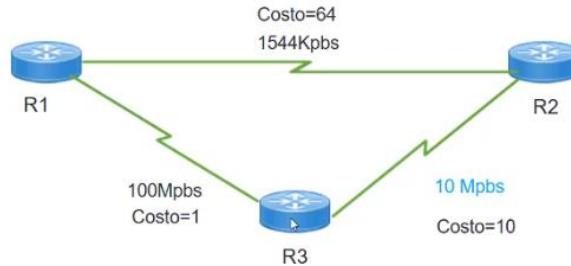
Ancho de banda de referencia: $10^8 = 100.000.000$ bps(bits por segundo) = 100Mbps

ALGUNOS COSTOS DEFAULT

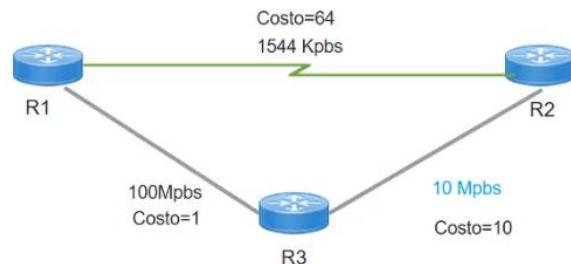
FastEthernet 100Mbps	Interface Serial
Costo=Ancho de banda referencia / ancho de banda interface Costo = $100.000.000 / 100.000.000$ Costo=1	Costo=Ancho de banda de referencia / ancho de banda de interface (1544Kbps default para interfaces serials x 1024) Costo = $100.000.000 / 1581056$ Costo=64

METRICA DE OSPF

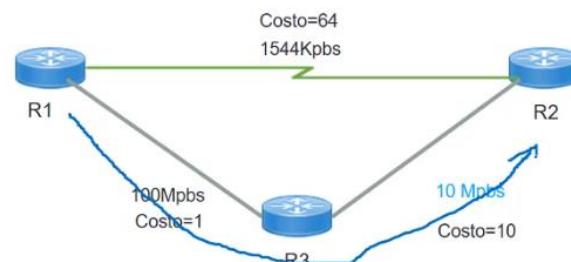
FastEthernet 100Mbps	Interface Serial
<p>Costo=Ancho de banda referencia / ancho de banda interface Costo = $100.000.000 / 100.000.000$ Costo=1</p>	<p>Costo=Ancho de banda de referencia / ancho de banda de interface (1544Kbps default para interfaces serials x 1024) Costo = $100.000.000 / 1581056$ Costo=64</p>



FastEthernet 100Mbps	Ethernet 10Mbps
<p>Costo=Ancho de banda referencia / ancho de banda interface Costo = $100.000.000 / 100.000.000$ Costo=1</p>	<p>Costo=Ancho de banda de referencia / ancho de banda de interface Costo = $100.000.000 / 10.000.000$ Costo=10</p>

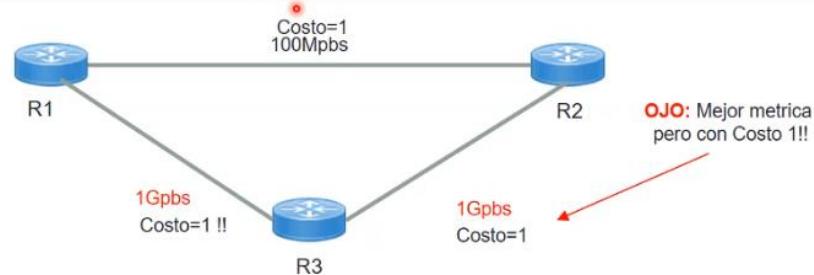


Ruta #1: De R1 a R2	Ruta #2: De R1-R3-R2
Costo=64	Costo= $1+10 = 11$



METRICA DE OSPF INTERFACE DE 1GBPS

1 GigaEthernet 1000Mbps	Ethernet 100Mbps
<p>Costo=Ancho de banda referencia / ancho de banda interface $\text{Costo} = 100.000.000 / 1000.000.000$ $\text{Costo}=0,1$ Se redondea a 1 Costo=1</p>	<p>Costo=Ancho de banda de referencia / ancho de banda de interface $\text{Costo} = 100.000.000/100.000.000$ Costo=1</p>



AJUSTANDO EL COSTO PARA GIGAETHERNET #1

- Se puede ajustar el ancho de Banda de Referencia
- Usar el comando “auto-cost reference bandwidth xx” dentro de router OSPF

```
R2(config)#  
R2(config)#router ospf 12  
R2(config-router)#auto-cost reference-bandwidth 1000  
% OSPF: Reference bandwidth is changed.  
    Please ensure reference bandwidth is consistent across all routers.  
R2(config-router)#[redacted]
```

AJUSTANDO EL COSTO PARA GIGAETHERNET #2

Ajustando el ancho de Bando de la interfaz: Comando Bandwidth dentro de la interfa

German Hernandez P.
CCIE #24492

```
R1(config-if)#int serial 0/0/0
R1(config-if)#bandwidth 128000
R1(config-if)#{^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#sh int Serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 172.16.1.1/30
  MTU 1500 bytes, BW 128000 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation DLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queuing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/0/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 96000 kilobits/sec
  5 minute input rate 57 bits/sec, 0 packets/sec
  5 minute output rate 59 bits/sec, 0 packets/sec
    1274 packets input, 87656 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1258 packets output, 86480 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
R1#
```

AJUSTANDO EL COSTO PARA GIGAETHERNET #3

Ajustando el costo de OSPF en la interfaz: commando “ip ospf cost” dentro de la interface

```
R1(config-if)#int serial 0/0/0
R1(config-if)#ip ospf cost 1
```

052 OSPF Tipos de paquetes

Hello

DBD: Database Description

LSR: Link State Request

LSU: Link State Update

LSAck: Link State Acknowledge

HELLO

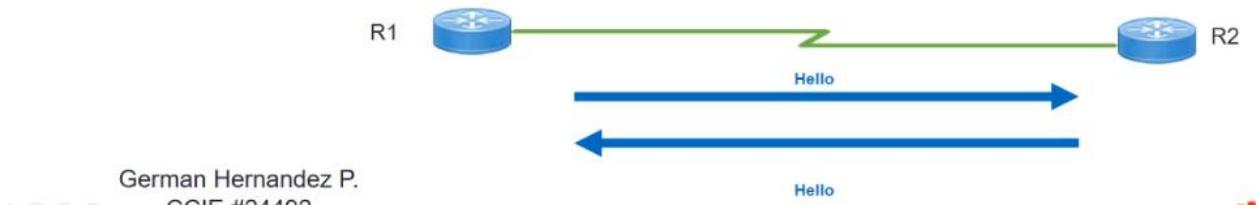
La adyacencia se dara cuando se negocien algunos parametros en comun y otros unicos :

- Router ID Local
- Hello/Dead Interval
- Neighbors (Router ID)
- ID de area Local
- Router Priority
- Network Mask
- DR IP / BDR IP
- Authentication Type
- Auth. Password
- Stub area



German Hernandez P.
CCIE #21102

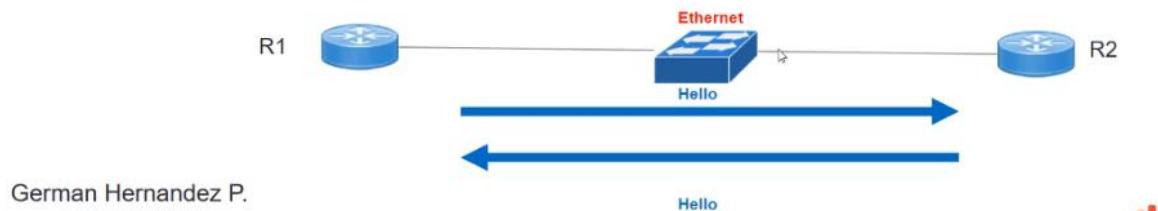
- Los paquetes de Hello se envian periodicamente, este timer se conoce como **Hello Interval**
- Si no se recibe el hello de un vecino en un periodo este se considera como DOWN, y se conoce como **Dead Interval**
- Paquete OSPF Type 1



German Hernandez P.
CCIE #21102
HELLO/DEAD INTERVAL

<https://n...>

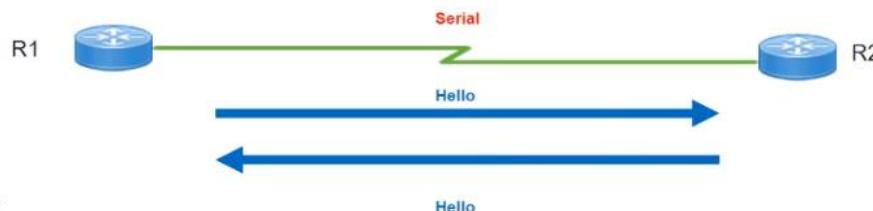
- En redes LAN el **Hello Interval** 10 segundos y el Dead Interval es de 40 segundos. El **dead interval** es 4 veces el Hello Interval
- Multicast 224.0.0.5



German Hernandez P.

En redes Punto a Punto el **Hello Interval** 10 segundos y el Dead Interval es de 40 segundos. El **dead interval** es 4 veces el Hello Interval

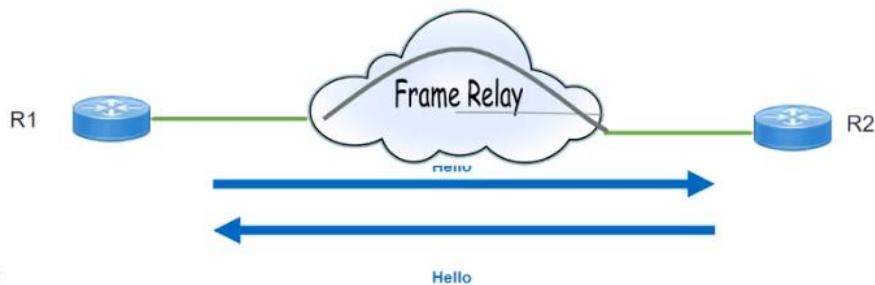
4



German Hernandez P.

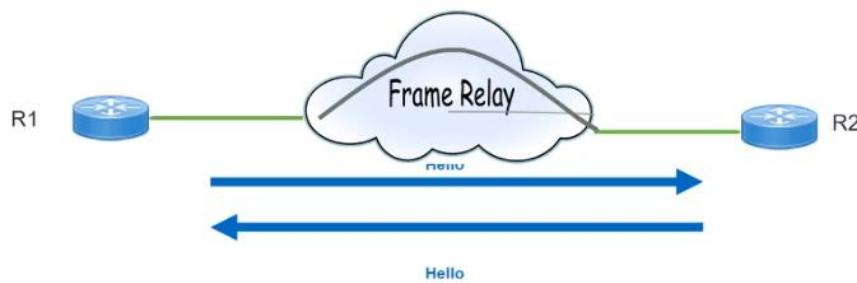
<https://blog/>

- En redes **Point-to-Multipoint (broadcast) Network** el **Hello Interval** es de 30 segundos y el **Dead Interval** es de 120 segundos. El **dead interval** es 4 veces el Hello Interval
- Multicast 224.0.0.5



German Hernandez P.

- En redes **Point-to-Multipoint (non-broadcast) Network** el **Hello Interval** es de 30 segundos y el **Dead Interval** es de 120 segundos. El **dead interval** es 4 veces el Hello Interval
- Unicast



German Hernandez P.

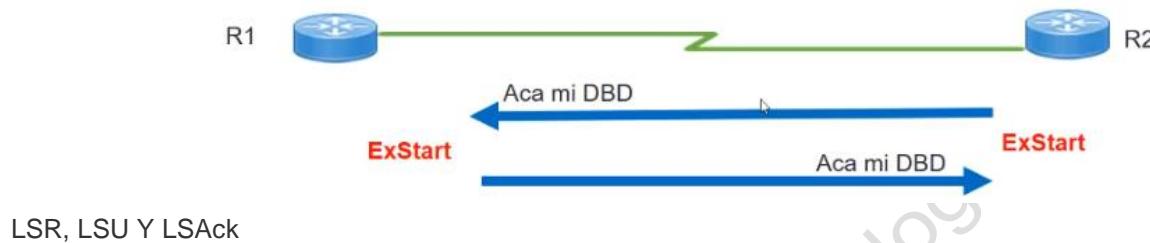
DBD

<https://blog/>

Usado para verificar si la LSDB entre 2 routers es la misma. Es un resumen de la LSDB.

Paquete OSPF Type 2

Se utilizan para asegurarse que estén sincronizados.



LSR: Solicita un registro específico del estado de enlace de un vecino. Paquete OSPF Type 3.

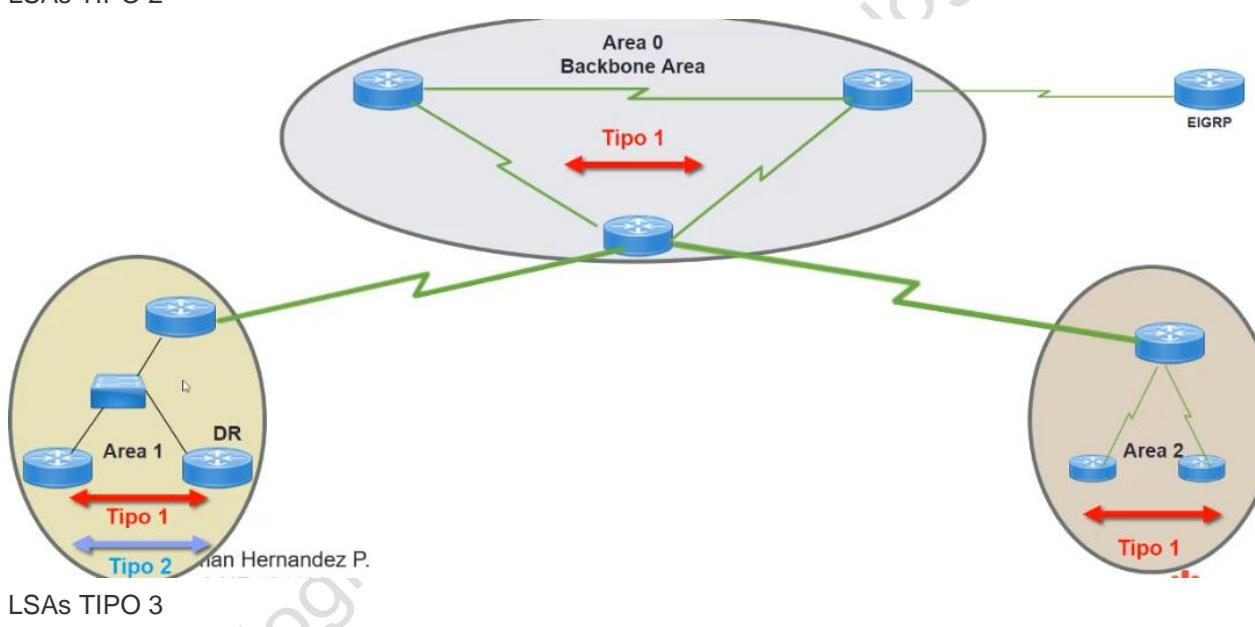
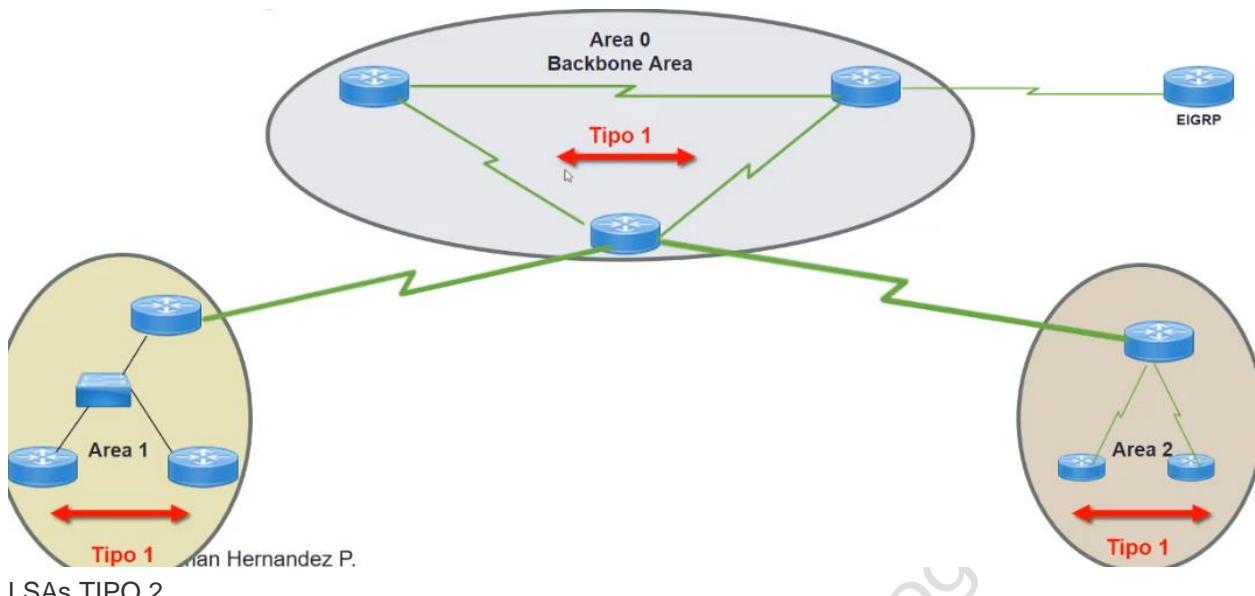
LSU: Envía registros específicos de un estado de enlace solicitado. Básicamente es un repositorio con varios LSAs. Paquete OSPF Type 4.

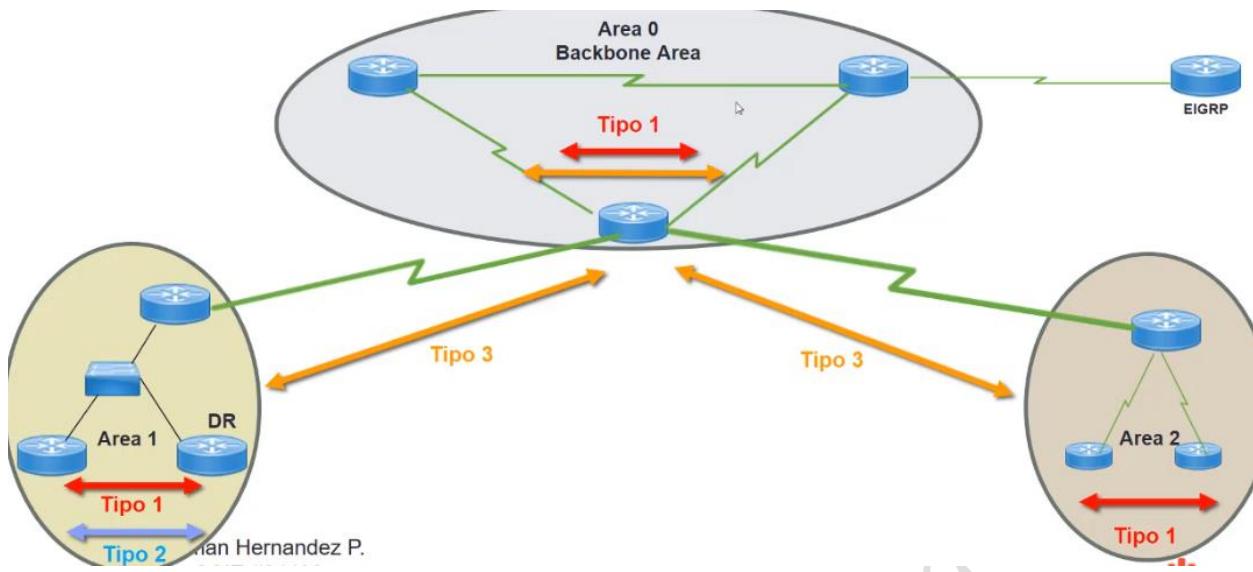
LSAck: Confirmación de recibido. Paquete OSPF Type 5.



053 OSPF Tipos de SLAs

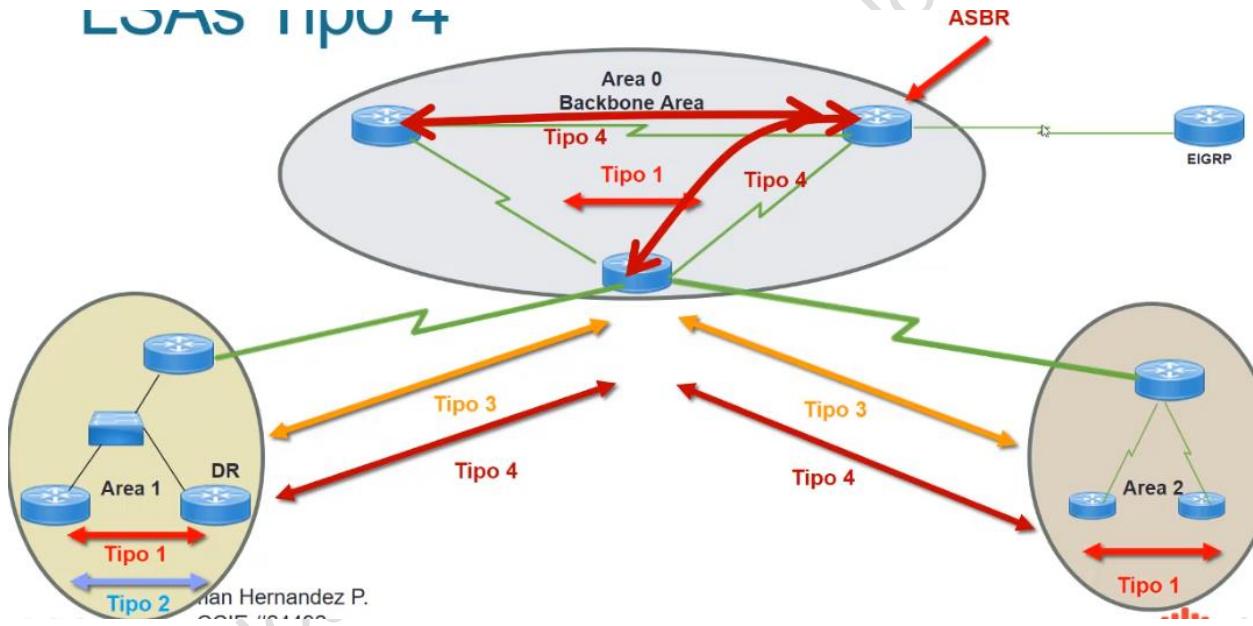
LSA TIPO 1





LSAs TIPO 4

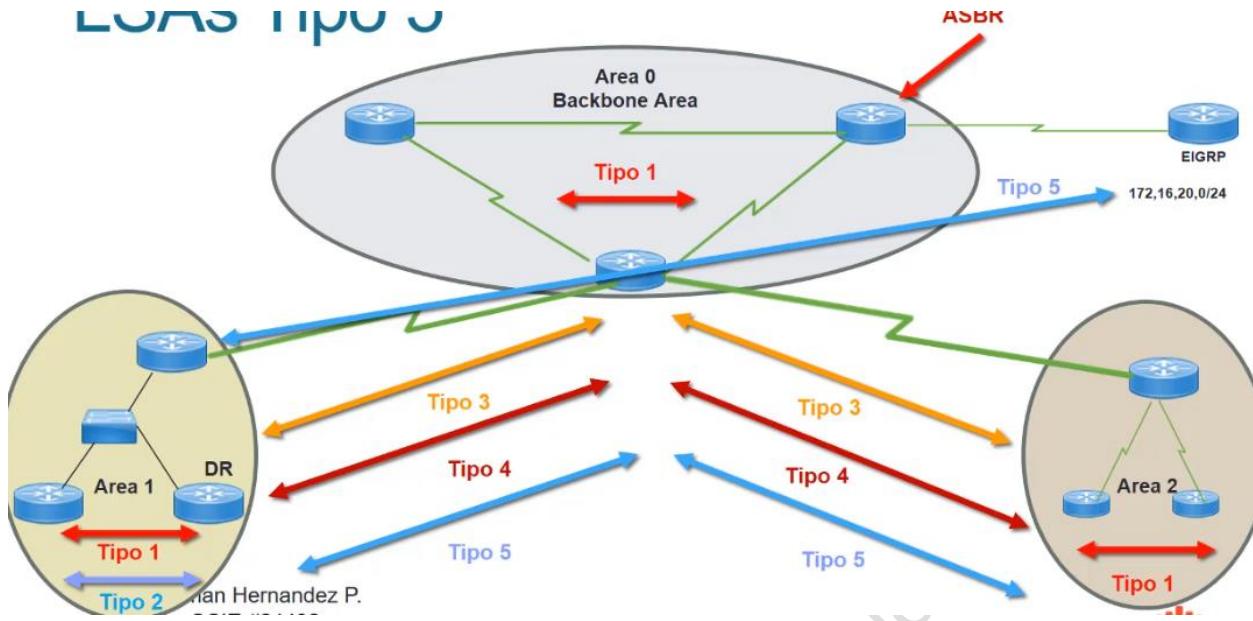
LSAs TIPO 4



LSAs TIPO 5

<https://blco.com>

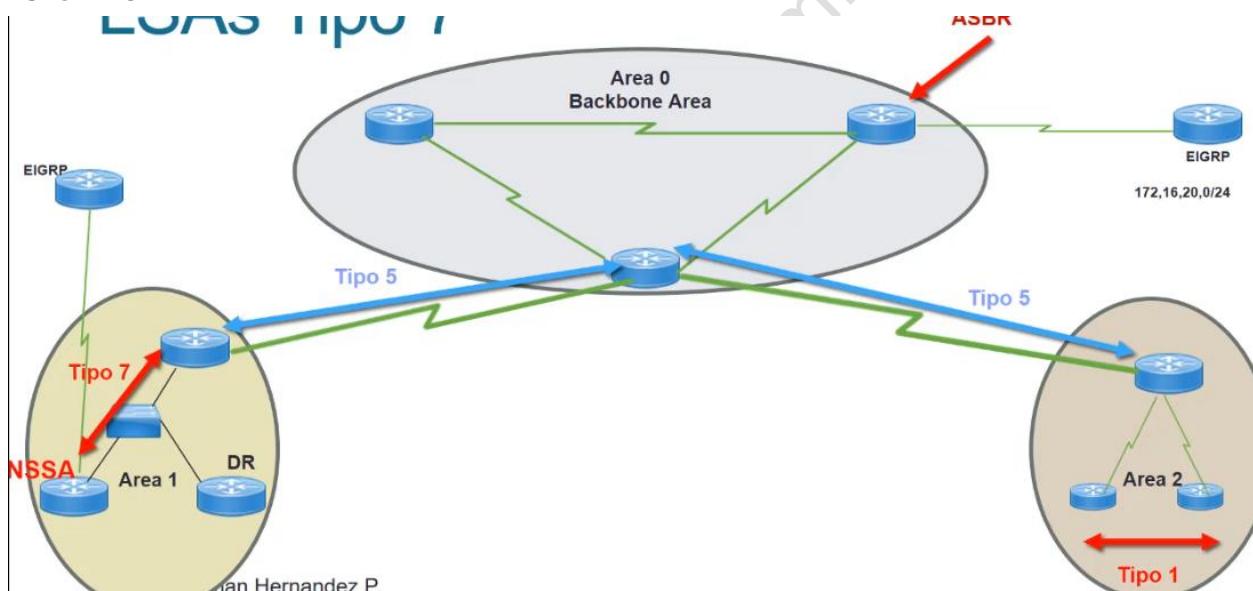
LSDS TIPO 5



LSAs TIPO 6 NO USADAS

LSAs TIPO 7

LSDS TIPO 7



COMO SE MUESTRAN EN LA TABLA DE ENRUTAMIENTO

<https://rechner.club>

```

R21#sh ip ro
Codes: L - local, C - connected, S - static, 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

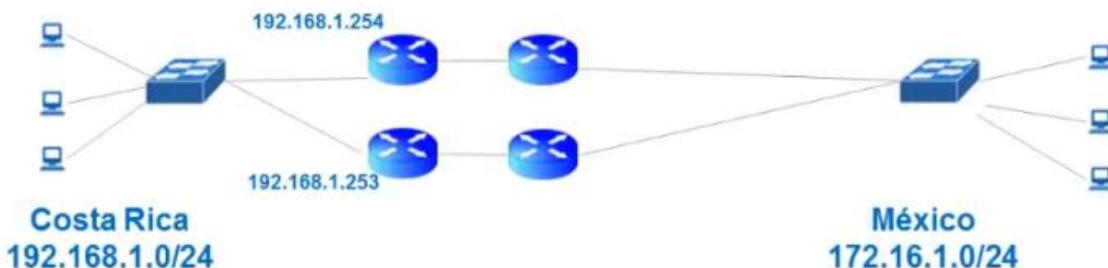
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O IA   10.1.1.0/24 [110/129] via 172.16.1.13, 00:04:27, Serial0/0/0
O IA   10.2.1.0/24 [110/129] via 172.16.1.13, 00:04:17, Serial0/0/0
O IA   10.3.1.0/24 [110/65] via 172.16.1.13, 00:04:42, Serial0/0/0
C     10.20.1.0/24 is directly connected, GigabitEthernet0/0
L     10.20.1.1/32 is directly connected, GigabitEthernet0/0
O IA   10.30.1.0/24 [110/192] via 172.16.1.13, 00:04:27, Serial0/0/0
O IA   10.31.1.0/24 [110/192] via 172.16.1.13, 00:04:27, Serial0/0/0
      20.0.0.0/24 is subnetted, 1 subnets
O E2   20.1.1.0/24 [110/100] via 172.16.1.13, 00:04:27, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
O IA   172.16.1.0/30 [110/192] via 172.16.1.13, 00:04:17, Serial0/0/0
O IA   172.16.1.4/30 [110/128] via 172.16.1.13, 00:04:27, Serial0/0/0
O IA   172.16.1.8/30 [110/128] via 172.16.1.13, 00:04:42, Serial0/0/0
C     172.16.1.12/30 is directly connected, Serial0/0/0
L     172.16.1.14/32 is directly connected, Serial0/0/0
O IA   172.16.1.16/30 [110/128] via 172.16.1.13, 00:04:27, Serial0/0/0
      192.168.1.0/30 is subnetted, 1 subnets
O E2   192.168.1.0/30 [110/100] via 172.16.1.13, 00:04:27, Serial0/0/0

```

055 First Hop Redundancy Protocol Introducción a HSRP y VRRP

HSRP

- Hot StandBy Router Protocol
- Protocolo que permite implementar routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.
- Propietario de Cisco.



Crea una Virtual IP address y una Virtual Mac-address para realizar la redundancia.

Existen tres tipos de routers :

Active Router : Es el router activo que recibe el trafico para ser reenviado a su destino .

Standby Router : Es el router de backup en caso de que el Active Router se no este disponible.

Virtual Router : No es un router, pero representa al grupo HSRP como un router virtual y es el actual default gateway para los hosts.

COMO FUNCIONA?

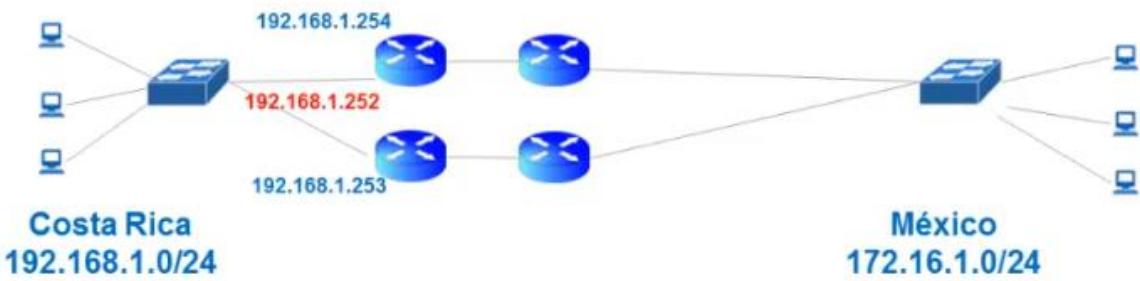
- Se crea un grupo de routers y una dirección IP virtual, en donde se define un router master que enruta el tráfico.
- Los demás están en StandBy en caso de fallo.
- Funciona la capa 3 del modelo OSI
- Entre los routers del grupo HSRP se intercambian mensajes "hello" cada 3 segundos, para conocer el estado en el que se encuentran.
- Estos mensajes utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985

Si el router maestro no envía mensajes tipo hello a los routers respaldo dentro de un periodo de tiempo (10 segundos), otro router del grupo se coloca como router maestro.

Esto consiste en que el nuevo router obtiene la dirección virtual que identifica al grupo.

Para determinar cuál es el router maestro se establece una prioridad en cada router (**0 – 255**). La prioridad por defecto es 100. El router de mayor prioridad es el que se establecerá como activo.

El router en espera toma el lugar del router maestro, una vez que el temporizador holdtime.



EJEMPLO DE CONFIGURACION DE HSRP

```
R1(config)# interface GigE 0/1
R1(config-if)# ip address 192.168.1.2 255.255.255.0
R1(config-if)# standby 1 ip 192.168.1.1
R1(config-if)# standby 1 priority 200
R1(config-if)# standby 1 preempt
```

```
R2(config-if)# ip address 192.168.1.3 255.255.255.0
R2(config-if)# standby 1 ip 192.168.1.1
R2(config-if)# standby 1 preempt
```

VRRP

- Virtual Router Redundancy Protocol (Protocolo de Redundancia de Router Virtual)
- Estandar IEEE (RFC 2338)
- El router Virtual que representa los router se conoce como VRRP group.
- El router activo se conoce como master virtual router.
- Utiliza la dirección multicast **224.0.0.18**
- VRRP esta soportado en Ethernet, Fast Ethernet, and Gigabit Ethernet asi como en Multi-protocol Label Switching (MPLS) virtual private networks (VPNs) y VLANs.

EJEMPLO DE CONFIGURACION DE VRRP

```
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
```

056 OSPF v3

Open Shortest Path First Version 3.
Desarrollado para el soporte de IPv6.
Utiliza IPv6 como transporte.
Utiliza el algoritmo SPF.

Tiene tablas de adyacencia, tablas de topología y tablas de IP routing al igual que OSPFv2 pero son independientes.

CARACTERISTICAS

Estado de enlace.

Algoritmo de enrutamiento: SPF

Métrica: costo.

Áreas: para minimizar la saturación de estado de enlace y tener mayor estabilidad con el dominio OSPF.

Tipos de paquetes OSPF: Hello, DBD, LSR, LSU y LSAck

Mecanismo de descubrimiento de vecinos: mensajes tipo Hello.

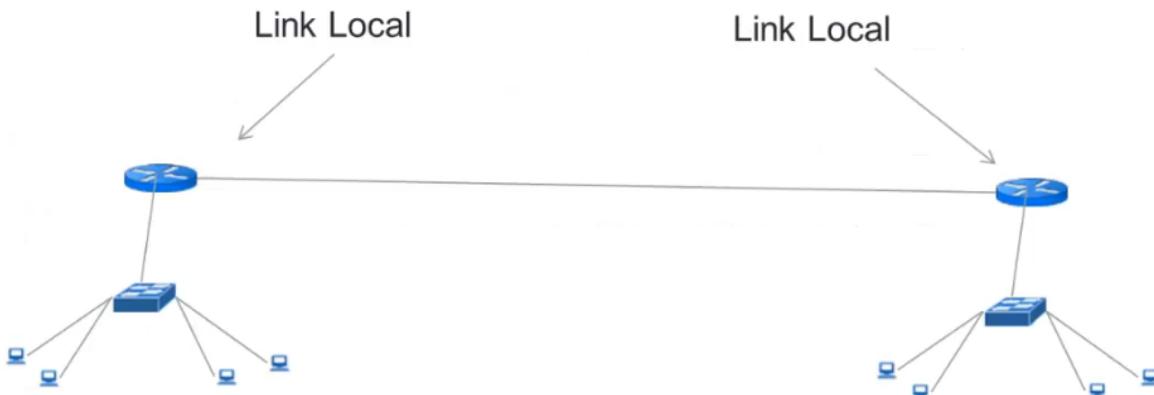
Proceso de elección del DR/BDR

ID del router: 32 bits. Por lo general, se trata de una dirección IPv4.

- **Anuncios:** OSPFv3 utilizando IPv6.
- **Dirección de origen:** link-local de la interfaz de salida.
- **Dirección de multicast :** OSPFv3 utiliza la dirección FF02::5.
- **Dirección de multicast de DR/BDR:** OSPFv3 utiliza la dirección FF02::6.
- **Anuncio de redes:** dentro de la interface: ***ipv6 ospf id-proceso area id-área.***
- **IP Routing :** global: ***ipv6 unicast-routing***.

DIRECCIONES LINK LOCAL

Origen: Dirección Link Local –Destino: Dirección Multicast:FF02::5 o FF02::56



CONFIGURACION

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

VERIFICACION

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

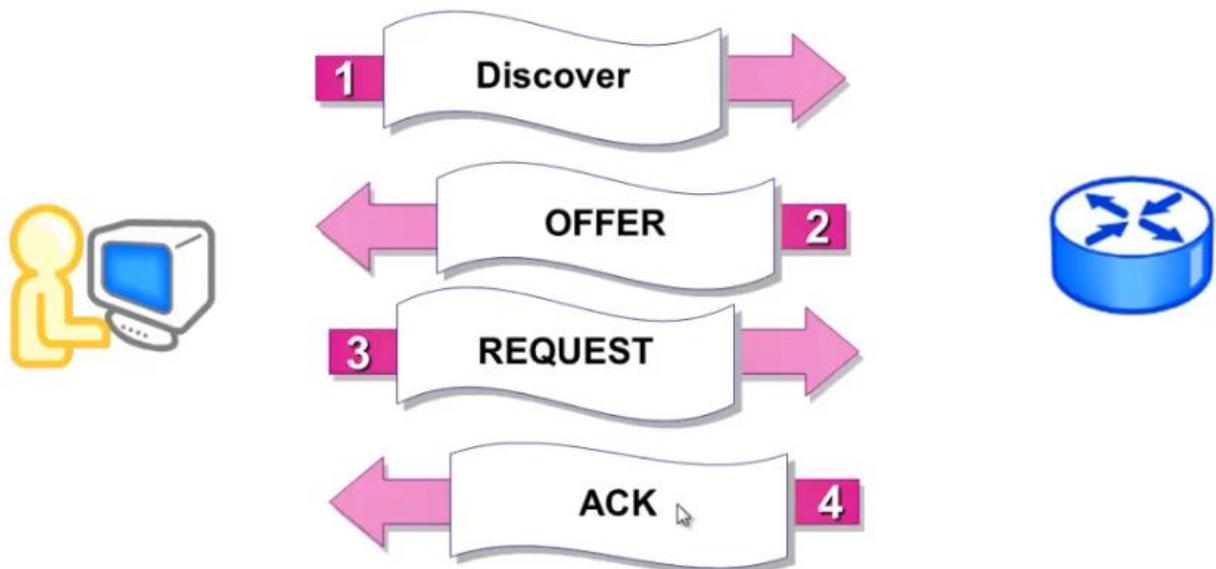
09 Servicios IP

057 DHCP

Que es DHCP

- Dynamic Host Configuration Protocol (DHCP)
- Protocolo que permite que un equipo conectado a una red pueda obtener su configuración de red en forma dinámica.
- Objetivos principales: simplificar la administración eficiente de la red, evitar errores respecto a la configuración IP e incluso disminuir el desperdicio de direcciones IP en la red.

Proceso DHCP



PAQUETES DHCP

DHCPDISCOVER: Paquete broadcast para ubicar servidores DHCP disponibles

DHCPOFFER : Paquete broadcast de respuesta del servidor a un paquete DHCPDISCOVER informando que hay presencia de un servidor DHCP disponible.

DHCPREQUEST: Paquete unicast de solicitudes varias del cliente al servidor DHCP disponible.

DHCPACK: Paquete de respuesta del servidor que contiene los parámetros solicitados por el cliente.

DHCPNAK: Paquete de respuesta del servidor para indicarle al cliente que su concesión ha vencido o en caso de que el cliente anuncie configuración de red errónea.

DCHPDECLINE: Paquete del cliente informando al servidor que la dirección ya está en uso.

DHCPRELEASE: Paquete del cliente liberando su dirección IP.

DHCPIINFORM: Paquete del cliente solicitando parámetros locales, ya tiene su dirección IP.

PASO #1: EXCLUIR DIRECCIONES IP

ip dhcp excluded-address

Ejemplo:

Router(config)# ip dhcp excluded-address 192.168.1.1

PASO #2: CREAR UN POOL DE DIRECCIONES IP

Comando:

ip dhcp pool name

Ejemplo:

Router(config)# ip dhcp pool dpool1

Router(config-dhcp)#

PASO #3: CONFIGURAR LAS OPCIONES DENTRO DE POOL

Comando:

ip dhcp pool *name*

network *red*

default-router *default gateway*

dns-server *direccion ip*

domain-name *dominio*

Ejemplo:

ip dhcp pool dpool1

network 10.10.0.0 255.255.255.0

default-router 10.10.10.10

dns-server 192.168.35.2

domain-name cisco.com

PASO #4: VERIFICAR LA CONFIGURACION

Comando:

show ip dhcp binding

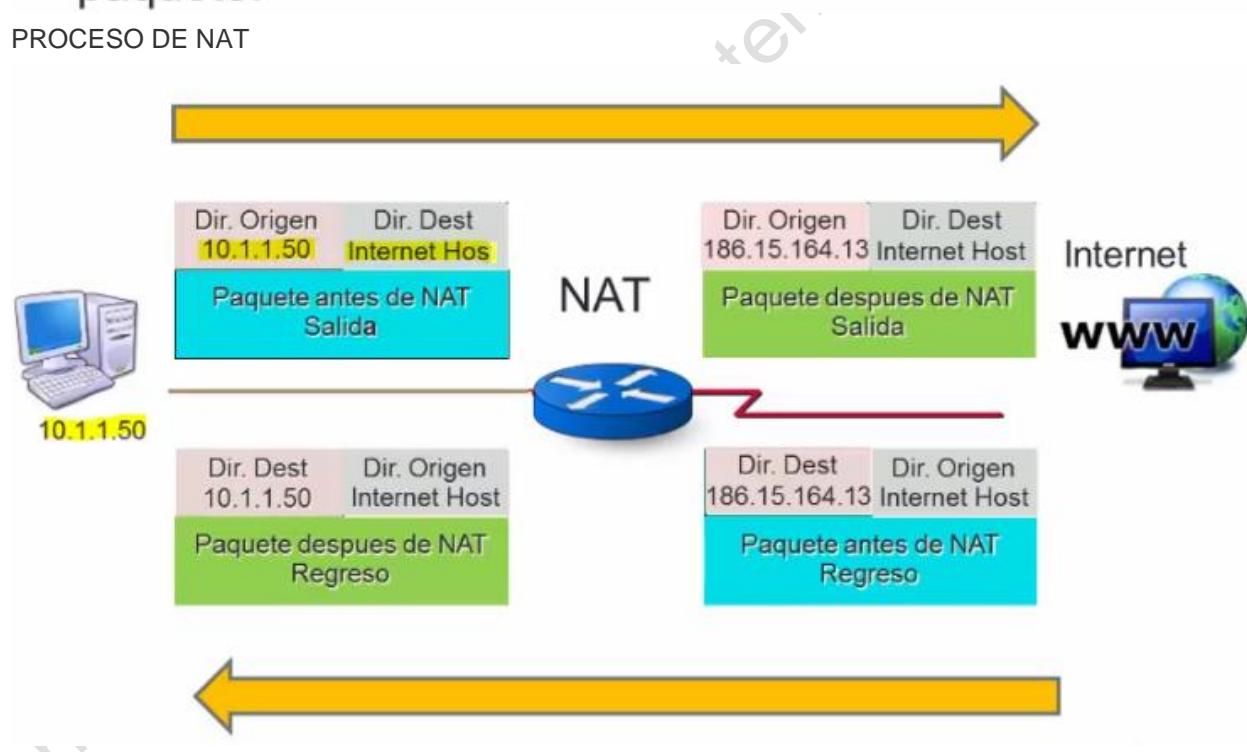
show ip dhcp pool

058 NAT Introducción a NAT y PAT

QUE ES NAT?

- Network Address Translation
- Proceso de Traducción de direcciones de red: públicas en privadas
- Diseñado para conservar las direcciones IP públicas
- Permite:
 - Acceder a Internet al traducir las direcciones PRIVADAS de la LAN en una dirección PÚBLICA
 - Esto aplica por ejemplo para usuarios navegando en internet o servidores accedidos desde internet.
 - Según la definición oficial del RFC 1631 es el proceso de cambiar la dirección por otra en el encabezado del paquete.

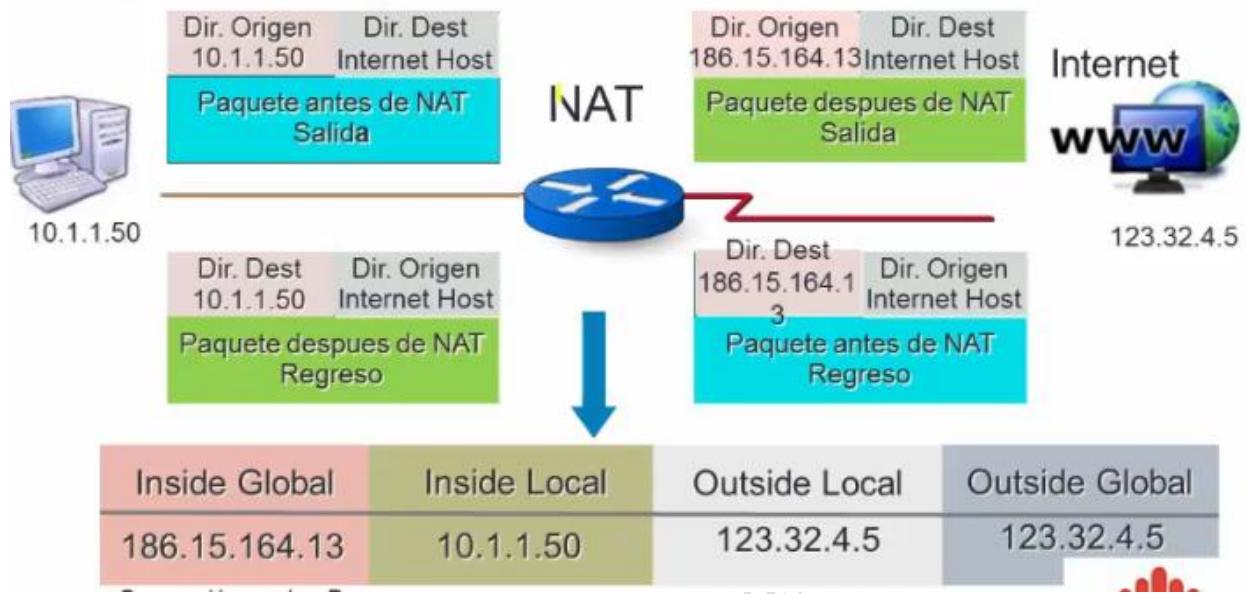
PROCESO DE NAT



Una dirección IP es o LOCAL o GLOBAL

Las direcciones LOCAL se ven en la red interna

Las direcciones IP GLOBAL se ven en la red externa



TIPOS DE NAT

- **Estático:**

- Se ingresan directamente en la configuración y siempre están en la tabla de traducción:

ip nat inside source static 10.1.1.50 171.69.68.10

- Usado principalmente para servidores que deban usar una dirección IP fija siempre.

- **Dinámico:**

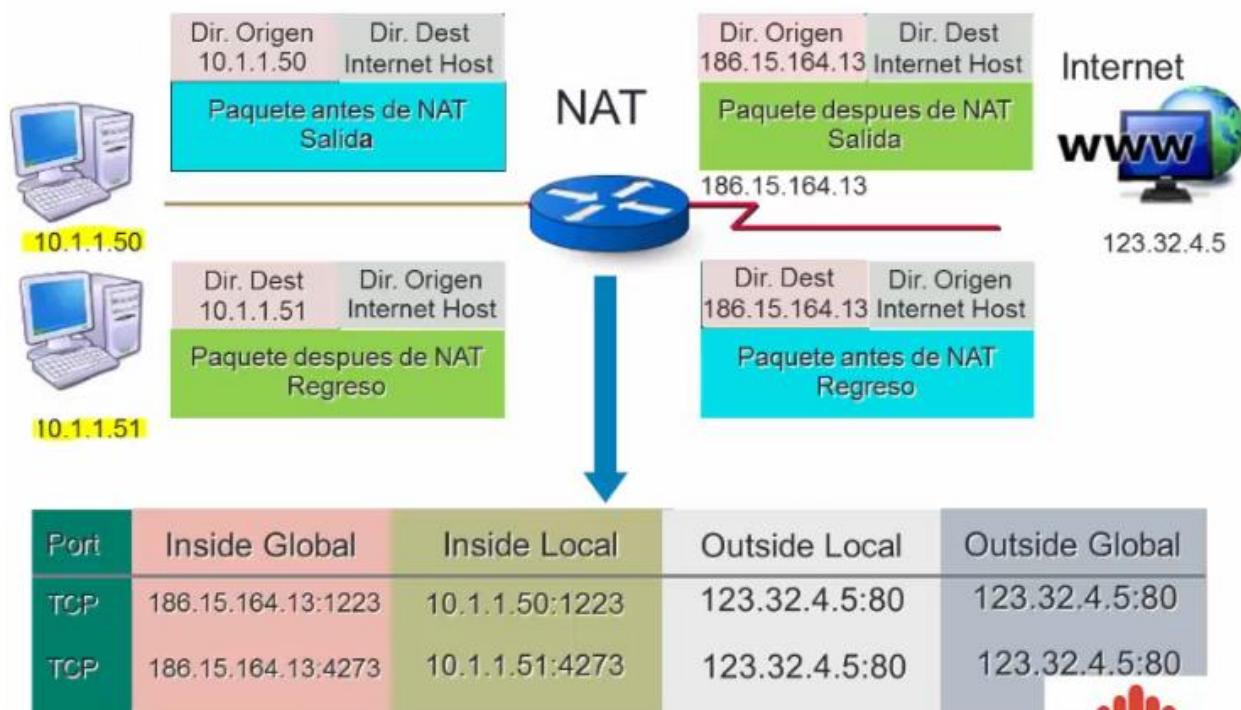
- Utiliza una lista de acceso para identificar las direcciones a las cuales se les debe hacer NAT:

ip nat inside source list 1 pool nat-pool

access-list 1 permit 10.0.0.0 0.255.255.255

- Usado para que los hosts internos de la LAN puedan acceder a Internet

- Permite que varias direcciones internas salgan hacia internet usando la misma dirección IP Pública.
- El PAT además de direcciones IP incluye puertos en la traducción.
- Cuando no hay suficientes direcciones IP para traducir 1 a 1. Ósea traducción de mucho a uno
- Un puerto origen ÚNICO para cada IP origen, permite identificar las traducciones.
- También conocido como NAPT en alguna documentación.
- También se conoce como la sobrecarga de NAT.



062 Calidad de Servicio (QoS)

QoS

Calidad de servicio:

Habilidad de los equipos para ofrecer mayor prioridad a un tipo de tráfico determinado.

Ancho de Banda sin QoS



Ancho de Banda con QoS



German Hernandez P.
CCIE #24492

NECESIDAD DE QoS

Tráfico de voz y video es muy sensible al retardo (delay), la pérdida de paquetes (packet lost) y el jitter (variación en el retardo).

Por ejemplo esto causa:

- audio entrecortado eco, o pausas excesivamente largas en la conversación.
- Video entrecortado

Ancho de Banda sin QoS



Ancho de Banda con QoS



German Hernandez P.
CCIE #24492

EN QUE AYUDA QoS

Garantiza ancho de banda para una aplicación o tipo de tráfico.

Reduce la latencia

Disminuye la perdida de paquetes

Reduce el jitter



German Hernandez P.
CCIE #24492

QUE TIPOS DE PROBLEMAS SE PUEDEN PRESENTAR

Parámetro	Unidad de medida	Descripción
Ancho de Banda o Bandwidth insuficiente	Kb/s	Cantidad de paquetes que se puede enviar a través de una conexión de red en un período de tiempo dado.
Retardo o delay	ms	También conocido como latencia y es promedio de tiempo que tardan en llegar los paquetes
Jitter	ms	Variaciones en el tiempo de llegada de los paquetes debido al delay.
Packet loss (Tasa de pérdidas)	%	Proporción de paquetes que no pudieron llegar a su destino

MECANISMOS DE QoS

- **Best Effort**

Es el default asi que no hay prioridad

- **Integrated Services Model – IntServ**

RSVP – Una ruta de QoS pre negociada de extremo a extremo.

- **Differentiated Services Model – DiffServ**

Cada salto (router) prioriza el trafico de acuerdo a una configuracion.

NECESIDAD DE ETIQUETAR EL TRAFICO (TAG)

- **Layer 2 – CoS – Class of Service field.**

- 3 bits 0-7 value
- Campo presenta tanto en encapsulaciones ISL como 802.1Q/P

- **Layer 3 – ToS – Type of Service field.**

- 3 bits 0-7 value Only relevant to IP
- Algunas veces conocido como “IP Precedence”

- **Layer 3 – DSCP – Differentiated Services Code Point**

- Supersedes ToS
- 6 bits (3 primeros bits son ToS) 0-63 value

0 es la prioridad mas baja!

DONDE MARCAR EL TRAFICO

Depende de las capacidades de los hosts, switches y routers en la red.

Algunas veces se usan diferentes tecnicas de marcado en diferentes puntos de la red.

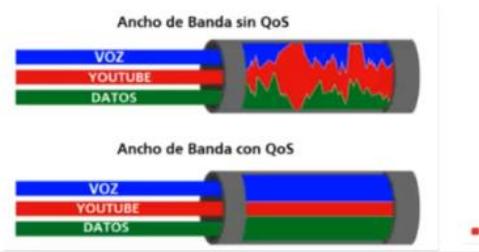
Por ejemplo es bastante comun el usar DSCP en los routers y marcar las tramas CoS en los switches.

MODULAR QoS COMMAND LINE INTERFACE MQC

Modelo de implementación de QoS basado en el IOS.

El modelo divide las tareas en:

- Identificar flujos de tráfico
- Clasificar los flujos de tráfico que pertenezcan a una clase común de QoS.
- Aplicar políticas de QoS a esa clase.
- Definir a las interfaces en las cuales la política será aplicada.



German Hernandez P.
CCIE #24492

LA CLASIFICACION DEL TRAFICO DE MQC EL CLASS MAP

- Se usa para asociar uno o varios atributos con el trato de QoS que se le dará a ese tráfico.
- Los atributos disponibles varían dependiendo del hardware

Ejemplo:

```
Switch(config)# class-map match-any critico
Switch(config-cmap)# match interface fastethernet
0/1
```

Cualquier tráfico que ingrese a esa interfaz se denomina critico.

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

LA CLASIFICACION DEL TRAFICO DE MQC EL POLICY MAP

Se usa para crear la política de tráfico (traffic policy). Su propósito es configurar las características de QoS que deben ser asociadas con el tráfico que se clasifica en el class map. Contiene 3 elementos:

- Nombre del Policy
- Traffic class (se especifica con el comando class)
- Políticas QoS que se aplican a cada clase.

Ejemplo:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class critico
Switch(config-pmap-c)# bandwidth 5000
```

En este caso se le da un ancho de banda de 5000 kbps al tráfico calificado como "critical" por el class-map definido anteriormente.

MQC:APLICACIÓN DE LA POLITICA A LA INTERFAZ

Como en una lista de acceso, se debe aplicar el service-policy a una interfaz específica ya sea al tráfico "input" o "output"

```
Switch(config)# interface gigaethernet 0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

063 Acceso remoto por SSH

QUE ES SSH

Secure Shell

Permite conexiones remotas encriptadas.

Estandar

Más seguro que Telnet.

Disponible en los equipos Cisco.

Encriptación robusta de 128 bits.

CONFIGURANDO SSH

Comando	Descripción
Switch(config)#username German password hvredes ↳	Crea un usuario y una contraseña local
Switch(config)#ip domain-name hvredes.com	Crea un dominio de host en el switch
Switch(config)#crypto key generate rsa	Activa el servidor SSH para la autenticación local y remota, además genera una clave RSA
Switch(config)#ip ssh version 2	Configura el switch para que corra SSH versión 2
Switch(config)#line vty 0 15 Switch(config-line)#login local	Ingresar a la configuración VTY Autentica la interfaz VTY con las credenciales locales
Switch(config-line)#transport input ssh	Configura el protocolo de comunicación SSH
Switch#show ip ssh	Despliega que servidor SSH está activo y la versión e información de configuración
Switch#show ssh	Muestra el estado del servidor SSH

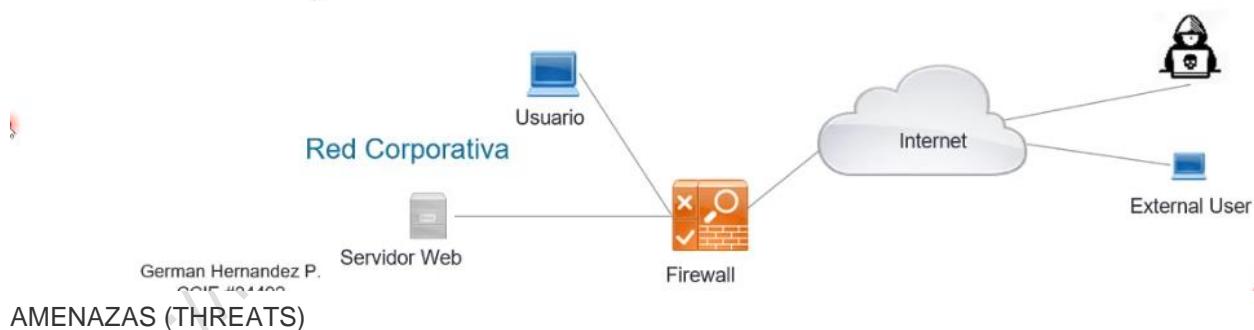
10 Seguridad

065 Conceptos básicos de seguridad

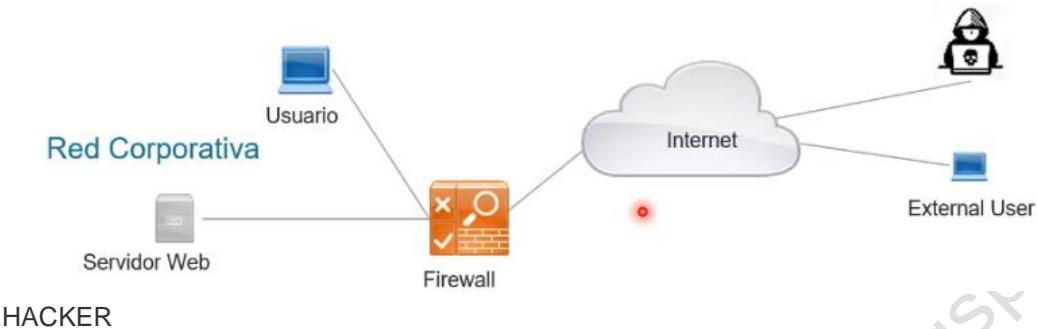
SEGURIDAD INFORMATICA O CIBERSEGURIDAD

Definición de Cisco:

- “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 en una red”

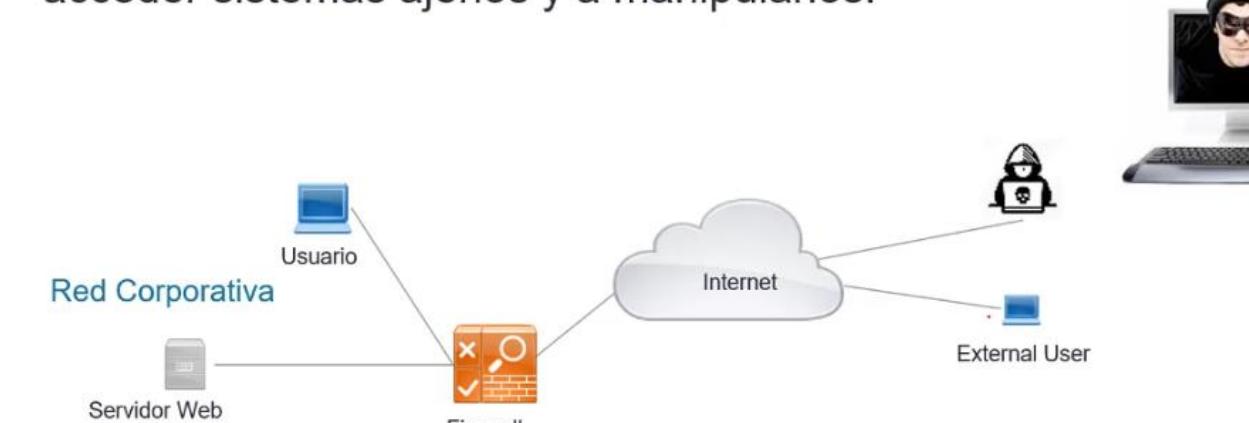


- Intentos maliciosos para comprometer la seguridad
- Malware, Ramsomware, Phising, DoS, Computer virus, Trojan horse, Rootkit, Botnet



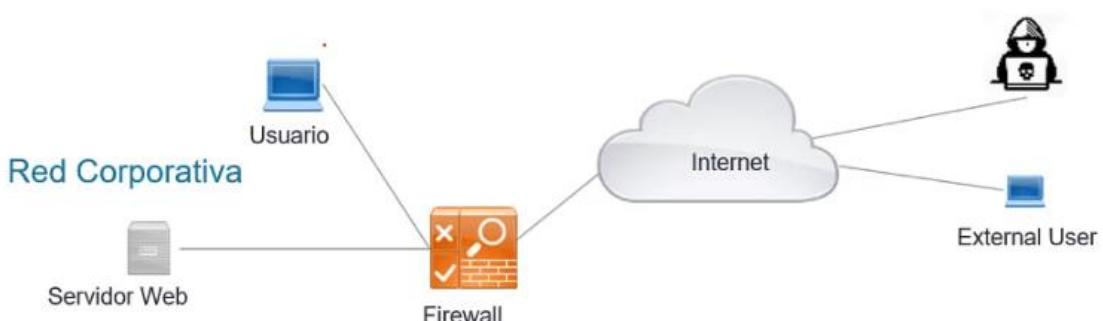
HACKER

- Conocimientos avanzados de informática que los utiliza para acceder sistemas ajenos y a manipularlos.



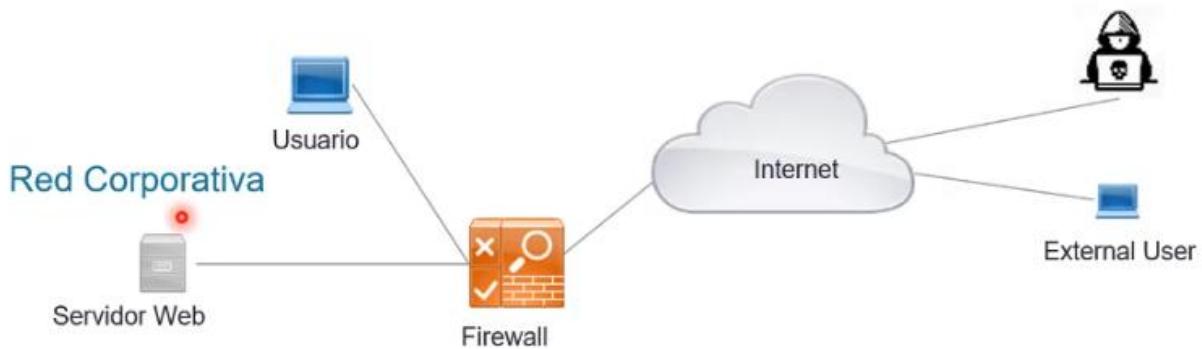
VULNERABILIDAD

- Una debilidad que se puede explotar
- Bugs en el software, sistemas con código mal programado



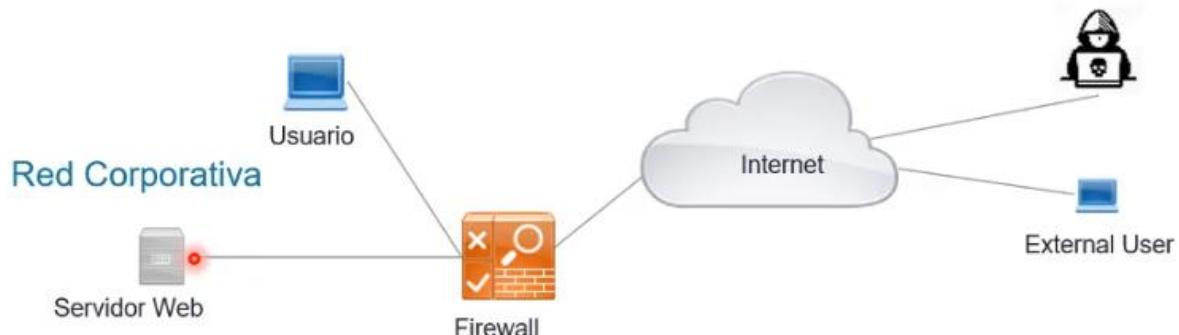
EXPLOTAR (EXPLOIT)

- Usar las vulnerabilidades para acceder los sistemas



TECNICAS DE MITIGACION

- Métodos usados para prevenir los riesgos
- Firewalls, Parches de Software, Antivirus, Antimalware



066 Elementos de un programa de seguridad

CONCIENTIZACION DEL USUARIO

- Importancia de que el usuario conozca sobre los riesgos
- Correos con información de los riesgos informáticos
- Pruebas de Phishing



CAPACITACION

- Capacitación periódica al usuario en temas de seguridad
- Webinars
- Capacitaciones en línea obligatorias



CONTROL DE ACCESO A EQUIPOS Y SERVIDORES

- Físico

- Gabinetes cerrados
- Acceso controlado a cuartos de cableado
- Acceso Controlado al DataCenter



German Hernandez P.
CCIE #24492



067 Elementos de las politicas de seguridad sobre claves

MEJORES PRACTICAS SOBRE CLAVES

Tamaño de la clave

- Mas de 6 caracteres

Uso de una combinación de letras + números + caracteres especiales

- Car2985!#

Cambio periódico de claves

- Cada 30 días mínimo

Forzar cambio periódico

ALTERNATIVAS PARA CLAVES

4ET%1ge6



1234

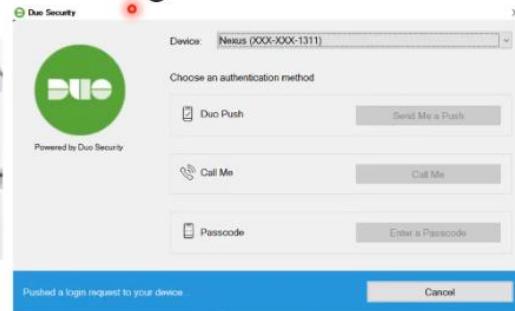


Autenticación Multifactor

- Ingreso del usuario o login + mensaje de SMS
- Ingreso del usuario o login + una App
- Ingreso del usuario o login + Token



German Hernandez P.
CCIE #24492



CERTIFICADOS

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.



BIOMETRICA

Biométrica

- Huella
- Lectura de retina



German Hernandez P.

068 ACLs Introducción a listas de acceso

ACL

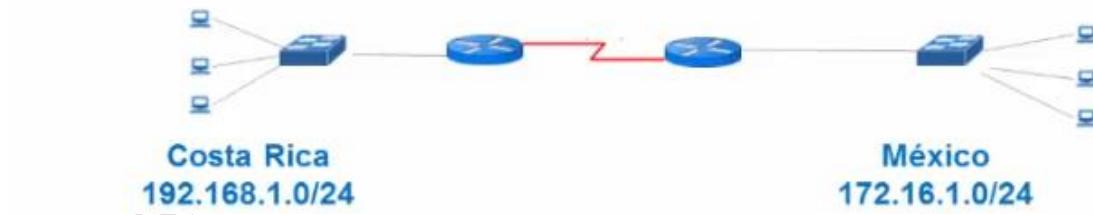
- Access Control List
- Mecanismo que permite al administrador filtrar paquetes
- Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición del encabezado de Capa 3 o Capa 4.
- El administrador puede restringir el acceso a segmentos de red, direcciones IP específicas o servicios.
- Por ejemplo la lista podría comparar la dirección IP del usuario y si tiene acceso o no a la dirección IP de un servidor.

- Se basa en “permitir” (permit) o “denegar” (deny) direcciones IP por ejemplo o puertos TCP.
- Es una lista secuencial de “permits” y “deny”
- Debe tener al menos un “permit”

```
Router#config t
Router(config)#access-list 1 permit 192.168.1.10
Router(config)#access-list 1 deny 192.168.1.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#interface Ethernet0
Router(config-if)#ip access-group 50 out
```

POR QUE USAR ACL?

- Limitar el trafico de red para controla el rendimiento de la red
- Controlar el trafico
- Provee un nivel básico de seguridad de acceso a la red
- Decidir que tipo de trafico se reenvia o bloquea en las interfaces



SINTAXIS

https://
SINTAXIS

- Paso 1:
 - Router (config)# **access-list access-list-number {permit/deny} {test condition}**
- Paso 2:
 - Router (config-if)# {protocol} access-group **access-list-number**

```

Router#config t
Router(config)#access-list 1 permit 192.168.1.10
Router(config)#access-list 1 deny 192.168.1.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#interface Ethernet0
Router(config-if)#ip access-group 50 out

```

Importante: Las listas de acceso numeradas no pueden ser modificadas. Deben ser borradas usando el comando **no access-list (numero de acl)**

PASOS PARA CREAR LA LISTA DE ACCESO



Paso 1-Crear el ACL:

- Crear el ACL usando el modo **global** de configuración
- Especificar un numero (o nombre)
- Seleccionar cuidadosamente el orden lógico de los enunciados
- Escoger los protocolos que de van a chequear

Paso 2-Aplicar a la Interface:

- Aplicar a la(s) interface el ACL creado
- Escoger la dirección Inbound(IN)

```

Router#config t
Router(config)#access-list 1 permit 192.168.1.10
Router(config)#access-list 1 deny 192.168.1.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#interface Ethernet0
Router(config-if)#ip access-group 50 out

```

CUANDO USAR ANY O HOST

Any

Es igual a usar 0.0.0.0 - 255.255.255.255

Ejemplo: access-list 2 permit any

Host

Es igual a usar IP-address 0.0.0.0

Ejemplo: 192.168.1.10 0.0.0.0

Ejemplo: access-list 2 deny host 192.168.1.10

```
Router(config)#access-list 20 deny host 192.168.1.10
```

```
Router(config)#access-list 20 deny 192.168.17.123
```

```
Router(config)#access-list 20 permit any
```

DOS TIPOS DE ACLs

- **Listas de acceso Standard**

- Solo pueden filtrar basadas en la **IP ORIGEN**

- **Listas de acceso extendidas (Extended ACLs)**

- Pueden filtrar basadas en:

- IP address ORIGEN
- IP address DESTINO
- Protocolo (TCP, UDP)
- Numero de puerto (Telnet – 23, http – 80, etc.)
- *Otros parametros*

DONDE UBICARLAS

- Todas las ACL deberían ubicarse donde más repercutan sobre la eficiencia.
 - Ubicar las ACL extendidas lo más cerca posible del origen del tráfico denegado. De esta manera, el tráfico no deseado se filtra sin atravesar la infraestructura de red.
-
- Como las ACL estándar no especifican las direcciones de destino, se colocan lo más cerca del destino posible.

NUMEROS DE ACL

Protocolo	Rango
Standard	1-99
Extendidas	100-199
Appletalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

069 ACLs Listas de acceso Standard

LISTAS DE ACCESO STANDARD

- Chequea la dirección IP Origen de los paquetes que ingresan o salen del router
- Permite o deniega el tráfico de protocolo basado en la red, subred o dirección de host
- Ubicarla cerca del destino

CONFIGURACION DE LA ACL STANDARD

Router(config)#access-list [1-99] [permit|deny] [dirección de origen] [wildcard]

1-99 Identifica numero de la lista.

Permit|deny indica si esta entrada permitirá o bloqueará el tráfico a partir de la dirección especificada.

Dirección de origen identifica la dirección IP de origen.

Wildcard identifica los bits del campo de la dirección que serán comprobados.

APLICAR LA ACL

Router(config-if)#ip access-group [1-99] [in|out]

In|out selecciona si se aplicará como filtro de entrada o de salida.

EJEMPLO



Ejemplo de una ACL estándar denegando un host:

Router#configure terminal

Router(config)#access-list 20 deny 192.168.1.3 0.0.0.0

Router(config)#access-list 20 permit any

Router(config)#interface serial 0/0/0

Router(config-if)#ip access-group 20 in

Se ha denegado al host 192.168.1.3 y luego se ha permitido a cualquier origen

EJEMPLO DE CONFIGURACION

Router (config)# access-list 2 deny 10.13.0.0 0.0.255.255

Router (config)# access-list 2 permit 10.0.0.0 0.255.255.255

Router (config)# interface fastethernet0/0

Router (config-if)# ip access-group 2 in

Si queremos borrar la lista:

Router (config)# no access-list 6

DENY IMPLICITO

Por default una interface permite el trafico en ambas direcciones.

Una vez que se aplica una ACL, el comportamiento por defecto bloquea el trafico en la dirección de la lista de acceso (IN/OUT).

Las ACL deben generalmente terminar con un sentencia para que se permita todo el trafico y así evitar que se deniegue todo el trafico.

```
Router(config)#access-list 20 deny host 192.168.1.10  
Router(config)#access-list 20 deny 192.168.17.123  
Router(config)#access-list 20 permit any
```

Las ACL deben generalmente terminar con un sentencia para que se permita todo el trafico y así evitar que se deniegue todo el trafico.

```
Router(config)#access-list 20 deny host 192.168.1.10  
Router(config)#access-list 20 deny 192.168.17.123  
Router(config)#access-list 20 permit any
```

■

```
Router(config)#access-list 20 deny host 192.168.1.10  
Router(config)#access-list 20 deny 192.168.17.123
```

070 ACLs Listas de acceso Extendidas

- Verifica la dirección IP Origen y la dirección IP Destino de los paquetes.
- Filtran paquetes IP según:
 - Direcciones IP de origen y destino
 - Puertos TCP y UDP de origen y destino
 - Tipo de protocolo (IP, ICMP, UDP, TCP o número de puerto de protocolo).

access-list [100-199] [permit|deny] [protocol] [dirección origen] [wildcard] [dirección destino] [wildcard] [puerto]

- Ubicarla cerca del origen

CONFIGURACION DE LA ACL EXTENDIDAS

access-list [100-199] [permit|deny] [protocol] [dirección origen] [wildcard] [dirección destino] [wildcard] [puerto]

100-199 identifica el rango y número de lista

Permit|deny: indica si la entrada permitirá o bloqueara la dirección especificada.

Protocolo: como por ejemplo IP, TCP, UDP, ICMP

Dirección origen y destino: identifican direcciones IP de origen y destino.

origen y mascara destino: Wildard

Puerto (opcional) puede ser por ejemplo: eq (igual a), o neq (distinto que) seguido de un número de puerto de protocolo correspondiente.

EJEMPLO DE CONFIGURACION

```
access-list 101 permit ip host 172.16.1.10 host 172.16.1.100  
access-list 101 deny ip 172.16.1.0 0.0.0.255 host 172.16.1.100  
access-list 101 permit ip any any
```

```
access-list 102 deny tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq  
80  
access-list 102 permit ip any any
```

```
Router(config)# interface F0/1  
Router0(config-if)#ip access-group 101 in
```

071 AAA Tacacs y Radius

QUE ES RADIUS Y TACACs?

Remote Authentication Dial-In User Service (RADIUS)

Terminal Access Controller Access Control System (TACACS)

Protocolos cliente/servidor que sirven para administrar los accesos a la red.

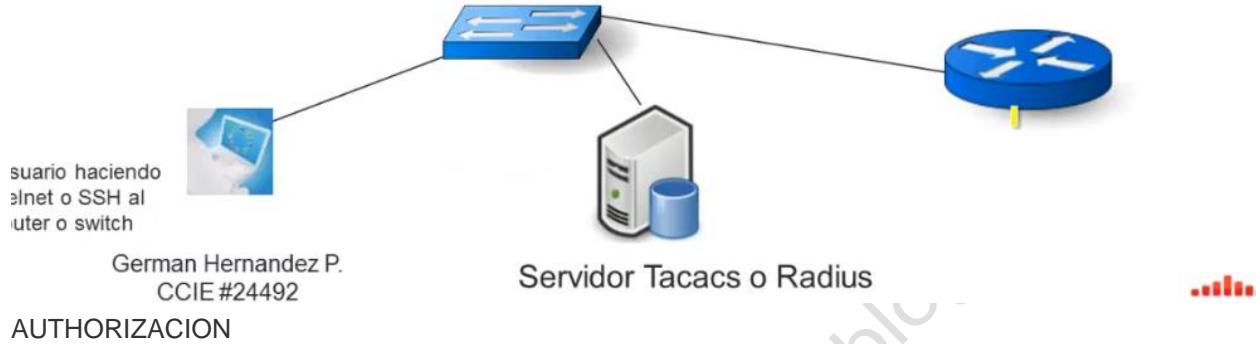
Utilizados en servidores de acceso (access servers)

Define lo que se conoce "AAA" : *Authentication, Authorization and Accounting*

AUTHENTICATION

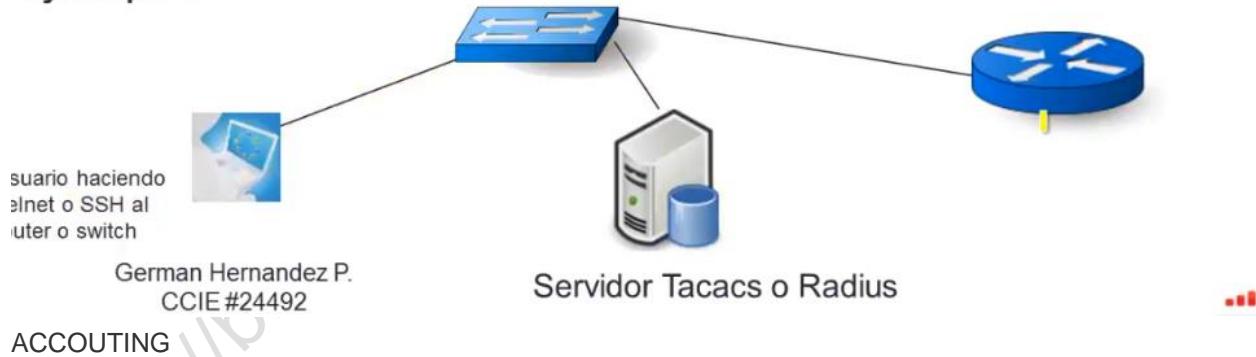
En este proceso el usuario se autentica pudiendo el sistema de alguna forma validar que el mismo puede ingresar al equipo. Por ejemplo mediante un usuario y contraseña o bien con un token.

En nuestro caso el usuario y password para ingresar a un equipo. Solo que en este caso la base de datos de estos usuarios y contraseñas, no esta en el router.



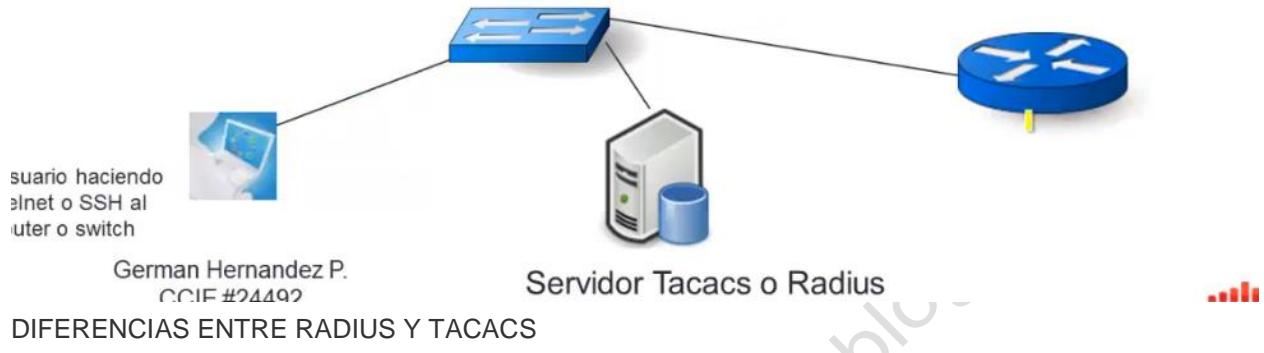
Una vez que el usuario se ha autenticado este proceso permite definir los derechos de ese usuario.

En nuestro caso podemos darle acceso a un usuario solo para que pueda ver la configuración y no modificarla por ejemplo.



Proceso que registra el acceso del usuario y detalles tales como: fecha, hora, duración u otros.

Muy útil para auditorias.



RADIUS

- UDP
- Encripta solo el password
- No es tan granular para routers
- Autenticación y Autorización combinadas

TACACS

- TCP
- Encripta todo el paquete
- Multiprotocolo
- Define qué comandos para router
- Autenticación y Autorización separadas

CONFIGURACION

https://

Primero se habilita AAA

```
aaa new-model
```

Luego se define el servidor

```
tacacs-server host 192.168.1.100
```

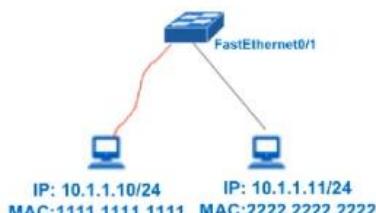
```
tacacs-server directed-request
```

```
tacacs-server key hvredes
```

072 Seguridad de Capa 2 Port Security

QUE ES PORT SECURY

Permite asegurar el uso de un puerto ya que lo puede limitar su uso a una sola direccion MAC o a una lista de direcciones MAC



CONFIGURANDO SWITCH PORT SECURITY

Comando	Descripción
Switch(config)#interface fastethernet 0/1	Ingresa a la configuracion de la interface
Switch(config-if)#switchport port-security	Activa la seguridad de puerto en la interface
Switch(config-if)#switchport port-security maximum 4	Establece el numero de direcciones MAC permitidas en este puerto
Switch(config-if)#switchport port-security mac-address 2222.2222.2222	Especifica una dirección MAC segura determinada. Se pueden añadir direcciones mac dependiendo del numero máximo configurado
Switch(config-if)#switchport port-security violation shutdown	Indica al puerto que si una dirección MAC no configurada intenta ingresar se apagara el puerto
Comando	Descripción
Switch(config-if)#switchport port-security violation restrict	Indica al puerto que si una direccion MAC no configurada intenta ingresar se descartaran los paquetes que pasen por el puerto, generando una advertencia
Switch(config-if)#switchport port-security violation protect	Indica al puerto que si una direccion MAC no configurada intenta ingresar se descartaran los paquetes que pasen por el puerto

VERIFICANDO SWITCH PORT SECURITY

Comando	Descripción
Switch#show port-security	Despliega la informacion de todas las interfaces
Switch#show port-security interface fastethernet 0/5	Despliega la informacion de seguridad en la interface
Switch#show port-security address	Despliega la informacion de seguridad de la tabla de direcciones MAC
Switch#show mac address-table	Despliega la tabla de direcciones MAC
Switch#clear mac address-table dynamic	Elimina todas las direcciones MAC dinamicas
Switch#clear mac address-table dynamic address aaaa.bbbb.cccc	Elimina una direccion MAC dinamica especifica
Switch#clear mac address-table dynamic interface fastethernet 0/5	Elimina todas las direcciones MAC dinamicas en la interface
Switch#clear mac address-table dynamic vlan 10	Elimina todas las direcciones MAC dinamicas en la VLAN
Switch#clear mac address-table notification	Limpia los contadores de notificacion global MAC

073 Control de acceso Asegurando la consola del equipo

ASEGURANDO EL ACCESO POR CONSOLA

- **Paso #1: Conectese por consola ☺**
- **Paso #2: Configure el “Line Console”**

Descripción	Comando
Ingrese al modo privilegiado y luego al submodo de “line”	<pre>router#configure terminal Enter configuration commands, one per line. End with CRTL/Z. router(config)#line con 0</pre>
Configure el password y habilite el chequeo de password en consola con login	<pre>router(config-line)#password miclave123 router(config-line)#login</pre>

- **Verificación**

Descripción	Salida del Comando
Ejecutar el comando: show running-config	<pre>router#show running-config Building configuration... ... !---- Se omiten lineas para facilidad de lectura---! line con 0 password miclave123 login line vty 0 4 ! end</pre>
	<pre>router#exit router con0 is now available Press RETURN to get started. User Access Verification Password:</pre>

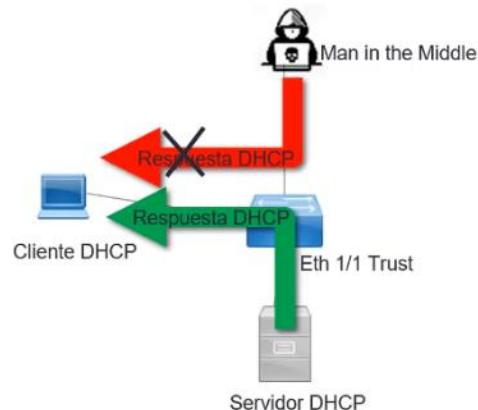
- Como usar usuarios en vez de solo password

Descripción	Comando
Ingresar al modo de configuracion y crear los usuarios	<pre>router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. router(config)#username pablo password miclave123 router(config)#username maria password miclave123</pre>
Ingresar al submodo de line y habilitar la utilizacion de usuarios mediante el comando "login local"	<pre>router(config)#line vty 0 4 router(config-line)# router(config-line)#login local</pre>

074 Seguridad de Capa2 DHCP Snooping

QUE ES DHCP SNOOPING

- Solo permite respuestas de paquetes del servidor DHCP en interfaces marcadas como “confiables”



CONFIGURACION DE DHCP SNOOPING

- Paso #1: Habilitar DHCP Snooping de forma global
- Paso #2: Habilitar DHCP Snooping en una interfaz

Descripción	Comando
Habilitar DHCP de forma global	Router(config)# ip dhcp snooping
Configurar DHCP snooping en una interfaz	<pre>Router# configure terminal Router(config)# interface FastEthernet 1/1 Router(config-if)# ip dhcp snooping trust</pre>

11 Automatizacion y Programacion orientado a Redes

075 SDN Automatizando la administracion de las redes

HERRAMIENTAS TRADICIONALES PARA ADMINISTRAR

- CLI limitado para automatizar
- SNMP principalmente para monitorear
- Netflow
- Scripts

```
Router(config-if)#
Router(config-if)#interface GigabitEthernet0/0
Router(config-if)#no cdp
% Incomplete command.
Router(config-if)#no cdp enable
```

RETOS DE HERRAMIENTAS TRADICIONALES

- Entre mas grande la red mas complejo programar algunas tareas básicas inclusive
- Conocimiento
- Fácil cometer errores
- Consumo mucho tiempo



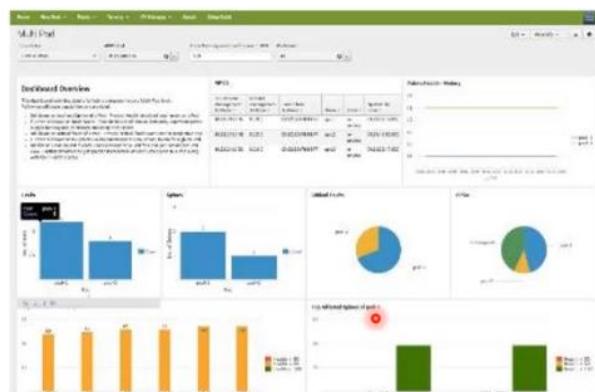
QUE SE LOGRA CON AUTOMATIZAR?

- Se eliminan tareas repetitivas
- No es necesario configurar equipo por equipo
- Upgrades masivos
- Cambios masivos
- Reducción del tiempo de troubleshooting
- Tareas que podrían tomar horas pueden tardar segundos



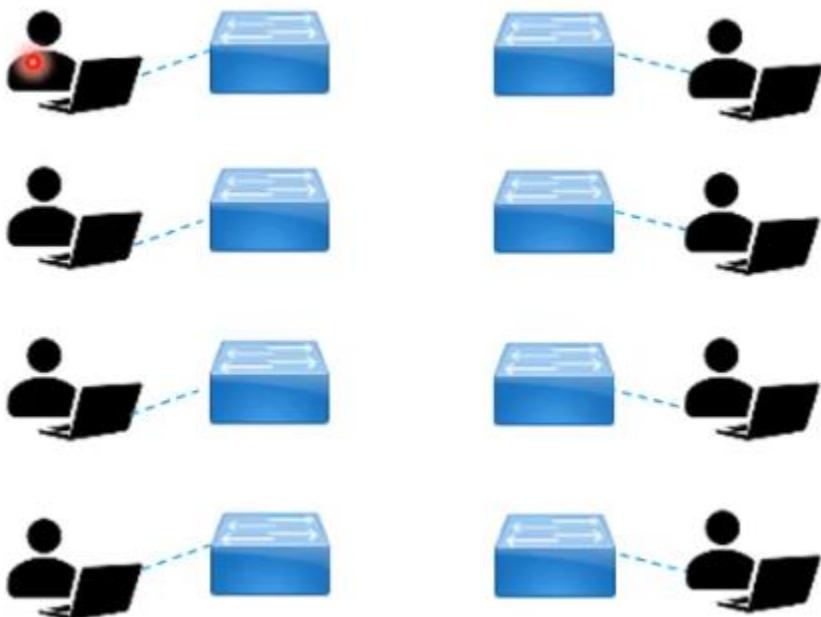
SOFTWARE DEFINED NETWORKS

- Acercamiento centralizados para aprovisionar, administrar y programar las redes.

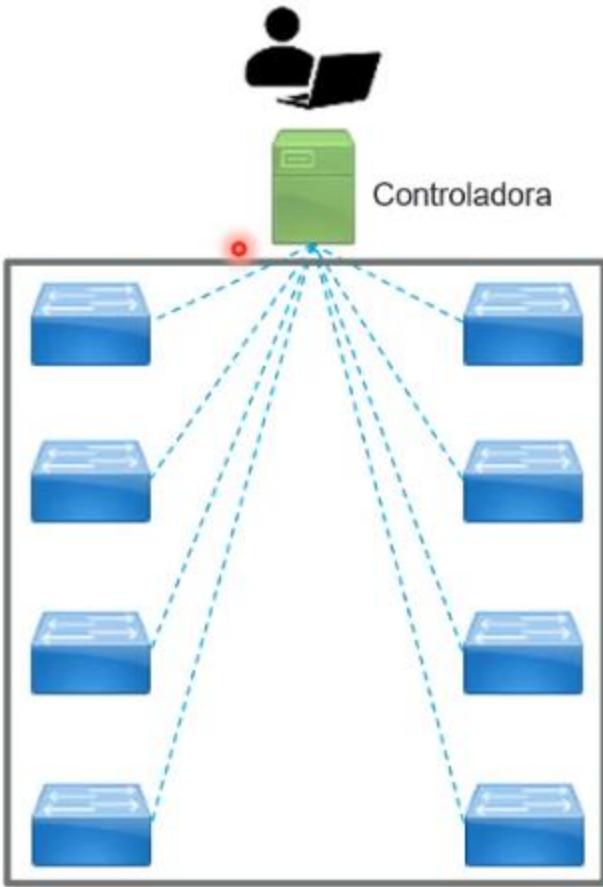


076 Redes tradicionales versus redes basadas en controladoras

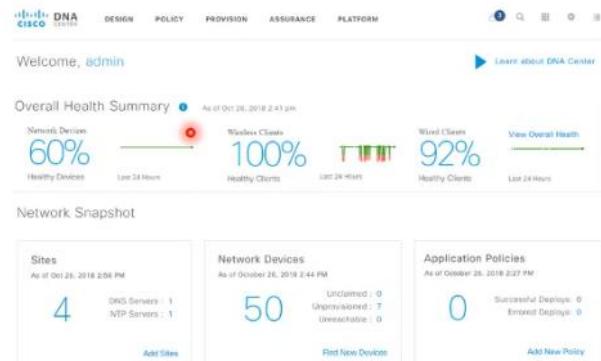
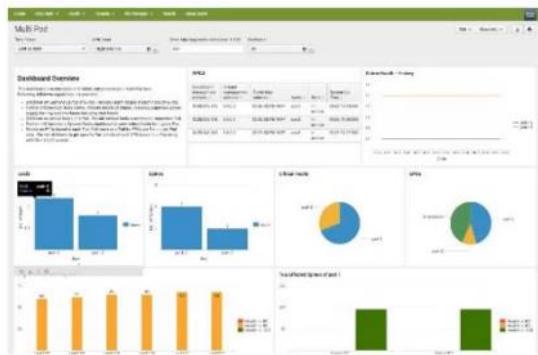
REDES TRADICIONALES



REDES BASADAS EN CONTROLADORAS



PANEL DE CONTROL



077 Conceptos de Overlay Underlay y Fabric

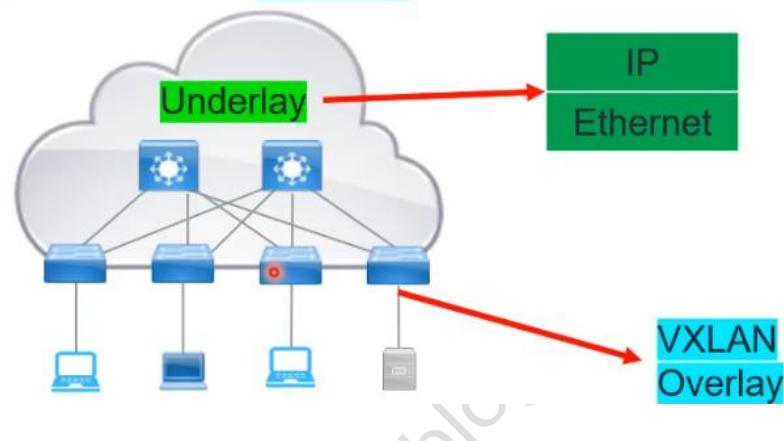
OVERLAY Y UNDERLAY

- La red **UNDERLAY** es la infraestructura **fisica-logica** sobre la cual la red Overlay esta construida.
- La red **OVERLAY** es una red **Virtual** construida sobre la red **UNDERLAY**

German Hernandez P.
https://uclm.es

UNDERLAY EN UNA LAN

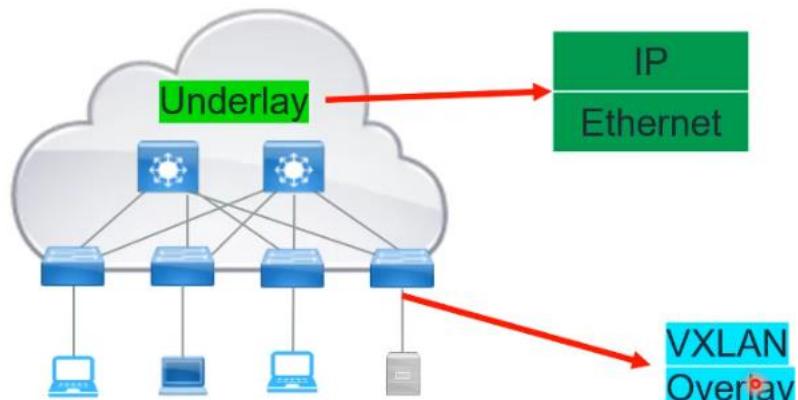
Ethernet + IP



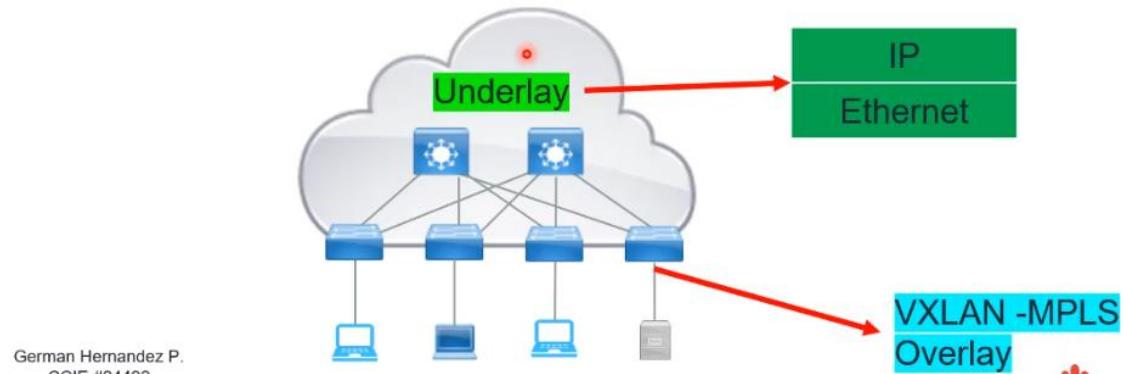
German Hernandez P.
https://uclm.es

OVERLAY EN UNA LAN

Ethernet + IP



Tunel: GRE – UDP
Multiplexador: MPLS - VXLAN



German Hernandez P.
CCIE #40440

UNDERLAY EN UNA WAN

Internet
MPLS
Punto a Punto



OVERLAY EN UNA WAN

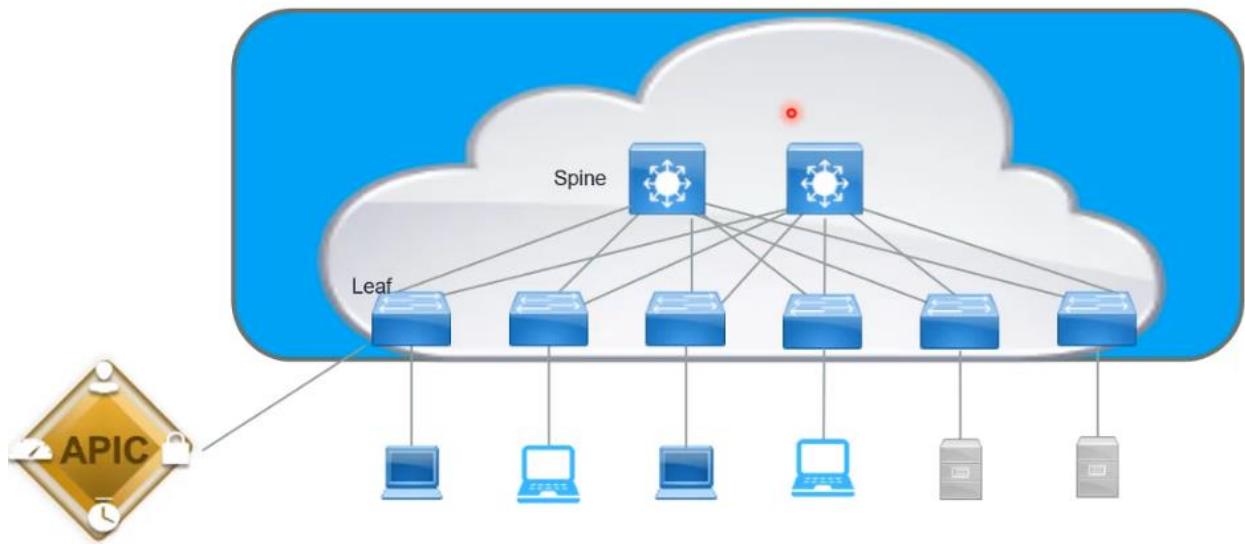
GRE
IPSEC



172.217.2.196

Google

FABRIC



GRACIAS . . .



<https://bloginformaticasystem.blogspot.com/>