# ADMINISTRACIÓN Y SEGURIDAD EN REDES

Ricardo López Bulla



# MIEMBRO DE LA RED

Administración y Seguridad en Redes Ricardo López Bulla Bogotá D.C.

Fundación Universitaria del Área Andina. 2018

Catalogación en la fuente Fundación Universitaria del Área Andina (Bogotá).

#### Administración y Seguridad en Redes

© Fundación Universitaria del Área Andina. Bogotá, septiembre de 2018 © Ricardo López Bulla

ISBN (impreso): 978-958-5462-96-0

Fundación Universitaria del Área Andina Calle 70 No. 12-55, Bogotá, Colombia Tel: +57 (1) 7424218 Ext. 1231 Correo electrónico: publicaciones@areandina.edu.co

Director editorial: Eduardo Mora Bejarano Coordinador editorial: Camilo Andrés Cuéllar Mejía Corrección de estilo y diagramación: Dirección Nacional de Operaciones Virtuales Conversión de módulos virtuales: Katherine Medina

Todos los derechos reservados. Queda prohibida la reproducción total o parcial de esta obra y su tratamiento o transmisión por cualquier medio o método sin autorización escrita de la Fundación Universitaria del Área Andina y sus autores.

#### **BANDERA INSTITUCIONAL**

Pablo Oliveros Marmolejo † Gustavo Eastman Vélez **Miembros Fundadores** 

Diego Molano Vega Presidente del Consejo Superior y Asamblea General

> José Leonardo Valencia Molano Rector Nacional Representante Legal

Martha Patricia Castellanos Saavedra Vicerrectora Nacional Académica

Jorge Andrés Rubio Peña Vicerrector Nacional de Crecimiento y Desarrollo

Tatiana Guzmán Granados Vicerrectora Nacional de Experiencia Areandina

> Edgar Orlando Cote Rojas Rector - Seccional Pereira

Gelca Patricia Gutiérrez Barranco Rectora-Sede Valledupar

María Angélica Pacheco Chica Secretaria General

Eduardo Mora Bejarano Director Nacional de Investigación

Camilo Andrés Cuéllar Mejía Subdirector Nacional de Publicaciones

# ADMINISTRACIÓN Y SEGURIDAD EN REDES

Ricardo López Bulla

# **AREANDINA** Fundación Universitaria del Área Andina

# MIEMBRO DE LA RED

## EJE 1

Introducción	7
Desarrollo Temático	8
Bibliografía	30

## EJE 2

Introducción	32
Desarrollo Temático	33
Bibliografía	50

## EJE 3

Introducción	53
Desarrollo Temático	54
Bibliografía	72

## EJE 4

Introducción	75
Desarrollo Temático	76
Bibliografía	104

NDICE NDICE

# ADMINISTRACIÓN Y SEGURIDAD EN REDES

Ricardo López Bulla

EJE 1



¿Qué elementos deben tenerse en cuenta al momento de generar una política de direccionamiento IP en la compañía?

El módulo de Administración y seguridad en redes está diseñado para que los estudiantes se acerquen al mundo de la gestión TI y comprendan los requerimientos que se exigen laboralmente a profesionales de TI.

En este primer eje se trabajará la gestión del plan de direccionamiento IPv4 e IPv6 y se dará una introducción a subnetting FLSM. El trabajo se acompaña de videocápsulas, lecturas complementarias y ejercicios de repaso, que ayudarán a consolidar los conocimientos adquiridos.

Administrador de red

## Administrador de red



Figura 1. pexels/7110

El rol del administrador de red (también llamado administrador de TI), se centra en generar procesos que optimicen la gestión de recursos, la configuración de equipos, el soporte al usuario final, el mantenimiento a las redes, la seguridad del hardware y software, además, tiene la responsabilidad de mantener la integridad, disponibilidad y confidencialidad de la información.

#### Plan de direccionamiento IP

Para empezar, lo invito a desarrollar la lectura complementaria; la cual nos dará una visión general del direccionamiento IP:

Lectura recomendada
Asignación de direcciones.
Fernando Boronat Seguí y Mario Montagud Climent.

Una de las actividades del administrador de TI es la gestión del plan de direccionamiento IP, es decir generar una adecuada asignación de direcciones IP a los equipos terminales de la compañía.

#### ¿Pero que se considera como adecuada asignación de direcciones IP?

Para resolver esta inquietud veamos que es direccionamiento IP y cómo funcionan las direcciones.

Direccionamiento IP (Internet Protocol): lo definimos como un identificador numérico que debe tener todo equipo terminal para poder conectarse a una red. Este identificador debe ser único dentro de la red o subred a la que pertenezca, ya que, si existen dos direcciones iguales en la misma red se presentará un conflicto pues no sabrá a dónde enviar la información, apareciendo el siguiente mensaje:

Error de red	X
Windows detectó un conflicto e	en la dirección IP
Otro equipo de esta red tiene la misma d el administrador de red para que le ayudo en el registro de eventos de sistema d <mark>e</mark> M	irección IP que este equipo. Póngase en contacto con e a resolver este problema. Pude obtener más detalles /indows.
	Cerrar
	Red no identificada Sin acceso a Internet

Figura 2. Error de red Fuente: propia

Este tipo de conflictos pueden llegar causar el bloqueo de los dispositivos de la red, lo cual generará una caída total de la misma.

La buena elección de un sistema de direccionamiento es clave en la gestión de la red y de esta dependerá el número de dispositivos terminales capaces de interactuar en la misma. Si pensamos en direccionamiento IPv4 debemos recordar que este tipo de direccionamiento se divide en clases y que cada clase tiene un número máximo de dispositivos terminales.

#### Tengamos en cuenta:

Clase	Inicio rango	Fin - Rango	Máscara y prefijo	Número de dispositivos terminales
A	1.1.1.1	126.255.255.255	255.0.0.0 /8	16`777.214
В	128.0.0.0	192.255.255.255	255.255.0.0/16	65.534
С	192.168.0.1	223.255.255.255	255.255.255.0 /24	254
D	224.0.0.0	239.255.255.255		
E	240.0.0.0	255.255.255.255		

Tabla 1. Clases de direccionamiento IPv4 Fuente: propia

Otro elemento importante a tener en cuenta es que las direcciones IPv4 se dividen en direcciones privadas (direcciones exclusivas para redes locales, no válidas en Internet) y direcciones públicas (direcciones asignadas por los ISP).



#### Instrucción

Antes de continuar, le invitamos a desarrollar la actividad de repaso 1. Se encuentra disponible en la página de inicio del eje 1.

Importante aclarar que a una red LAN (red de área local) no se le deben asignar direcciones públicas ya que podría causar conflicto al intentar salir a Internet.

#### Rangos de redes privadas

Para empezar, veamos una videocápsula sobre las direcciones públicas y privadas. Esta se encuentra disponible en la página de inicio del eje 1.



Autor: Cámaras de Seguridad Ecuador

Veamos a continuación, los rangos de redes privadas:

Inicio de rango	Fin de rango	Cantidad de IP
10.0.0.0	10.255.255.255	16′777.214
172.16.0.0	172.31.255.255	1′048.574
192.168.0.0	192.168.255.255	65.534

Tabla 2. Rangos de redes privadas Fuente: propia

Existe una serie de direcciones IPv4 de uso especial es decir que no se asignan a redes públicas ni privadas, pues están reservadas para usos exclusivos dentro de estas tenemos:

Dirección	Función	
0.0.0.0	Reservada por la IANA.	
100.64.0.0/10	NAT masivo - NAT a gran escala.	
127.X.X.X/8	Dirección de <i>Loopback</i> o bucle invertido (pruebas con la misma máquina).	
169.254.X.X/16	Dirección de enlace local de Windows "Apipa". (Dirección privada IP automática).	
192.0.2.X/24	Direcciones TEST-NET.	
255.255.255.255	Dirección de Broadcast.	

Tabla 3. Direcciones IPv4 de uso exclusivo Fuente: propia

Teniendo claridad en estos conceptos podemos tomar una adecuada decisión respecto al plan de direccionamiento IP que se requiere.

#### Recomendaciones en toda de decisiones de direccionamiento IPv4

La familia de direcciones 192.168.X.X/24 son apropiadas para redes en hogares, café Internet y redes de oficinas pequeñas hasta 220 dispositivos terminales.



## Importante

Aunque en este rango se tiene la posibilidad de 254 direcciones IP, no se recomienda la ocupación total de direcciones. Una buena práctica recomendada es reservar un rango de direcciones para equipos activos, gateway, servidores, equipos de red, impresoras y posible crecimiento de la red.

La familia de direcciones 172.16.0.0/16 a 172.31.255.255/16 se recomienda en empresa de mediano tamaño como universidades, campus empresariales, entre otros.

La familia de direcciones 10.X.X.X/8 es poco usada en la actualidad por la gran cantidad de direcciones IP que desperdicia.

Pero si se usa la dirección 10.X.X.X/24 en grandes compañías como la Secretaría de Educación de Bogotá.

#### Configuración del protocolo IPv4

Por último, es importante que comprendamos que el protocolo IPv4 se puede configurar de dos maneras:

#### Direccionamiento estático

Este es recomendado en redes pequeñas. Es necesario configurar cada máquina manualmente con la dirección IPv4 apropiada (panel de control- centro de redes y recursos compartidos - cambiar configuración del adaptador de red – clic secundario sobre el dispositivo a configurar – propiedades - protocolo de Internet versión 4 - propiedades), (el acceso rápido a red, tecla **Windows+R** escribir **ncpa.cpl** 

iciones de red			General	
onectar usando:			Puede hacer que la configuración IP se a	asigne automáticamente si la
Adaptador de	red Broadcom 802.11n	j	red es compatible con esta funcionalidad consultar con el administrador de red cu apropiada.	d. De lo contrario, deberà ál es la configuración IP
		Configurar	Obtener una dirección JP automátic	camente
ta conexión usa lo	os siguientes elementos:		• Usar la siguiente dirección IP:	
Cliente para	a redes Microsoft	Diver	Direction 17	192.168.1.10
VirtualBox i	nuiso bridged inetworking or de paquetes QoS	g Unver	Máscara de subred:	255 . 255 . 255 . 0
<ul> <li>Beompartir in</li> <li>Protocolo d</li> </ul>	npresoras y archivos para le Internet versión 6 (TCP)	rede: Microsoft /IPv6)	Puerta de enlace predeterminada:	192.168.1.1
Gompartir in     Arotocolo d     Arotocolo d	npresoras y archivos para le Internet versión 6 (TCP, le Internet versión 4 (TCP, <u>de E/S del asignador de</u> lor de detección de topolo	rece Microsoft (IPv6) (IPv4) Lección de topol grías de civel de v	Puerta de enlace predeterminada: O Obter de direction der servicion en O Usar las siguientes direcciones de s	192 . 158 . 1 . 1
Compartir in     Arrow Protocolo d     Arrow Protocolo d     Arrow Protocolo d     Arrow Protocolo d     Arrow Responded     Instalar	npresoras y archivos para le Internet versión 6 (TCP, le Internet versión 4 (TCP, r de E/S del asignador de dor de detección de topolo Desinstalar	rede Microsoft /IPv6) /IPv4) gras da eivel do v Propiedades	Puerta de enlace predeterminada: Obten de dirección del sel vidor o O Usar las siguientes direcciónes de s Servidor DNS prefendo.	192 . 168 . 1 . 1 Servidor DNS: 200 . 75 . 51 . 132
<ul> <li>Resimpartir in</li> <li>Protocolo d</li> <li>Protocolo d</li> <li>Protocolo d</li> <li>Responded</li> <li>Instalar</li> <li>Descripción</li> </ul>	npresoras y archivos para le Internet versión 6 (TCP, le Internet versión 4 (TCP, r de E/S del asignador de lor de detección de topolo Desinstalar	rece Microsoft (IPv6) (IPv4) decelión de topol grías da elvet de v Propiedades	Puerta de enlace predeterminada: Obtes da dirección del servidor de Obtes da dirección del servidor de Obtes direcciónes de s Servidor DNS prefendo. Servidor DNS alternativo:	192.168.1.1         192.168.1.1         192.168.1.1         192.168.1.1         200.75.51.133
Compartir in     A Protocolo d     Protocolo d     Protocolo d     Protocolo d     Seponded     Instalar  Descripción Protocolo TCP/IP predeterminado qu redes conectadas	npresoras y archivos para le Internet versión 6 (TCP) le Internet versión 4 (TCP) r de E/S del asignador de dor de detección de topolo Desinstalar P. El protocolo de red de án ue permite la comunicació s entre sí.	reac Microsoft /IPv6) /IPv4) dececión de topol gías da circl do v Propiedades rea extensa n entre varias	Puerta de enlace predeterminada: Obten de dirección derservidor o Obten de dirección derservidor o Obten de dirección derservidor o Obten de dirección de se Servidor DNS prerendo. Servidor DNS alternativo: Ualidar configuración al salir	192, 168, 1, 1         192, 168, 1, 1         192, 168, 1, 1         192, 168, 1, 1         200, 75, 51, 132         200, 75, 51, 133         Opciones avanzadas

Figura 3. Configuración protocolo IPv4 en equipo Windows Fuente: propia

#### Direccionamiento dinámico

Se trata de la asignación automática de direcciones IP, para lo cual se utiliza el protocolo DHCP el cual se configurará en prácticas posteriores. Este tipo asignación de direccionamiento se recomienda en redes de más de 20 dispositivos.



DHCP (Dynamic Host Configuration Protocol), asignación dinámica de direcciones IP.

#### Agotamiento de direcciones IPv4

El crecimiento exponencial de Internet, ha exigido una gran cantidad de direcciones IPv4 lo cual ha causado el agotamiento de las direcciones.

¡Datos!

En febrero 2011 la IANA asignó el último rango de direcciones IP disponibles y los RIR han venido anunciando su agotamiento en las regionales. Lacnic la encargada de administrar el direccionamiento para América Latina y el Caribe informó en el año 2014 el inicio de la fase de agotamiento.

Aunque desde los años 80 se veía venir este agotamiento de direcciones IP se desarrollaron e implementaron una serie de acciones que permitieron aplazarlo por muchos años, entre estas tenemos:

- Creación de subredes CIDR.
- división en direccionamiento público y privado.
- NAT.
- entre otros.



NAT
Network Address Translation,
enmascaramiento de direcciones
privadas para salir por inter-
medio de una única dirección
pública.

Sin embargo, en la actualidad con la telefonía móvil y el inicio del IoT (Internet de todo o Internet de las cosas), ni siquiera estas acciones evitan lo inevitable, el agotamiento de direcciones IPv4 y, por tal motivo se requiere una medida drástica: el cambio de protocolo.

#### Protocolo IPv6

Para comenzar, veamos una video cápsula que explica el direccionamiento IPv6 sus características y ventajas respecto a IPv4.



En el año 1994 la IETF propone el protocolo IPng (IP *Next Generation*), el cual es publicado 1996 por RFC2460. Este es presentado como la gran solución al inconveniente de agotamiento de direcciones IPv4.

Las principales características de IPv6 son:



Figura 4 Fuente: propic

- Mayor rango de direcciones 128 bit lo cual permite 340 sextillones de direcciones IP.
- Mayor seguridad (IPsec por defecto).
- Mayor capacidad de transmisión.
- Mejor calidad del servicio.
- Menos campos en el encabezado lo cual lo hace más eficiente.
- Desaparece el broadcast (los mensajes serán Unicast o Multicast).
- Se minimiza el uso de NAT (existe para pruebas, pero **no** se utiliza).

El direccionamiento IPv6 se puede asignar de tres formas diferentes:

**1. Direccionamiento estático:** en donde el administrador de red asigna manualmente la direcciona a cada *host* o dispositivo de red.

2. Direccionamiento DHCPv6: este asignará el DNS.

**3.** Configuración dinámica SLAAC: este hace más eficiente el direccionamiento y con poco uso de recurso ya que, asigna una dirección IPvó y la puerta de enlace de forma dinámica, sin necesidad de un servidor DHCPvó. Para la ID de la interfaz se utiliza el proceso EUI-64. Para complementar recomendamos revisar la lectura, que explica el mecanismo de asignación de direcciones IPvó EUI 64.



Acceso rápido a opciones de red, tecla **Windows+R** escribir **ncpa.cpl** 

unciones de red	General	
Concetor usando:	Puede hacer que la configuración IPv6 se funcionalidad. De lo contrario, deberá co configuración IPv6 apropiada.	e asigne automàticamente si la red es compatible con esta naultar con el administrador de red cuál es la
Configurar Esta conexión usa los siguientes elementos:  Ciente para redes Microsoft  Ciente para redes Microsoft  Programador de paquetes QoS  Ciente para redes Microsoft  Protocolo de Internet versión 6 (TCP/IPv6)  Protocolo de Internet versión 4 (TCP/IPv6)  A Controlador de E/S del asignador de detección de topol  Ciente para redes privada y una seguidad detección de topol  Ciente para redes detección detección de topol  Ciente para redes detección detecc	Obtener una dirección IPv6 automá     Ilsar la siguiente dirección IPv6:     Dirección IPv6:     Longitud del prefijo de subred:     Puerta de enlace predeterminada:     Obtener la dirección del servidor DM	ticamente 2001:DB8:CADA:AF::A 64 FEB0::1 IS automáticamente
Instalar Desinstalar Propiedades	Servidor DNS preferido:	2001:2DA:301::E
Descripción	Servidor DNS alternativo:	2001:2DA:301::F
ICI'/II' versión (5. Versión más reciente del protocolo de Internet que pemite la comunicación a través de varias redes interconectadas.	Validar configuración al salir	Opciones avanzadas
Aceotar Cancelar		Aceptar

Figura 5. Configuración IPv6 en equipo Windows Fuente: propia Ejemplo de dirección IPv6:



Figura 6 Fuente: propia

#### Direcciones especiales IPv6 de unidifusión:

IPv6	Función	
::/128	Dirección no especifica.	
::/0	Ruta por defecto.	
:: 1/128	Bucle invertido-LoopBack.	
FE80::/10	Dirección Enlace-Local.	
FC00::/7- FDFF::/7	Local Única ULA (antiguas priva- das).	
2000::/3- 3FFF::/3	Global Unicast (antiguas públicas).	

Tabla 4. Direcciones especiales IPv6 Fuente: propia



¡Tengamos en cuenta!

El rango 2000::/3 a 3FFF FC00::/7- FDFF::/7/3 (Global Unicast) es el rango de direcciones de unidifusión que se le asignará a todo equipo terminal, representa lo que en IPv4 serían las direcciones públicas, en IPv6 debido a la cantidad de direcciones existentes, todos los dispositivos terminales tendrán direcciones públicas, evitando el NAT.

Dentro de este rango tenemos la dirección 2001:DB8::/32 la cual se reserva para documentación o estudio.

El rango FC00::/7- FDFF::/7 Local Única ULA. Esto es lo que en IPv4 se conocía como direcciones privadas estas direcciones no son enrutables.

#### Reglas para reducir la notación de direcciones IPv6

Debido a la extensión de las direcciones IPv6 se han creado una serie de normas o reglas que permiten reducir la longitud de su notación sin modificar la dirección original, así:



#### Regla 1

Reducir los ceros que se encuentren a la izquierda de un segmento o hexteto (grupo de 16 bit), si los cuatro dígitos son ceros, colocar un único cero; ejemplo:

Dirección IPv6 Original: 2001:0DB8:000A:0DF0:0000:0000:0020:0001/64

Dirección omitiendo ceros iniciales: 2001:DB8:A:DF0:0:0:20:1/64

#### Regla 2:

Reemplazar una única vez en la dirección IPv6 los segmentos (hextetos) consecutivos de ceros por dos puntos:

Ejemplo 1:

- Dirección IPv6 original: 2001:0DB8:0000:0000:0000:00AC:0000:000F/64
- Aplicando la regla 2: 2001:0DB8::00AC:0000:000F/64
- Aplicando la regla 1: 2001:DB8::AC:0:F/64 dirección resumida

Ejemplo 2:

#### Dirección Original: 2001:0000:0000:00DA:0000:000F:0FEA/64

Para este caso especial aparecen dos grupos de ceros consecutivos, pero la regla dice que se debe aplicar el reemplazo una sola vez en la dirección IPv6, entonces podemos escoger cualquiera de los dos grupos a reemplazar y el otro grupo dejarlo igual:

- Dirección Original: 2001:0000:0000:00DA:0000:000F:0FEA/64
- Aplicando la regla 1: 2001:0:0:DA:0:0:F:FEA/64
- Aplicando la regla 2: 2001::DA:0:0:F:FEA/64 dirección resumida.
- Opción 2: 2001:0:0:DA::F:FEA/64 dirección resumida.

Es de anotar que las dos direcciones resumidas son válidas y equivalen a la misma dirección IPv6 original.

### Instrucción

Ahora, los invitamos a realizar la actividad de repaso 2, disponible en la página de inicio del eje 1.

#### Coexistencias IPv4 e IPv6

Desde el año 2016 el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia ha venido promoviendo la transición a IPv6. A comienzos del año 2017, el Mintic anunció que llegó al 100 % de la implantación y que toda su infraestructura y sus servicios están en este protocolo, fomentando así el desarrollo e implementación en el país.

Mintic

Ministerio de las tecnologías de la información y la Comunicación de Colombia http://www.mintic.gov. co/portal/604/w3-article-5956. html

ĩ

Pero las estadísticas son poco alentadoras, menos del 7 % de las empresas en Colombia han iniciado el proceso de transición ¿Cuál es la causa de esto? el semillero de investigación de redes *Kerberos* en el artículo de investigación sobre transición a IPv6 presenta las siguientes causas:



Figura 8. Freepik/1027055

• Desconocimiento del protocolo IPv6 por parte del departamento de TI, lo cual causa incertidumbre en adoptar algo desconocido.

• La infraestructura no es adecuada para la implementación IPv6, por lo tanto, se requiere inversión en el cambio de esta.

• Los ISP en Colombia todavía tienen direcciones públicas IPv4, entonces cuando una empresa les solicita direccionamiento público, asignan IPv4, desmotivando la adopción a IPv6.

• Problemas de compatibilidad IPv6 con ambientes IPv4.

Analizando dichas causas nace la necesidad imperante de prepararse en el protocolo IPv6.

#### Técnicas de coexistencia IPv4-IPv6

Para empezar, veamos la videocápsula "Transición y coexistencia IPv4 - IPv6".



Es importante aclarar que IPv4 es un protocolo totalmente diferente a IPv6 y no son compatibles. Aunque el objetivo debe ser que, las comunicaciones sean IPv6 nativas -de origen a destino-, es decir, tanto infraestructura como los servicios sean IPv6, en la actualidad no es posible ya que, la mayoría de infraestructura está en IPv4, es por ello que la IETF ha trabajado sobre diversos protocolos y herramientas que permitan la co-existencia entre IPv4 e IPv6.

Entre las principales técnicas de coexistencia o mecanismos de transición se tiene *Dual-Stack*, Tunelización, y Traducción Nat 64. Le invitamos a complementar con la lectura:



#### **Dual-Stack**

Esta técnica hace referencia a implementar pilas de protocolos IPv4 e IPv6 simultáneamente sobre toda la infraestructura, es decir en los equipos terminales colocarles dirección IPv4 y dirección IPv6 al igual que en los dispositivos intermediarios como router los cuales deben crear doble tablas de rutas y mayor trabajo para mantener dichas tablas y generar el enrutamiento. Resultado de esto es coexistencia, pero con gran consumo de recursos y tráfico de red.

#### Tunelización

Útil en el transporte de tramas IPv6 sobre redes IPv4, dado que la mayoría de infraestructura está en IPv4, los paquetes IPv6 deben encapsularse en paquetes IPv4 y transportarse como IPv4.

#### Traducción NAT 64

Esta técnica se basa en que los dispositivos habilitados en IPv6 sean capaces de comunicarse con dispositivos IPv4, traduciendo la dirección IPv6 a una dirección IPv4, tal cual cómo funciona NAT en IPv4.

#### Segmentando redes para administrar recursos

Entendamos *subnetting* o subredes como la división de una red física en varias redes lógicas que comparten los mismos dispositivos.



Subnetting para IPv4

Reflexionemos

Imaginémonos una compañía con 500 equipos terminales, distribuidos en cuatro pisos, con recursos compartidos como impresoras, bases de datos, servidores, entre otros, la gestión y administración sería complicada si la trabajáramos como una sola red. Para este tipo de situaciones se plantea crear subredes, es decir dividir la red en redes más pequeñas, para una mejor administración de usuarios, recursos y seguridad.



Para dar inicio al tema los invito a ver la videocápsula "Subnetting"

Autor: RedesUNAH

Subnetting redes en IPv4 permite optimizar las direcciones de red de tal forma que se minimice el desperdicio de las mismas en direcciones públicas. Dada la escasez de direcciones IPv4 los ISP entregan direcciones divididas.

En la red local -como ya se dijo-, se dividen para una mejor administración de usuarios, recursos y seguridad.

Para realizar el subnetting comencemos por recordar que toda dirección IP está formada por dos partes, un identificador de red y un identificador de host, también es importante aclarar que la máscara define la red.

Los invito a realizar la lectura complementaria, la cual permitirá entender el concepto de subred y la importancia de la misma:

Lectura recomendada
¿Qué es subnetting?
Juan Carlos Romero Jijón.

#### Ejemplo:

Clase	Dirección de ejemplo	ID. Red	ID. Host	Máscara y prefijo
А	10.10.10.10	10	10.10.10	255.0.0.0/8
В	172.16.10.20	172.16	10.20	255.255.0.0/16
С	192.168.1.50	192.168.1	.50	255.255.255.0/24

Tabla 5. Clases de direccionamiento IPv4 Fuente: propia

- En clase A, el primer octeto define la red y los tres octetos restantes los hosts.
- En clase B, los dos primeros octetos definen la red y los dos últimos los hosts.
- En clase C, los tres primeros octetos definen la red y el último los hosts.



#### Ejemplo 1:

Dada la red 192.168.10.0/24 dividirla en dos subredes y determinar cuántos hosts permite cada subred.

ldentificador	ID de red	ID de host	
Dirección	192.168.10	0	
Máscara	255.255.255	1 0000000	

Tabla 6. Dirección y máscara de red Fuente: propia

1. Encendemos el primer bit del segmento de *host* de la máscara y se le asigna a la subred, luego se lo restamos a la ID de *host*, es decir, tenemos ahora un bit para subredes y siete bits para *host*.

Identificador	ID de red	ID subred	ID de host
Dirección	192.168.10		0
Máscara	255.255.255	1	1 000000

Tabla 7. Dirección de red, subred y máscara Fuente: propia

2. Para calcular el # de direcciones de host disponibles en cada segmento de subred aplicamos la fórmula: #host =  $2^n$ -2; donde n es el número de bit disponibles para host. Para nuestro ejemplo tenemos 7 bit en la ID de host:

#host =  $2^{n} - 2 = 2^{7} - 2 = 128 - 2 = 126$ 

Esto quiere decir que, aunque tenemos 128 direcciones disponibles en cada segmento de red, le debemos restar dos direcciones, la primera del segmento que identificará a la subred y la última del segmento que identificará el *broadcast* de la subred, quedando 126 direcciones de *host* disponibles.

**3.** Para determinar el número de subredes disponibles aplicamos la fórmula: #Subredes=  $2^n$  donde n es el número de bit asignados a la subred. Para nuestro ejemplo hemos asignado 1 bit a la subred=>#Subredes=  $2^n = 2^1 = 2$ .

Es decir, tendremos dos subredes cada una de 128 direcciones.

#Subred	ID subred	Primera IP válida	Última IP válida	ID broadcast
SN 1	192.168.10.0/25	192.168.10.1	192.168.10.126	192.168.10.127
SN 2	192.168.10.128/25	192.168.10.129	192.168.10.254	192.168.10.255

Tabla 8. Tabla de ID de red, primera y última dirección válida Fuente: propia

Las nuevas subredes 192.168.10.0/25 y 192.168.10.128/25 significa que la máscara será 255.255.255.128.

El "/25" significa el número de bit que se le asignan a la máscara, como era una clase C, su máscara era/24 bit como hemos encendido un bit más ahora es/25.

#### Ejemplo 2:

Supongamos que ahora necesitamos cuatro subredes. Procederemos sobre la misma dirección de red. Repitiendo el procedimiento, encendemos el bit adyacente al que estaba encendido y obtendremos:

	ID de red	ID subred	ID de <i>host</i>
Dirección	192.168.10		0
Máscara	255.255.255	11	000000

Tabla 9. Dirección y máscara de red ejemplo 2 Fuente: propia

#subredes =  $2^n$  n=2 (bit asignados a la subred).

#subredes =  $2^n = 2^2 = 4$  cuatro subredes.

#host =  $2^{n}$  - 2 n = 6 (bit asignados a host).

#host =  $2^n - 2 = 2^6 - 2 = 64 - 2 = 62$  (64 direcciones válidas, 62 direcciones disponibles para host).

En conclusión, tenemos cuatro subredes, cada una de 64 direcciones para un total de 256 direcciones.

#Subred	ID subred	Primera IP válida	Última IP válida	ID broadcast
SN 1	192.168.10.0/26	192.168.10.1	192.168.10.62	192.168.10.63
SN 2	192.168.10.64/26	192.168.10.65	192.168.10.126	192.168.10.127
SN 3	192.168.10.128/26	192.168.10.129	192.168.10.190	192.168.10.191
SN 4	192.168.10.192/26	192.168.10.193	192.168.10.254	192.168.10.255

Tabla 10. Dirección de red primera, última dirección válida en rango e ID broadcast ejercicio 2 Fuente: propia

Las nuevas subredes 192.168.10.0/26, 192.168.10.64/26, 192.168.10.128/26, 192.168.10.192/26 significa que la nueva máscara será 255.255.255.192.

El "/26" significa el número de bit que se le asignan a la máscara, como era una clase C su máscara era/24 bit. Como hemos encendido dos bits ahora es/26.

Ahora bien, si seguimos dividiendo tendremos que habilitar el bit adyacente al último encendido, es decir, tendremos 3 bit para ID de subred y 5 para ID de *host*.

	ID de red	ID subred	ID de host
Dirección	192.168.10		0
Máscara	255.255.255	111	00000

Tabla 11. Dirección y máscara de red con 3 bit asignados a la subred Fuente: propia

#subredes =  $2^n$  n=3 (bit asignados a la subred).

#subredes =  $2^n = 2^3 = 8$  cuatro subredes.

#host =  $2^{n}$  - 2 n = 5 (bit asignados a host).

#host =  $2^n - 2 = 2^5 - 2 = 32 - 2 = 30$  (32 direcciones validas, 30 direcciones disponibles para host).

En conclusión, tenemos 8 subredes, cada una de 32 direcciones para un total de 256

direcciones.

#Subred	ID subred	Primera IP válida	Última IP válida	ID broadcast
SN 1	192.168.10.0/27	192.168.10.1	192.168.10.30	192.168.10.31
SN 2	192.168.10.32/27	192.168.10.33	192.168.10.62	192.168.10.63
SN 3	192.168.10.64/27	192.168.10.65	192.168.10.94	192.168.10.95
SN 4	192.168.10.96/27	192.168.10.97	192.168.10.126	192.168.10.127
SN 5	192.168.10.128/27	192.168.10.129	192.168.10.	192.168.10.159
SN 6	192.168.10.160/27	192.168.101161	192.168.10.190	192.168.10.191
SN 7	192.168.10.192/27	192.168.10.193	192.168.10.222	192.168.10.223
SN 8	192.168.10.224/27	192.168.10.225	192.168.10.254	192.168.10.255

Tabla 12. Dirección y máscara de red/27 Fuente: propia

Las nuevas subredes son:	192.168.10.96/27
192.168.10.0/27	192.168.10.128/27
192.168.10.32/27	192.168.10.160/27
192.168.10.64/27	192.168.10.192/27

92.168.10.224/27

# Importante

Podríamos continuar hasta ocupar los 8 bits de *host* pero no tendría sentido ya que no tendríamos direcciones disponibles para *host* y si no tenemos por lo menos dos *hosts* no podríamos realizar una red. Como el prefijo es "/27" Significa que la nueva máscara tendrá asignado 27 bits lo que se traducirá en una máscara 255.255.254.

Prefijo	·Máscara	•# subredes	# host
/24	255.255.255.0	0	254
/25	255.255.255.128	2	126
/26	255.255.255.192	4	62
/27	255.255.255.224	8	30
/28	255.255.255.240	16	14
/29	255.255.255.248	32	6
/30	255.255.255.252	64	2
/31	255.255.255.254	128	0
/32	255.255.255.255	256	0

Para una red clase C tendríamos:

Tabla 13. Número de *host* y subredes de acuerdo al prefijo Fuente: propia

Importante: tengamos en cuenta que los únicos posibles valores que pueden ir en una máscara de red son: 0, 128,192, 224, 240, 248, 252, 254, 255, y el prefijo máximo de red /30.

Para finalizar, les invitamos a desarrollar la actividad de repaso 3 denominada *Subnetting* FLSM.

- Bellido, Q. (2014). Equipos de interconexión y servicios de red (UF1879). Madrid, España: IC Editorial.
- Bermúdez, L. (2012). Montaje de infraestructuras de redes locales de datos: UF1121. Madrid, España: IC Editorial.
- Calvo, G. (2014). Gestión de redes telemáticas (UF1880). Madrid, España: IC Editorial.
- Feria, G. (2009). Modelo OSI. Córdoba, Argentina: El Cid Editor | apuntes.
- García, M. (2012). Mantenimiento de infraestructuras de redes locales de datos (MF0600\_2). Málaga, España: IC Editorial.
- Hillar, G. (2004). *Redes: diseño, actualización y reparación*. Buenos Aires, Argentina: Editorial Hispano Americana HASA.
- Íñigo, G., Barceló, O., y Cerdà, A. (2008). Estructura de redes de computadores. Barcelona, España: Editorial UOC.
- Martínez, Y., y Riaño, V. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid, España: Servicio de Publicaciones. Universidad de Alcalá.
- Molina, R. (2014). Implantación de los elementos de la red local. Madrid, España: RA-MA Editorial.
- Mora, J. (2014). Desarrollo del proyecto de la red telemática (UF1870). Madrid, España: IC Editorial.
- Purser, M. (1990). Redes de telecomunicación y ordenadores. Madrid, España: Ediciones Díaz de Santos.
- Roa, B. (2013). Seguridad informática. Madrid, España: McGraw-Hill España.
- Robledo, S. (2002). *Redes de computadoras*. Ciudad de México, México: Instituto Politécnico Nacional.
- Romero, J. (2009). Estudio de subnetting, VLSM, Cidr y comandos de administración y configuración de routers. Córdoba, Argentina: El Cid Editor | Apuntes.
- S.L. Innovación y Cualificación. (2012). Guía para el docente y solucionarios: montaje y mantenimiento de sistemas de telefonía e infraestructuras de redes locales de datos. Málaga, España: IC Editorial.
- Vásquez, D. (2009). Base de la teleinformática. Córdoba, Argentina: El Cid Editor | apuntes.
- Velte, T., y Velte, A. (2008). *Manual de Cis*co. Ciudad de México, México: McGraw-Hill Interamericana.

# ADMINISTRACIÓN Y SEGURIDAD EN REDES

## Ricardo López Bulla

# EJE 2

Analicemos la situación

	1000000.10101000.11001100.0	<b>.</b>	
	11000000.10101000.110011	00000	192.1.
	11000000.10101000.11001	000	192.168.20
2	11000000.10101000.110011	00	192.168.207.0
<	11111 111111111	2	255.255.255.0

host, and

L.



network

Binary

¿Qué beneficios administrativos y de seguridad genera el hecho de segmentar la red por medio de direccionamiento IP?

La toma de decisiones adecuadas respecto a la administración y seguridad de la red minimiza el riesgo y la vulnerabilidad de la misma y optimiza los procesos de gestión.

En este segundo eje trabajaremos en la técnica VLSM de *subnetting* la cual es la que se utiliza en redes de producción y es más adecuada que FLSM porque genera menor desperdicio de direcciones. Para afianzar el conocimiento nos apoyaremos en videocápsulas, lecturas complementarias, estudio de casos y talleres.

Subnetting

Para empezar, veamos la videocápsula que explica la configuración de *subnetting* en VLSM.



Subnetting VLSM, Juancar Molinero

Aplicar CIDR (*Classless Inter-Domain Routing-* enrutamiento entre dominios sin clase) permite a la red generar administración adecuada de recursos y servicio, pero una mala política de *subnetting* causará desperdicio de direcciones y, ante la escasez de direcciones IPV4 no es admisible dicha situación. De ahí la importancia de prepararnos para dar solución a este tipo de situaciones.

Para reafirmar los conceptos los invito a realizar la lectura complementaria VLSM CIDR, la cual nos dará una visión del *subnetting* por el método VLSM.



Veamos algunos ejemplos:

#### Caso 1:

La compañía XYZ tiene cuatro departamentos: tesorería, compras, ventas y TI, maneja un plan de direccionamiento en el cual todos comparten la misma red y los recursos, la dirección de red actual es 192.168.10.0/24.



ting, es lo que se entiende como Subneting.

Figura 1. Fuente: shutterstock/451342774



Se le solicita al departamento de TI que realice un plan de segmentación y optimización de recursos para cada departamento.

Si la decisión de *subnetting* depende únicamente del número de subredes que se necesitan (como es nuestro caso), la decisión es sencilla, comenzamos por elegir el número de bit necesarios para obtener cuatro subredes.

#### Dirección original

	ldentificador de red	ID host	decimal
Dirección	11000000 10101000 00001010	00000000	192.168.10.0
máscara	11111111 1111111 11111111	00000000	255.255.255.0

Tabla 1. Dirección de host y de red en formato en binario y decimal Fuente: propia

Los invitamos a ver la videocápsula que explica cómo hallar la dirección de red, la dirección de *brocadcast*, la primera y última dirección válida.



Calculo de dirección, Adrián Zambrano

#### ¡Recordemos que !

Para el subnetting se toman bit prestados de los asignados al host de la máscara de subred, es decir los que están apagados, encendiendo uno a uno de izquierda a derecha hasta encontrar el requerimiento. Para hallar el número de subredes aplico la formula **2**<sup>n</sup> donde n representa el número de bits asignados a la subred.

Si tomo 1 bit prestado para la máscara tendría 21= 2 subredes (no aplica pues nos solicitan 4 subredes).

Si tomo 2 bit prestados para la máscara tendría 22= 4 subredes (aplica).

	Identificador de red	ID subred	ID host	Representación decimal
Dirección	11000000 10101000 00001010	00000000		192.168.10.0
máscara	11111111 1111111 11111111	11	000000	255.255.255. <b>192</b>

Tabla 2. Dirección de host, de red y sub red en formato en binario y decimal Fuente: propia Esto quiere decir que ahora tengo 3 secciones en la máscara un ID de red, un ID de subred y un ID de *host*.

• El identificador de red sigue siendo el mismo pues no se ha modificado: 11111111 1111111

	Bit subred		Bit asignados a <i>host</i>					
Decimal	128	64	32	16	8	4	2	1
Potencia	2 <sup>7</sup>	2 <sup>6</sup>	2 <sup>5</sup>	24	2 <sup>3</sup>	2 <sup>2</sup>	2 <sup>1</sup>	2º
Binario	1	1	0	0	0	0	0	0

• Al identificador de subred se le han asignado dos bits.

Tabla 3. Tabla de potencias binarias y su equivalencia decimal Fuente: propia

Por consiguiente, el valor decimal de la máscara será la suma de los valores decimales que representa los bits encendidos esto quiere decir: **128 + 64 = 192.** 

 Ahora para calcular el número de direcciones disponibles en cada subred aplicamos la formula # host = 2<sup>n</sup>-2 donde n representa el número de bit asignados a host, es decir el número de bit apagados en la máscara, para el ejemplo 6 bit apagados y el -2 las direcciones ID de subred e ID de *broadcast* que no se pueden asignar.

# Host= 2<sup>n</sup>-2 = 2<sup>6</sup>- 2 = 64 -2 = 62

Para terminar el ejercicio hallaremos las cuatro subredes, el ID de la red, el primer y último valor válido para la subred y el ID del *broadcast*.

Número de subredes = 4. Número de direcciones en cada subred = 128. Número de direcciones válidas para *host* = 126. Nueva mascara = 255.255.255.192 es decir "/26" para todas las subredes.

	ID de red	Primera dirección válida	Ultima dirección válida	ID broadcast
Subred 1	192.168.10.0	192.168.10.1	192.168.10.62	192.168.10.63
Subred 2	192.168.10.64	192.168.10.65	192.168.10.126	192.168.10.127
Subred 3	192.168.10.128	192.168.10.129	192.168.10.190	192.168.10.191
Subred 4	192.168.10.192	192.168.10.192	192.168.10.254	192.168.10.255

Tabla 4. Dirección de red, primera y última dirección válida, ID *broadcast* Fuente: propia
Como respuesta al ejercicio se asigna una subred a cada departamento, y cada departamento tiene la posibilidad de conectar 62 dispositivos como máximo.

- Departamento de TI: subred 1.
- Departamento de tesorería: subred 2.
- Departamento de compras: subred 3.
- Departamento de ventas: subred 4.

#### Caso 2:

La compañía XYZ requiere desarrollar un plan de direccionamiento que optimice los recursos y la administración de la red, después de levantar el inventario se obtiene:

- Departamento de tesorería, 12 computadoras y una impresora de red.
- Departamento de compras, 28 computadoras y dos impresoras de red.
- Departamento de ventas, 98 computadoras y tres impresoras de red.
- Departamento de TI, 4 computadoras 1 impresora de red.

La dirección de red actual 192.168.10.0/24, calcular la máscara y el desperdicio de direcciones.

> En este ejercicio se requiere el plan de direccionamiento de acuerdo al número de direcciones IP por departamento.

#### Datos:

- 4 subredes.
- 142 direcciones de host + 7 direcciones de impresoras.
- La red con mayor número de host requiere 98 direcciones + 3 direcciones de impresoras un total de 101 direcciones en la red.



Fuente: shutterstock/521671348

Tomando de referencia el ejercicio anterior para cuatro redes necesitaríamos 2 bits y obtendremos:

## 2<sup>2=</sup> 4 subredes y # Host= 2<sup>n</sup>-2 = 2<sup>6</sup>- 2 = 64 -2 = 62 en cada subred

Pero no aplica porque la red con mayor requerimiento de direcciones necesita 101 direcciones IP y aquí nos ofrecen 62 (aplicando FLSM).

Ahora bien, si realizamos el análisis contrario a partir del número de bit que necesito para *host* requeriríamos 7 bits de *host*.

### # Host= 2<sup>n</sup>-2 = 2<sup>7</sup>- 2 = 128 -2 = 126 direcciones válidas en cada subred

	Subred			Bit c	asignac	los a h	ost	
Decimal	128	64	32	16	8	4	2	1
Potencia	27	26	2 <sup>5</sup>	24	2 <sup>3</sup>	2 <sup>2</sup>	2 <sup>1</sup>	2 <sup>0</sup>
Binario	1	0	0	0	0	0	0	0

2<sup>1</sup>= 2 subredes (no aplica por que tendríamos solo dos subredes).

Tabla 5. Tabla de potencias para el ejercicio planteado Fuente: propia

De acuerdo con esto este ejercicio no tendría solución según los requerimientos planteados.

Surge entonces VLSM (*Variable Length Subnet Mask*) máscara de subred de longitud variable, con la cual se le asigna la máscara de red de acuerdo a la necesidad de cada subred.

# Pasos para desarrollar VLSM

- 1. Ordenar las redes de mayor a menor de acuerdo al requerimiento de direcciones IP por cada departamento:
  - a. Departamentos ventas: 101 direcciones.
  - b. Departamentos compras: 30 direcciones.
  - c. Departamento tesorería: 13 direcciones.
  - d. Departamento de TI: 5 direcciones.





- 2. Crear la tabla para subnetting VLSM.
- 3. Escribir el segmento de la dirección IP que identifica la red en decimal.
- 4. Escribir el segmento de *host* de la dirección IP en binario.
- 5. Colocar el valor decimal correspondiente a cada bit del segmento de *host*.
- 6. Trazar una línea divisoria a la derecha del valor más cercano que cubra el requerimiento de direcciones IP solicitadas.
- Encender el bit menos significativo que quedó a la izquierda de la línea divisoria. La suma de los valores decimales encendidos en el segmento de host serán el identificador de la siguiente subred.
- 8. El prefijo será el número de bit del identificador de red MAS el # bit a la izquierda de la línea que trazamos.
- 9. El broadcast de la subred será el resultado de la nueva subred-1.

10. Repetir desde el paso	6 hasta determinar las subredes necesarias.	

ID Subred	Segmento de red	Segmento de <i>host</i>	prefijo	Broadcast subred
		128 64 32 16 8 4 2 1		
192.168.10.0	192.168.10	120 04 32 10 0 4 2 1		192.168.10.127
		00000000	/25	
192.168.10.128		10000000	/27	192.168.10.159
192.168.10.160		10100000	/28	192.168.10.175
192.168.10.176		10110000	/29	192.168.10.183
192.168.10.184		10110000		

Tabla 6. Tabla de cálculo sub redes por VLSM Fuente: propia

Después de elaborar la tabla comencemos a llenarla.

Tomamos el mayor requerimiento de direcciones IP para este caso es 101 direcciones, ubicamos el valor más cercano que cubra esa cantidad, para el ejemplo es 128, es decir el primer bit, trazamos una línea separando este bit, con esto obtenemos el prefijo que será igual a 24 bits del ID de red + 1 bit del ID de subred => 24 + 1 = 25 será nuestro primer prefijo.



A continuación, hallamos el ID de la segunda subred, encendiendo el bit menos significativo a la izquierda de la línea trazada, como solo tenemos un bit a la izquierda encendemos ese bit, el cual convertido a decimal representa el valor 128. Con esto obtenemos el segundo ID de subred 192.168.10.**128.** 

Ahora debemos determinar el *broadcast* de la primera subred para esto restamos 1 (uno) al valor del ID de red de la segunda subred 128 - 1 = 127 y obtenemos el *broadcast* de la primera subred **192.168.10.127.** 

Repitiendo el procedimiento desde el paso 6 tenemos:

El segundo mayor valor de requerimiento de direcciones es 30, entonces ubicamos el valor más cercano que cubra esa cantidad, para el ejemplo es 32 es decir el tercer bit, trazamos una línea separando este bit, con esto obtenemos el prefijo que será igual a 24 bits del ID de red + 3 bits del ID de subred => 24 + 3 = 27 será nuestro segundo prefijo.

A continuación, hallamos el ID de la tercera subred, encendiendo el bit menos significativo a la izquierda de la línea trazada, sin modificar los demás, este bit menos significativo será el tercero, el cual convertido a decimal representa el valor 32. Procedemos a sumar los bits encendidos a la izquierda de la línea 128 + 32 = 160 y obtenemos el ID de la 3 subred 192.168.10.**160.** y a la vez podemos obtener el ID de *broadcast* de la segunda red restando 1 es decir **192.168.10.159** 

Repitiendo el procedimiento desde el paso 6 tenemos:

El tercer mayor valor de requerimiento de direcciones es 13, entonces ubicamos el valor más cercano que cubra esa cantidad, para el ejemplo es 16, es decir el cuarto bit, trazamos una línea separando este bit, con esto obtenemos el prefijo que será igual a 24 bits del ID de red + 4 bit del ID de subred => 24 + 4 = 28 será nuestro tercer prefijo.

A continuación, hallamos el ID de la cuarta subred, encendiendo el bit menos significativo a la izquierda de la línea trazada, sin modificar los demás, este bit menos significativo será el cuarto, el cual convertido a decimal representa el valor 16, procedemos a sumar los bits encendidos a la izquierda de la línea 128 + 32 + 16 = 160 y obtenemos el ID de la 4 subred 192.168.10.**176** y a la vez podemos obtener el ID de *broadcast* de la tercera red restando 1 es decir **192.168.10.175** 



Repitiendo el procedimiento desde el paso 6 tenemos:

Para finalizar tomamos el último valor de requerimiento de direcciones, es decir 5, y ubicamos el valor más cercano que cubra esa cantidad, para el ejemplo es 8, es decir el cuarto bit, trazamos una línea separando este bit, con esto obtenemos el prefijo que será igual a 24 bits del ID de red + 5 bit del ID de subred => 24 + 5 = 29 será nuestro tercer prefijo.

A continuación, hallamos el ID de la quinta subred, encendiendo el bit menos significativo a la izquierda de la línea trazada, sin modificar los demás, este bit menos significativo será el quinto, el cual convertido a decimal representa el valor 8, procedemos a sumar los bits encendidos a la izquierda de la línea 128 + 32 + 16 + 8 = 184 y obtenemos el ID de la 4 subred 192.168.10.**184** y a la vez podemos obtener el ID de *broadcast* de la tercera red restando 1 es decir **192.168.10.183** 

> Figura 4. Fuente: shutterstock/538301581



#### ¡Importante!

Debemos siempre hallar el ID de subred de la próxima red para determinar el ID de broadcast de la subred actual.

# Cálculo de desperdicio de direcciones

Para empezar, veamos una videocápsula en donde se realiza la resolución de ejercicio de direccionamiento con máscara variable.



Para calcular el desperdicio de direcciones restamos de la cantidad de direcciones asignadas a la subred de la cantidad de direcciones requeridas.

Desperdicio total de IP = 28 direcciones

Para profundizar en el tema los invito a realizar la lectura complementaria:



Estudio de de subnetting, VLSM, Cidr y comandos de administración y configuración de routers.

Juan Carlos Romero Jijón

Practiquemos.

Les invitamos a realizar la actividad de repaso 1 sobre *Subnetting* VLSM. Ésta se encuentra disponible en la página de inicio del eje 1.

Administración y seguridad en switch

# Administración y seguridad en switch

Para empezar, veamos una videocápsula en donde se explican los comandos básicos de configuración de un switch Cisco.

# Video

Configuración Básica de un switch, Kenan Li.



Figura 5. Switch no administrables Fuente: propia

El switch es un dispositivo de red capa 2 (aunque existen multicapa o capa 3) encargado de conmutar la información que por él pasa; los hay de diversos tipos, marcas y precios desde \$ 30 000 pesos hasta aparatos con valores superiores a los \$ 40 000 000. Debido a sus características y funcionalidades, no existe una clasificación oficial de este dispositivo, pero lo cierto es que cualquier red necesita uno, pues es el conmutador central de la red local es decir el que permite interconectar dispositivos en una red local.

**Switch no administrables:** denominados de escritorio, son aquellos que ofrecen la función básica de conmutación utilizado en hogares y oficinas pequeñas, vienen configurados de fábrica de 4, 8, 16 y 24 puertos, cumplen con el estándar IEE802.3.

Antes de continuar, les invitamos a consultar la lectura, en donde se explica que es la IEEE y cuál es su misión:



**Switch administrables:** este tipo ofrece características configurables como la velocidad del puerto, el ancho de banda, seguridad de acceso por medio de MAC, entre otras características. Permite generar VLAN, puertos troncales, etherchannel, además es capaz de separar servicios de VoIP de datos y ofrecen QoS (calidad de servicio), escalabilidad, seguridad, alto rendimiento, utilizados normalmente en oficinas medianas y grandes.



Figura 6. Switch administrables Fuente: propia

# ilmportante!

Existen otros tipos de switch apilables, troncales, modulares, pero no son parte del tema de este curso por lo tanto no los trabajaremos. Para complementar, les invitamos a realizar la lectura, la cual explica los conceptos básicos de los switch y su configuración:



# Lectura recomendada

Manual de Cisco, leer de la parte 2 el numeral 5: Conmutador.

Tony Velte y Anthony Velte.

# Configuración básica de un switch Cisco



Los switch configurables de Cisco tienen un sistema operativo denominado IOS de Cisco, un puerto de consola que permite mediante cable de consola conectarse a un PC por interfaz serial RS232, el cual puede acceder al IOS del switch mediante un programa terminal que se debe instalar.

Figura 7. Fuente: shutterstock/20898286 Le invitamos a realizar la lectura, que explica los comandos básicos para configurar los parámetros de un switch:

1



# Lectura recomendada

Configuración básica del switch.

Curso de CCNA.

ົ້າ

ilmportante!

Los equipos modernos ya **no** traen instalado el puerto serial RS232 por lo cual se hace necesario adquirir un convertidor de serial a USB para poder conectarse por cable de consola.



Cable de consola

Visitar página

Entre los principales programas terminales tenemos <u>Putty, Hyper-</u>

terminal (propietario de Microsoft), TeraTeam (propietario de Cisco).

> Figura 8. Cable de consola Fuente: propia

#### IOS

Hace referencia al sistema operativo del dispositivo de Cisco.

Una vez conectados por cable de consola al switch accedemos por medio de un terminal de consola (Putty) configurando los parámetros básico de conexión tipo de conexión, puerto y velocidad, al aceptar esta configuración accedemos al IOS del dispositivo.

Category:			100 ASSEMDLY Part NUMber	: 800-266/1-02	(d)
E- Session	Basic options for you	r PuTTY session	Top Assembly Revision Number	: B0	
Jession     Logging     Terminal     Keyboard     Bell     Features     Window     Appearance     Behaviour     Translation     Selection	Specify the destination you was Serial line COM4 Connection type Baw Teinet O Riog Load, save or delete a stored s Saved Sessions	int to connect to Speed 9600 gin SSH Serial	Version ID CLEI Code Number Hardware Board Revision Number Switch Forts Model Image 	: V02 : COM3K00BRA er : Ox01 SW Version 	SW C2960-
Colours Connection 	Close window on exit:	Load Save Delete	Cisco IOS Software, C2960 So 12.2(25)FX, RELEASE SOFTWARE Copyright (c) 1986-2005 by C Compiled Wed 12-Oct-05 22:05 Press RETURN to get started!	ftware (C2960-LANBASE-M (fcl) isco Systems, Inc. by pt_team	), Version
About		pen Cancel	Consola del Switch	Cisco 2960	j.

Figura 9. Acceso por cable serial a dispositivo Fuente: propia El IOS de Cisco divide el acceso de administración en diversos modos y muestra por medio de símbolos la ubicación y las propiedades de ese modo. En la siguiente tabla observamos Algunos de los modos de acceso, su símbolo y características principales.

Símbolo de modo	Modo	Características
Switch>	Modo usuario. > (mayor que)	<ul> <li>Es el modo inicial del switch.</li> <li>Permite acceso a comandos básicos de monitoreo.</li> <li>Acciones restringidas.</li> </ul>
Switch#	Modo privilegiado o modo EXEC. # (numeral)	<ul> <li>Permite acceso a todos los comandos.</li> <li>Se usa para administración y control.</li> <li>Permite el ingreso a otros modos de configuración específica.</li> <li>Desde este modo se puede formatear, reiniciar, eliminar la configuración del dispositivo.</li> </ul>
Switch (config)#	Modo de configura- ción global. <b>(config)#</b>	<ul> <li>Permite generar las configu- raciones básicas del SW como nombre, mensaje de inicio, se- guridad de acceso, sincronizar reloj, entre otras.</li> <li>Permite acceder a configura- ciones específicas.</li> </ul>
Switch (config- if)#	Modo de configura- ción de interfaz. (config- if)#	<ul> <li>Permite acceder a la configu- ración del puerto, estado de puerto, seguridad del puerto, velocidad del puerto, entre otros.</li> </ul>
Switch (config- line)#	Modo de configuración de línea de comandos. (config-line)#	<ul> <li>Permite el acceso a configura- ción de línea de consola LINE CON 0.</li> <li>Permite el acceso a configura- ción de línea de acceso remoto LINE VTY 0 4.</li> </ul>

Tabla 7. Modos de operación de switch Cisco Fuente: propia



Figura 10. Conexión a equipo por cable de consola Fuente: propia

Abrimos el PC, pestaña Desktop y seleccionamos terminal, luego aceptamos los parámetros de conexión, modo, velocidad y puerto.

s Per Second; :a Bits:	9600
ta Bits:	8
	<u></u>
ity:	None
p Bits:	1
w Control:	None
30	yp Bits: w Control:

Figura 11. Acceso a dispositivo por terminal Fuente: propia Una vez dentro de Switch procedemos a realizar la configuración inicial del mismo, el modo inicial del Switch es: modo usuario.

**Switch> enable** (este comando lo habilita y lo lleva a modo privilegiado).

**Switch#configure terminal** (este comando nos lleva al modo configuración).

**Switch (config)# hostname** SW1 (cambia el nombre a SW1).

**SW1 (config # enable password** PALA-BRA (crea una contraseña "PALABRA" al modo privilegiado de acceso, se considera la contraseña más importante, esta contraseña no está encriptada).

**SW1 (config)# enable secret** PALABRA (crea una contraseña encriptada "PALA-BRA" al modo privilegiado de acceso, se considera la contraseña más importante, reemplazó a enable password por los niveles de seguridad).

**SW1 (config)# banner mot #** Propiedad de Area Andina **#** (crea un mensaje de advertencia o saludo al acceder al dispositivo, el mensaje debe ir entre símbolos especiales **#mensaje#** y no admite tildes).

**SW1 (config)#line con 0** (accede a configurar la línea de consola, el 0 representa el único puerto de consola que tiene el dispositivo).

**SW1 (config-line)#password** PALABRA (se agrega una clave "PALABRA" para acceder por medio de cable de consola al dispositivo).

**SW1 (config-line)# login** (login habilita la seguridad del acceso por consola).

**SW1 (config-line)# Exit** (regresa al modo anterior del dispositivo).

**SW1 (config)# line vty 0 15** (VTY línea de terminal virtual, habilita el acceso remoto vía Telnet o SSH, al igual que la **line con 0** requiere **password** y **login** para habilitar el acceso).

**SW1 (config-line)#password** PALABRA (se agrega una clave "PALABRA" para acceder por medio de cable de consola al dispositivo).

SW1 (config-line)# login (login habilita la seguridad del acceso por consola).

Protocolo de acceso remoto no seguro.

Telnet

SSH Protocolo de acceso remoto seguro.

SW1 (config-line)# end (lo lleva al modo privile-

giado).

**SW1# write** (guarda la configuración de dispositivo).

**SW1#** copy startup-config running-config (guarda la configuración de dispositivo cumple la misma función que **write**).



Para finalizar, desarrollemos el caso simulado sobre configuración subnetting - parámetros iniciales de switch. Este se encuentra disponible en la página de inicio del eje 2.

- Bellido, Q. (2014). Equipos de interconexión y servicios de red (UF1879). Madrid, España: IC Editorial.
- Bermúdez, L. (2012). Montaje de infraestructuras de redes locales de datos: UF1121. Madrid, España: IC Editorial.
- Calvo, G. (2014). Gestión de redes telemáticas (UF1880). Madrid, España: IC Editorial.
- Feria, G. (2009). *Modelo OSI*. Córdoba, Argentina: El Cid Editor | apuntes.
- García, M. (2012). Mantenimiento de infraestructuras de redes locales de datos (MF0600\_2). Málaga, España: IC Editorial.
- Hillar, G. (2004). *Redes: diseño, actualización y reparación*. Buenos Aires, Argentina: Editorial Hispano Americana HASA.
- Íñigo, G., Barceló, O., y Cerdà, A. (2008). *Estructura de redes de computadores*. Barcelona, España: Editorial UOC.
- Martínez, Y., y Riaño, V. (2015). *IPv6-Lab:* entorno de laboratorio para la adquisición de competencias relacionadas con *IPv6*. Madrid, España: Servicio de Publicaciones. Universidad de Alcalá.
- Molina, R. (2014). Implantación de los elementos de la red local. Madrid, España: RA-MA Editorial.
- Mora, J. (2014). Desarrollo del proyecto de la red telemática (UF1870). Madrid, España: IC Editorial.
- Purser, M. (1990). *Redes de telecomunicación y ordenadores*. Madrid, España: Ediciones Díaz de Santos.
- Roa, B. (2013). Seguridad informática. Madrid, España: McGraw-Hill España.

- Robledo, S. (2002). Redes de computadoras. Ciudad de Méxic, México: Instituto Politécnico Nacional.
- Romero, J. (2009). Estudio de subnetting, VLSM, Cidr y comandos de administración y configuración de routers. Córdoba, Argentina: El Cid Editor | Apuntes.
- S.L. Innovación y Cualificación. (2012). Guía para el docente y solucionarios: montaje y mantenimiento de sistemas de telefonía e infraestructuras de redes locales de datos. Málaga, España: IC Editorial.
- Vásquez, D. (2009). Base de la teleinformática. Córdoba, Argentina: El Cid Editor | apuntes.
- Velte, T., y Velte, A. (2008). *Manual de Cis*co. Ciudad de México, México: McGraw-Hill Interamericana.

# ADMINISTRACIÓN Y SEGURIDAD EN REDES

240

Ricardo López Bulla

# EJE 3 ongamos en práctica

 AREANDINA
 MIEMBRO DE LA RED

 Fundación Universitaria del Área Andina
 ILUMNÓ

¿Al implementar VLAN en la red qué beneficios administrativos y de seguridad se generan?

La experticia en el desarrollo de planes de direccionamiento, subnetting y VLAN se obtiene con la práctica y la mejor forma de desarrollar prácticas sin causar traumatismo en la empresa, es con el uso de simuladores, los cuales permiten analizar posibles fallos, errores en segmentación o diseño del plan de direccionamiento.

En este eje se trabajará el reconocimiento y configuración de VLAN y la forma adecuada de administrar y asegurar este recurso, nos apoyaremos en videocápsulas, lecturas complementarias, casos simulados, talleres los cuales ayudarán a fortalecerán los conocimientos y habilidades adquiridos.

# VLAN



Figura 1. VLAN Fuente: Shutterstock/564493375

# Lectura <u>recomendada</u>

Redes de área local virtual VLAN.

Jordi Íñigo Griera, José María Barceló Ordinas, Llorenç Cerdà Alabern, Enric Peig Olivé, Jaume Abella Fuentes y Guiomar Corral Torruela.

Las VLAN (Virtual LAN) o redes virtuales LAN, es una tecnología que ofrecen algunos dispositivos capa 2 (switch), la cual permiten subdividir de forma lógica la red, creando grupos o segmentos de acuerdo a la función, los servicios que requiera, los recursos que necesiten, las aplicaciones que usen, la ubicación física o la necesidad del administrador. A las VLAN creadas se les debe asignar puertos del switch, de lo contrario no tendrá ningún efecto sobre las mismas, los dispositivos conectados a los puertos de una determinada VLAN serán visibles únicamente a esa.

En una infraestructura con varias VLAN, cada una actuará como una red independiente, así compartan un mismo dispositivo físico.

La gran ventaja de configurar VLAN en una red, es que disminuye el tráfico en la misma (reducción de <u>dominio de</u> <u>broadcast</u>) ya que los mensajes

de multidifusión (*multicast*), de difusión (*broadcast*) y unidifusión (*unicast*) <u>inun-</u> <u>daran o saturaran</u> solo los puertos pertenecientes a la misma VLAN, esto contribuirá al mayor rendimiento de la red.

Dominio de broadcast: Hace referencia al segmento

Hace referencia al segmento de la red al que le llegará la información de difusión.

#### <u>Inundaran o saturaran:</u>

Término utilizado para indicar que el mensaje se ha enviado a todos los miembros de la red que pertenecen al mismo dominio de broadcast, excepto a quien genera o emite el mensaje.

# ຶ່ງ

# ¡Importante!

La VLAN es ideal para separar el tráfico de la red de acuerdo a características y necesidades específicas, ejemplo de esto y buena práctica recomendada es la separación del tráfico de voz IP y el tráfico de datos, dado que la voz requiere mayor calidad de servicio y si esta se mezcla con los datos se distorsionará o será afectada por ruido disminuyendo la calidad.

Las VLAN también ofrecen mayor rapidez en él envió de datos, mayor calidad de servicio (QoS), seguridad de la información, menor tráfico en la red, segmentación y optimización de recursos.

¿Entonces, cuál es la diferencia con subnetting?

Los dispositivos pertenecientes a las subredes generadas por medio de direccionamiento IP (*subnetting*) estarán en el mismo dominio de difusión o *broadcast* y el mensaje de difusión llegará a todos los dispositivos, así no estén en la misma subred, consumiendo recursos innecesarios de red.

Otra gran diferencia es que *subnetting* no permite dividir el tráfico y utilizan un diseño plano de red, es decir todo tipo de tráfico por la red.

Sin embargo, en implementaciones empresariales se utiliza las VLAN acompañadas del CIDR lo cual creará un plan óptimo de direccionamiento, seguridad y rendimiento.



# Datos!

Sabías que, al diseñar VLAN se debe tener en cuenta un esquema de direccionamiento IP (donde cada una debe tener su propio rango de direcciones).



Desarrollo de guías para el diseño e implementación de redes locales virtuales.

Mauricio Javier Tufiño Coloma.

En la siguiente figura se muestran dos edificios con 3 departamentos, cada uno con su respectiva VLAN y con un adecuado plan de direccionamiento con CIDR (*subnetting*).



Figura 2. Topología de VLAN Fuente: propia

## **Tipos de VLAN**

Existen diversos tipos de VLAN, cada una con características y funciones diferentes, entre las que se destacan:

VLAN de datos: como su nombre lo indica se diseña para transportar datos de usuario exclusivamente, los puertos asignados a esta VLAN se deben configurar en "mode Access" o modo acceso.

VLAN de voz: esta se diseña con el fin de transportar voz sobre la red de datos, tecnología denominada VoIP, para esto se requiere que garantice ancho de banda, disponibilidad, calidad del servicio, y además debe priorizar este servicio sobre los demás, en dispositivos Cisco, el comando "switchport Voice VLAN" convertirá el puerto con prioridad para voz.



Configuración VLAN de voz. Estqf Sirc.

https://youtu.be/44u47cz\_e8E

**VLAN predeterminada:** en un *switch Cisco* es la VLAN1, denominada también VLAN por defecto, esta no se puede eliminar ni renombrar, por lo demás puede cumplir las funciones de cualquier VLAN.

Un *switch* Cisco sin configuración, al arrancar asignará por defecto todos los puertos a esta VLAN 1. **VLAN administrativa:** esta se utiliza para administrar de manera remota el dispositivo (*switch*), para lo cual se necesita

la asignación de una dirección IP a una interfaz, pero como este dispositivo no cuenta con interfaces se debe crear la <u>SVI</u> (interfaz virtual del *switch*) a la cual se le asignará la dirección IP. Es importante aclarar



Interfaz virtual de switch, la cual permite acceder a la configuración de forma remota.

que la SVI solo sirve para acceso remoto vía Telnet o SSH a las configuraciones de administración del *switch*.

La VLAN administrativa configurada por defecto en los *switch* Cisco es la VLAN 1, por tal razón se recomienda como buena práctica administrativa cambiar a otra VLAN la función de la administrativa ya que es vulnerable de ser atacada.

**VLAN nativa:** es la que va permitir el tráfico que generan diversas VLAN, además permite tráfico sin etiquetar, es decir tráfico que proviene de dispositivos que no están asociados a ninguna VLAN, por tal razón los puertos asociados a la VLAN nativa deben estar en modo *Trunk* o troncal IEEE 802.1Q.

Por defecto la VLAN nativa al igual que la administrativa viene asociada a la VLAN 1, lo cual genera altos grados de inseguridad, por consiguiente, se recomienda configurar una VLAN nativa diferente a la VLAN 1.

Video

Configuración VLAN Trunk. Sistema summa.

https://youtu.be/71lol-RsNBA

**VLAN de parqueo:** a esta VLAN se le asignan los puertos que **no** se van a utilizar, es una VLAN de seguridad, se recomienda apagar todo puerto que no se utilice.



Manual de Cisco, leer de la parte 2 el numeral 5: Conmutador el tema VLAN. Tony Velte y Anthony Velte.

# RI OCK BLOCK 0

# Rango de VLAN en switch Cisco

En los *switch* Cisco se permiten configurar diversas VLAN, admite hasta 4096 VLAN, estas están divididas en dos segmentos normales que van de la 1 a la 1005 y las LAN extendidas van de la 1006 a 4094.

Figura 3. Imagen de red - VLAN Fuente: Shutterstock/606840716 **VLAN normal:** este tipo son las más usadas y se configuran en redes pequeñas y medianas, se enumeran de la 1 a la 1005, aunque el rango 1002 a 1005 se encuentra reservado para para VLAN de *token ring* y fibra óptica, la información de estas VLAN se almacena en el archivo VLAN.dat, y permite el uso del protocolo <u>VTP</u> el cual se usa para administrar y configurar VLAN entre los *switch Cisco*. **VLAN extendidas:** se utilizan en empresas grandes que requieren de una gran cantidad, por ejemplo, ISP, cuenta con menor número de características que las VLAN normales, se enumeran del 1006 al 4094, la configuración se almacena en archivo de configuración en ejecución y no admite VTP.



# ¿Cómo se crean las VLAN?



Configuración básica de VLAN Alfredo Heranz

https://youtu.be/71lol-RsNBA

Para crear VLAN existen tres formas diferentes y estas son:

**a)** En el modo Exec o modo privilegiado se escribe el comando VLAN *database* switch#VLAN database

#### **IOS Command Line Interface**

Switch#vlan data
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated. Please consult user documentation for configuring VTP/VLAN in config mode.
Switch(vlan)#vlan 10 name sistemas
VLAN 10 added: Name: sistemas
Switch(vlan)#vlan 20 name tesoreria

Figura 4. Creación de VLAN por *database* Fuente: propia

Fijémonos que al utilizar la función VLAN database sale un mensaje de advertencia que informa que se recomienda configurar VLAN en el modo de configuración global (en IOS de cisco superiores a la versión 15.x desaparece esta función). Una vez en el submenú VLAN se procede a crear la VLAN asignándole un número y un nombre (se recomienda el uso de <u>nemotecnia</u> para la asignación de nombres).

Nemotecnia: Se refiere a utilizar nombres que hagan referencia al objeto.

E



Para verificar si las VLAN se crearon podemos digitar el comando Show VLAN en modo privilegiado.

En la siguiente imagen observamos que se han creado las VLAN sistemas y tesorería, pero no tienen ningún puerto asociado.

Swite	ch#shot	w vlan									
VLAN	Name				Sta	tus Po	orts				
1	defaul	lt			act:	ive <mark>F</mark> a	Fa0/1, Fa0/2, Fa0/3, Fa0/4				
						Fa	10/5, 1	Fa0/6, Fa	0/7, Fa	0/8	
						Fa	10/9, 1	Fa0/10, F	a0/11, 1	Fa0/12	
						Fa	0/13,	Fa0/14,	Fa0/15,	Fa0/16	
						Fa	0/17,	Fa0/18,	Fa0/19,	Fa0/20	
						Fa	0/21,	Fa0/22,	Fa0/23,	Fa0/24	
						Gi	.g0/1,	Gig0/2			
10	sister	mas			act:	ive					
20	tesore	eria			act:	ive					
1002	fddi-	default			act,	/unsup					
1003	token	-ring-defa	ault		act.	/unsup					
1004	fddine	et-default	5		act.	/unsup					
1005	trnet	-default			act,	/unsup					
VLAN	Туре	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Transl	Trans2	
1	enet	100001	1500	-	-	-	-	-	0	0	
10	enet	100010	1500	. <del></del>		3774		2	0	0	
20	enet	100020	1500	_	-	<u>_</u>	-	월	0	0	
1002	fddi	101002	1500	-	-	() <del></del> ()	-	8	0	0	
1003	tr	101003	1500	्रत्त ह	-	1. <del></del> )	-	=	0	0	
1004	fdnet	101004	1500			3774	ieee		0	0	
		101005	1500	100	12	<u> </u>	ibm	- 22	0	0	

Figura 5. Resultado de emitir el comando Show VLAN Fuente: propia **b)** Otra forma de crear VLAN y la recomendada es ubicarnos en el modo configuración Global, crearla VLAN con el comando VLAN acompañado del número de VLAN, ya dentro del menú VLAN crear el nombre de la misma.

Switch (config)# VLAN 30 Switch (config-VLAN)#name compras Switch (config)#exit Switch (config)# VLAN 40 Switch (config-VLAN)#name ventas

#### **IOS Command Line Interface**

```
Switch>ena
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 30
Switch(config-vlan)#name compras
Switch(config-vlan)#exit
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name tesoreria
VLAN #20 and #40 have an identical name: tesoreria
Switch(config-vlan)#name ventas
```

Figura 6. Creación de VLAN desde el modo de configuración global Fuente: propia

En la siguiente figura verificamos la creación de las VLAN con el comando ya explicado Show VLAN, pero si observamos todos los puertos siguen asignados a la VLAN 1.

1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
			Fa0/5, Fa0/6, Fa0/7, Fa0/8
			Fa0/9, Fa0/10, Fa0/11, Fa0/12
			Fa0/13, Fa0/14, Fa0/15, Fa0/16
			Fa0/17, Fa0/18, Fa0/19, Fa0/20
			Fa0/21, Fa0/22, Fa0/23, Fa0/24
			Gig0/1, Gig0/2
10	sistemas	active	
20	tesoreria	active	
30	compras	active	
40	ventas	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	

Figura 7. Verificando la creación de VLAN Fuente: propia **c)** La tercera forma de crear una VLAN es asignar un puerto o un conjunto de puertos a una VLAN inexistente, al no encontrarla informará que no existe y la creará automáticamente.

¿Cómo se asigna un puerto a una VLAN?



direccionamiento de VLAN. Net Config.

https://youtu.be/I9AaSvrwWQY

Para asignar un puerto a una VLAN debemos acceder a la configuración del puerto ya dentro de él utilizamos el comando "*switchport*" el cual permite configurar las principales características del puerto, el modo de trabajo y a la seguridad del mismo.

Existen dos modos de trabajo de los puertos mode Access y mode Trunk.



El modo acceso se usa para conectar una máquina a un puerto, este puerto transportara información de una única VLAN.

El modo *Trunk* o troncal permite el transporte de varias VLAN por un único puerto, se recomienda para interconectar dispositivos intermediarios como *switch* o *router* (una buena práctica empresarial es interconectar dispositivos intermediarios por puertos de alta velocidad).

Para el ejemplo iniciaremos asignando el puerto 1 a la VLAN 10:

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#switchport mode access (se le indica el modo de trabajo).

Switch(config-if)#switchport access VLAN 10 (se asigna el puerto a la VLAN 10).

En la siguiente figura observamos las características configurables de *switchport* y la asignación del puerto f0/1 a la VLAN 10.

```
Switch>ena
Switch#
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) #int
Switch(config) #interface f
Switch(config) #interface fastEthernet 0/1
Switch (config-if) #switchport ?
             Set access mode characteristics of the interface
 access
               Set trunking mode of the interface
 mode
               Set trunking native characteristics when interface is in
 native
               trunking mode
 nonegotiate Device will not engage in negotiation protocol on this
                interface
 port-security Security related command
               Set appliance 802.1p priority
 priority
 trunk
                Set trunking characteristics of the interface
 voice
                Voice appliance attributes
Switch (config-if) #switch
Switch(config-if) #switchport mode access
Switch(config-if) #switchport mode access
Switch(config-if)#switchport access vlan 10
                                                              Autoría Propia
```

Figura 8. Características configurables en *switchport* Fuente: propia También se pueden configurar conjuntos de puertos que trabajarán de forma similar y que se encuentren en las misma VLAN, para esto trabajaremos con la función *Range*.

Para el ejemplo asignaremos el conjunto de puertos *fastEthernet* del 2 al 6 a la VLAN 10.

Switch(config)#interface Range fastEthernet 0/2-6

Switch(config-if-range)#switchport mode access (modo de trabajo).

Switch(config-if-range)#switchport access VLAN 10 (asigna los puerto a la VLAN).10)

Siguiendo el proceso anterior asigne los puertos 7 al 10 a la VLAN 20; los puertos 11 al 15 a la VLAN 30, los puertos 16 al 20 a la VLAN 40 y los puertos Giga en modo *trunk* (troncal).

En la siguiente imagen observamos que están asignados los puertos de la manera solicitada.

```
Switch(config-if-range) #int ran g0/1-2
Switch(config-if-range) #sw
Switch(config-if-range) #switchport mode trunk
Switch(config-if-range) #end
Switch#
SYS-5-CONFIG_I: Configured from console by console
Switch#sh vlan
VLAN Name
                               Status Ports
1
  default
                               active Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                      Gig0/1, Gig0/2
                               active Fa0/1, Fa0/2, Fa0/3, Fa0/4
10 sistemas
                                       Fa0/5, Fa0/6
                               active Fa0/7, Fa0/8, Fa0/9, Fa0/10
20 tesoreria
                               active Fa0/11, Fa0/12, Fa0/13, Fa0/14
30 compras
                                       Fa0/15
                               active Fa0/16, Fa0/17, Fa0/18, Fa0/19
40 ventas
                                                            Autoria propia
                                       Fa0/20
```

Figura 9. Asignación de puertos a VLAN Fuente: propia

# **Eliminando VLAN**

Para eliminar VLAN nos debemos ubicar el modo de configuración global y la instrucción "NO VLAN" acompañado del número de VLAN a eliminar.

Switch(config)# no VLAN 10 (eliminará la VLAN 10).

# ¡Importante!

- Con el comando anterior se elimina la VLAN 10, pero, ¿qué pasa con los puertos que estaban asignados a esta VLAN?
- Los puertos que estaban asignados a la VLAN quedarán inactivos hasta que se reasignen a una nueva VLAN o se coloque en la VLAN por defecto.
- **3.** Para evitar este tipo de inconvenientes se aconseja antes de eliminar la VLAN asignar los puertos a la VLAN nativa o a una VLAN de parqueo.
- 4. Para eliminar la configuración de todas las VLAN es necesario eliminar el archivo VLAN.dat que se encuentra en la memoria flash, debemos ubicarnos en el modo privilegiado y digitar el comando "delete VLAN.dat". Switch# delete VLAN.dat

# Creando VLAN administrativa



Figura 10. Red Fuente: Shutterstock/71146456

Para crear la VLAN administrativa es necesario configurar la dirección IP en el puerto SVI, recordemos que esta VLAN se usará únicamente para configuración de *switch* de forma remota ya sea por Telnet o SSH.



Recordemos que para acceder de forma remota no solo se tiene que tener una dirección IP en el *switch*, sino que también se necesita que el dispositivo tenga un nombre, una contraseña, y configurado la línea de acceso remoto VTY. Iniciaremos por asignarle un nombre al switch, una contraseña al modo privilegiado y una contraseña a la línea de acceso remoto VTY (pasos fundamentales para poder acceder de forma remota). Switch> enable

Switch# configure terminal

Switch(config)#hostname Sw1 (asigna el nombre al switch).

Sw1(config)# enable secret CISCO (crea contraseña de acceso).

Sw1(config)#line vty 0 15 (entra a configuración línea VTY).

Sw1(config-line)#password CISCOVTY (asigna contraseña a línea VTY).

Sw1(config-line)# login (sube el servicio VTY).

Siguiendo las buenas prácticas continuamos creando una VLAN diferente a la 1 para volverla administrativa, para el ejemplo crearemos la VLAN 100.

Sw1(config)#VLAN 100 (se crea la VLAN 100).

Sw1(config-VLAN)# name VLANadmin (le asignamos un nombre a la VLAN).

Sw1(config-VLAN)#exit (salimos del modo configuración de VLAN).

Sw1(config)#interface VLAN 100

(accedemos a la VLAN 100 como interfaz SVI).

Sw1(config-if )#ip address 192.168.10.1 255.255.255.0 (asignamos dirección IP).

Sw1(config-if)# no shutdown (encendemos la interfaz SVI).

Hasta este punto hemos configurado los elementos básicos del *switch*, creando la VLAN 100, asignado la dirección IP al SVI, al igual que mascara de red y por último la encendimos. Con estos pasos la hemos convertido en VLAN administrativa.

Paso siguiente, es asignar un puerto a esta VLAN para poder acceder vía Telnet o SSH al dispositivo, para lo cual asignaremos el puerto 24 a la VLAN 100.

Sw1(config)# interface fastEthernet 0/24 (accedemos al puerto 24).

Sw1(config-if)# switchport mode access (colocamos el puerto en modo acceso).

### Sw1(config-if)# switchport access VLAN 100 (se vincula el puerto a la VLAN 100).

Ahora si conectamos un equipo al puerto 24 de *switch* podremos accede vía Telnet al dispositivo.

# **Creando VLAN nativa**

La VLAN nativa es la que permitirá el tráfico entre diversas VLAN y el tráfico no etiquetado, por lo tanto, los puertos asignados a esta deben estar en modo Trunk o modo troncal (se recomienda que los puertos troncales sean los de mayor velocidad ya por ellos pasaran todo el tráfico de la red).

Sw1(config)# interface GigabitEthernet 0/1 (accede al puerto G0/1). Sw1(config-if)# switchport mode trunk (lo convierte en modo troncal).

Sw1(config-if)# switchport trunk native VLAN 110 (configura VLAN native 110).

Sw1(config-if)# switchport trunk allowed VLAN 10,20,30,40,100 (permite el tráfico de VLAN indicadas).

# **Experimentemos**

## Creación de VLAN

Requerimientos: un *switch* 2960 y seis computadoras.

**1.** Diseñar en *Packet Tracer* la siguiente arquitectura de red, y asignar el direccionamiento IP a las máquinas (conectar los PC a los puertos 1 a 6 del *switch*).



2. Hacer ping entre las máquinas ¿Pasan todos los paquetes?, ¿por qué?

- **3.** Crear 3 VLAN y asignar puertos a ellas de la siguiente manera:
  - a. VLAN 11 puertos 1 al 10.
  - b. VLAN 12 puertos 11 al 15.
  - c. VLAN 13 puertos 16 al 20.

**4.** Cambiar el puerto de conexión de los Pc2 y el Pc3 a los puertos 12 y 13 consecutivamente.

- 5. Cambiar el puerto de conexión de los Pc4 y Pc5 a los puertos 18 y 19.
- 6. Hacer ping entre las máquinas ¿pasan todos los paquetes?, ¿por qué?
- 7. Cambie a modo simulación y analice cómo pasan los paquetes.

# ilmportante!

Atención al direccionamiento asignado en el ejercicio anterior, **no** es el indicado (solo se realiza para experimentar), ya que cuando se generar VLAN se deben asignar rangos de redes diferentes o realizar un direccionamiento jerárquico con la ayuda de CIDR.

# Comparemos resultados y analicemos

Dando respuesta a la pregunta del punto dos, donde se cuestiona si los paquetes pasan y por qué.

Si analizamos el direccionamiento, todas las máquinas están en el mismo segmento de red es decir pertenecen a la misma red (192.168.10.0 /24) y como están conectadas al mismo dispositivo (*switch*) y este presenta una configuración por defecto o de fábrica, los paquetes pasaran sin ningún inconveniente.

Al analizar el punto seis observamos que ya no hay paso de paquetes entre todas las máquinas, esto se debe a que se han cambiado de VLAN algunos equipos. Por ejemplo, el PC2 y PC3 se cambiaron a los puertos 12 y 13 respectivamente y estos puertos pertenecen a la VLAN 12.

Por otra parte, el PC4 y PC5 se cambiaron a los puertos 18 y 19 respectivamente y este rango de puertos pertenece a la VLAN 13.



Figura 12. Comparación Fuente: Shutterstock/390415018

Por último, observamos que el PCO y PC1 no se modificaron de puerto y los puertos del 1 al 10 pertenecen a la VLAN 11.

Analizando esto la comunicación solo se dará entre equipos que estén en la misma VLAN, ya que al generar VLAN se crean segmentos lógicos e independientes de red los cuales solo se podrán ver con la ayuda de un dispositivo capa 3, la cual permita el enrutamiento entre VLAN.



Para afianzar el conocimiento adquirido hasta el momento los invito a desarrollar el caso simulado y la actividad de repaso 1; disponible en la página de inicio del eje 3.

- Bellido, Q. (2014). Equipos de interconexión y servicios de red (UF1879). Madrid, España: IC Editorial.
- Bermúdez, L. (2012). Montaje de infraestructuras de redes locales de datos: UF1121. Madrid, España: IC Editorial.
- Calvo, G. (2014). Gestión de redes telemáticas (UF1880). Madrid, España: IC Editorial.
- Feria, G. (2009). Modelo OSI. Córdoba, Argentina: El Cid Editor | apuntes.
- García, M. (2012). Mantenimiento de infraestructuras de redes locales de datos (MF0600\_2). Málaga, España: IC Editorial.
- Hillar, G. (2004). *Redes: diseño, actualización y reparación*. Buenos Aires, Argentina: Editorial Hispano Americana HASA.
- Íñigo, G., Barceló, O., y Cerdà, A. (2008). Estructura de redes de computadores. Barcelona, España: Editorial UOC.
- Martínez, Y., y Riaño, V. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid, España: Servicio de Publicaciones. Universidad de Alcalá.
- Molina, R. (2014). Implantación de los elementos de la red local. Madrid, España: RA-MA Editorial.
- Mora, J. (2014). Desarrollo del proyecto de la red telemática (UF1870). Madrid, España: IC Editorial.
- Purser, M. (1990). Redes de telecomunicación y ordenadores. Madrid, España: Ediciones Díaz de Santos.
Roa, B. (2013). Seguridad informática. Madrid, España: McGraw-Hill España.

- Robledo, S. (2002). *Redes de computadoras*. Ciudad de México, México: Instituto Politécnico Nacional.
- Romero, J. (2009). Estudio de subnetting, VLSM, Cidr y comandos de administración y configuración de routers. Córdoba, Argentina: El Cid Editor | Apuntes.
- S.L. Innovación y Cualificación. (2012). Guía para el docente y solucionarios: montaje y mantenimiento de sistemas de telefonía e infraestructuras de redes locales de datos. Málaga, España: IC Editorial.
- Vásquez, D. (2009). Base de la teleinformática. Córdoba, Argentina: El Cid Editor | apuntes.
- Velte, T., y Velte, A. (2008). *Manual de Cis*co. Ciudad de México, México: McGraw-Hill Interamericana.

# ADMINISTRACIÓN Y SEGURIDAD EN REDES

Ricardo López Bulla

EJE 4

Propongamos



ك كشo administrador de TI de una compañía, qué política de enrutamiento recomendar y por qué?

En el diseño y configuración de una red LAN es necesario visualizar la globalidad de dicha red y entender que esta requerirá de una salida al exterior, es decir necesitará interconectar diversos segmentos de red, conectarse a Internet, y/o conectarse a otras redes, para esta labor se necesita de un dispositivo que posibilite dicha interconexión.

En este eje estudiaremos la funcionalidad y configuración de dicho dispositivo de interconexión, al igual que la generación de tablas de rutas estáticas y dinámicas, para lo cual nos apoyaremos de lecturas complementarias, videocápsulas, casos simulados, talleres, los cuales ayudarán a afianzar los conocimientos adquiridos.

Enrutamiento de redes



Con lo que hemos visto hasta el momento, sabemos que dos dispositivos terminales se podrán comunicar si y solo si se encuentran en la misma red, en el mismo segmento de red y/o en misma VLAN.

Si un dispositivo de la red se quiere comunicar con otro dispositivo que pertenezca a una red, segmento o VLAN diferente, necesitarán la intervención de un dispositivo intermediario capaz de generar el proceso de enrutamiento, a este dispositivo se le denomina enrutador (*router*) o encaminador.

El router es un dispositivo que trabaja en capa de red (capa 3 del modelo OSI) su función es encaminar paquetes de una red a otra, tiene las características similares a un equipo de cómputo, pues posee procesador, memoria (RAM, ROM, memoria Flash, memoria Nvram), sistema operativo, puertos de entrada y puertos de salida. Aunque no posee una tarjeta de video, cuenta con un puerto de consola que permite acceder a la configuración del mismo con la ayuda de un cable de consola y de un programa emulador de terminal com Putty, TeraTeam, Hyper Terminal, entre otros.

Para reafirmar los conceptos vistos hasta el momento los invito a desarrollar la siguiente lectura complementaria, la cual explica que es un *router* y que papel cumple en la red.

## Lectura recomendada

Manual de Cisco, leer de la parte 2 el numeral 3: Revisión general de los enrutadores.

Tony Velte y Anthony Velte.



Figura 2. Puertos y componentes de un *router* Fuente: propia

El enrutamiento (encaminamiento) hace referencia a la búsqueda del mejor camino para el viaje de los paquetes entre dos redes, segmentos de redes o VLAN.

La elección del router y del mejor camino o ruta se dará gracias a las tablas de rutas, las cuales para su creación tienen en cuenta dos factores fundamentales: la distancia administrativa (DA) y la métrica.

Antes de definir los conceptos de DA y métrica los invito a realizar la lectura complementaria:



## Lectura recomendada

Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF, leer métrica y distancia administrativa.

Fernando Boronat Seguí y Mario Montagud Climent. La cual explica la importancia de la métrica y la distancia administrativa al momento de tomar la decisión de envió de un paquete.

**Distancia administrativa (DA):** Cisco define la DA como la medida de confiabilidad del origen de la ruta.

Es el primer criterio que un router usa para determinar el protocolo de enrutamiento a utilizar.

Si un *router* reconoce a una red por diversos protocolos de enrutamiento escogerá el de menor valor de DA, es decir el más confiable.

La distancia administrativa es local y no se publica en las actualizaciones de ruteo.

En la siguiente tabla se muestran las distancias administrativas predeterminadas en *router Cis*co:

Tipo de ruta	Valor distancia administrativa
Directamente conectado	0
Rutas estáticas	1
Rutas sumarizadas	5
Rutas EBGP	20
Rutas EIGRP	90
Rutas IGRP	100
Rutas OSPF	110
Rutas IS-IS	115
Rutas Rip	120
Rutas EIGRP (externo)	170
Rutas BGP	200

Tabla 1. Distancia administrativa Fuente: propia

Como ejemplo veamos qué pasa si un router descubre una red por medio del protocolo Eigrp interno y el protocolo RIP.

- 1. El router comparará los valores de DA de los dos protocolos. Para el ejemplo: DA - Eigrp interno = 90, DA - Rip = 120.
- 2. El router se decide por el protocolo más confiable, el que tienen menor distancia administrativa. Para el ejemplo Eigrp interno.
- **3.** Incluirá esta ruta en su tabla de rutas.



Figura 3. Fuente: shutterstock/574000213

**Métrica**: es una medida utilizada para calcular la mejor ruta hacia una red destino. Cada protocolo de enrutamiento utiliza unos determinados factores para el cálculo de su métrica. Algunos de los factores más utilizados para el cálculo de la métrica son:

Número de saltos: medido como el número de router por lo que necesita pasar el paquete para llegar al destino.

- Retardo o tiempo: tiempo que dura el paquete en llegar de un extremo a otro.
- Velocidad de enlace, también denominada tasa de transferencia. Es la velocidad de transmisión del enlace medida en <u>bps</u>, las velocidades más comunes de los enlaces son 10 Mbps, 100 <u>Mbps</u>, 1000 Mbps y 10 000 Mbps.
- Costo: sobrecarga que se requiere para el envío de paquetes a través de la interfaz, inversamente proporcional al ancho de banda.
- Ancho de banda: cantidad de datos que pueden viajar por la red de forma simultánea en un determinado periodo de tiempo.
- Confiabilidad: medida de fiabilidad de la fuente de información.

bps Bit por segundo, es la unidad de medida de velocidad de transferencia de bit.

#### <u>Mbps</u>

Megabit por segundo, múltiplo de bit. 1Mbps= 1024bps.

## Tipos de enrutamiento

Una vez vista la importancia del enrutamiento en la interconexión de redes, debemos entender cómo se forman o crean las tablas de rutas.



Figura 4. Mapa conceptual protocolos de enrutamiento Fuente: propia

## រាំ ¡Impor tante!

La creación de dichas tablas de rutas o tablas de enrutamiento se puede dar de dos formas, por medio del enrutamiento estático y por medio de enrutamiento dinámico, el ingeniero director de TI y su departamento de tecnología, se encargará de definir entonces cual es mejor esquema de enrutamiento. **Enrutamiento estático:** en este esquema las tablas de rutas son creadas y definidas manualmente por el administrador de red.

Entre las principales ventajas de crear enrutamiento estático están:

- Bajo consumo de recursos de red, esto debido a que no se requieren procesos adicionales de router (memoria o procesador), ni generan sobrecarga de procesos.
- Optimiza el ancho de banda pues no consume recursos ni genera procesos constantes de actualización del router en la red.
- Seguridad, al ser generado de forma manual los router no anunciaran las rutas a sus vecinos, esto evitará que personas ajenas a la organización accedan a estos equipos y a las redes que ellos interconectan.
- Rapidez, al estar configuradas las rutas de forma estáticas se crean caminos predefinidos, lo cual agiliza el envío de paquetes ya que no debe tomar decisiones si no seguir la ruta asignada.
- Enrutamiento desde y hacia redes de conexión única, es decir conjunto de router con una única puerta de enlace o de último recurso, comúnmente utilizado al interior de las empresas.
- Uso de una única ruta, por defecto usada en caso de que no existan coincidencias en la tabla de rutas.



Figura 5. Fuente: shutterstock/585410489

El enrutamiento estático presenta también una serie de debilidades por lo cual es recomendable generar un análisis detallado de la red antes de tomar una decisión de enrutamiento, sin olvidar que es posible combinar los dos tipos de enrutamiento para optimizar dicho proceso y generar una red más segura y estable.

Dentro de las principales debilidades del enrutamiento estático tenemos:

- Entre más grande la red más compleja la configuración. Por esto se recomienda para redes pequeñas.
- No se adapta a topologías cambiantes, es decir para cada cambio ocurrido en la red, debe intervenir el administrador dela misma.

- No determina la ruta óptima, ya que no realiza análisis de costos, ancho de banda, saltos, es decir no utiliza métricas para el envío de paquetes, pues ya está determinada su ruta, si la ruta sufre fallo o congestión el reintentara el envío por la misma ruta, hasta que el administrador de red configure otra.
- No es escalable, lo que significa que cada vez que lleguen nuevos dispositivos intermediarios (router o switch capa 3) no se reconocerán ni habrá convergencia hasta que sean configurados en las tablas de rutas de cada dispositivo de forma manual por el administrador y se generen las nuevas rutas y caminos.
- En redes muy grandes y por requerir la intervención del ser humano la configuración es susceptible a errores.
- Se requiere conocimiento de toda la red para una óptima configuración.
- El mantenimiento se vuelve complejo entre más rutas se tengan.

## Lectura recomendada

Redes locales, por favor leer enrutadores o router y rutas estáticas.

Rafael Jesús Castaño Ribes y Jesús López Fernández. Para afianzar los conceptos de enrutamiento los invito a realizar la lectura complementaria:

La cual da una introducción al enrutamiento y explica la importancia de las rutas estáticas.

## Datos:

- La configuración del IOS de los router Cisco es muy similar a la configuración del IOS del switch, los modos de usuario, modo privilegiado, modo de configuración global, modo de configuración de línea son los mismos.
- La diferencia radica en que los router poseen interfaz, mientras los switch tienen puertos, cada Interfaz de un router es un dominio de broadcast, es decir separa el dominio de difusión de las redes.

Las interfaces de los *router* requieren ser configuradas para ser usadas, a estas se les debe configurar:

- La dirección IP.
- El *clock rate* o tasa de transferencia (únicamente a la interfaz serial DCE).
- Deben encenderse (por defecto las interfaces están apagadas).

**Reto 1:** configurar una *router Cis*co 1941 para que permita que dos redes diferentes se interconecten entre sí.

Requerimientos: un *router* 1941, dos *switch* 2960, cuatro máquinas terminales PC.

• Desarrolle en *Packet Tracerel* montaje de la topología de acuerdo a la figura.



Figura 6. Topología reto 1 Fuente: propia

- Configure los PC de acuerdo al direccionamiento mostrado en la figura.
- Conecte un PC1 al *router* con cable de consola para poder ingresar por medio terminal al IOS del *router*.
- Una vez haya ingresado al sistema operativo del router configure los parámetros básicos del dispositivo. (nombre R1; Password= CISCO; password en la línea de consola = CISCOCON; Password en la línea VTY=CISCOVTY; IP interfaz g0/0 = 192.168.10.1 255.255.255.0; IP interfaz G0/1 =10.10.10.1 255.255.255.0) y encienda las interfaces.

router> enable (modo usuario). router# configure terminal (modo privilegiado). router(config)#hostname R1 (modo configuración- asignación de nombre). R1(config)#Enable secret CISCO (crea el password de acceso). R1(config)#line con 0 (accede a la línea de configuración de consola). R1(config-line)#password CISCOCON (crea el password de acceso a consola). R1(config-line)#login (activa el password). R1(config-line)#exit R1(config-line)#exit R1(config)#line vty 015 (accede a la línea de configuración VTY). R1(config-line)# password CISCOVTY

R1(config-line)# login

R1(config-line)#exit

R1(config)#interface G0/0 (accede a la interfaz Giga 0/0).

R1(config-if)# IP address 192.168.10.1 255.255.255.0 (asigna dirección IP).

R1(config-if)# no shutdown (enciende la interfaz Giga 0/0).

R1(config-if)#exit

R1(config)#interface G0/1

R1(config-if)# IP address 10.10.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)#exit

## Analicemos

 Haga ping de cada máquina a la dirección del router, ¿responden los pings? y ¿por qué?

En el PC0 C:\>ping 192.168.10.1

En el PC2 C:\>ping 10.10.10.1

- Haga ping entre las máquinas conectadas al mismo switch, ¿responden los pings? y ¿por qué?
  - En el PC0 C:\>ping 192.168.10.11 En el PC2 C:\>ping 10.10.10.11
- Haga *ping* entre las máquinas de diferente red, ¿responden los pings? y ¿por qué?

En el PC0 C:\>ping.10.10.10.11 En el PC2 C:\>ping 192.168.10.10

Al generar el *ping* entre las máquinas y el *router* este responde porque se encuentra en la misma red, están conectados y está encendida la interfaz del mismo.

Al generar el *ping* entre las máquinas de la misma red, los *pings* responden por que se encuentran en la misma red, el mismo segmento de red y en la misma VLAN.

Al generar ping entre redes diferentes, el ping es fallido porque están en diferente red.

¿El router no permite que se interconecten redes diferentes?

Precisamente esa es la función del router interconectar diversas redes, lo que sucede es que en los equipos falto la configuración de la puerta de enlace o gateway.

El gateway o puerta de enlace es el que va a permitir entrar o salir de la red local, y todo paquete que pertenezca a una red diferente de la red que emite el mensaje se direccionara al *router* para que este encamine el paquete a la red destino siempre y cuando se encuentre un camino en la tabla de rutas.

## <mark>ាំ</mark> ;lmpor tante!

En las redes caseras y/o empresariales la puerta de enlace va a ser el *router* o el servidor que permite la salida al exterior y/o a Internet y la dirección del *gateway* debe pertenecer al mismo segmento de red o a la misma red del host o equipo terminal que emite el mensaje.

Para configurar el gateway en los equipos terminales o *host* entramos a la configuración de la tarjeta de red de cada equipo y le agregamos la dirección del gateway.

En la siguiente figura observamos la configuración del *gateway* en *Packet Tracery* en un equipo real.

PCI		Propiedades: Protocolo de Internet versio	in 4 (TCP/IPv4)
Physical Config Desktop	Attributes Software/Services	General	
IP Configuration IP Configuration		Puede hacer que la configuración IP se as red es compatible con esta funcionalidad. consultar con el administrador de red cua apropiada.	igne automàticamente si la De la contrario, deberá es la configuración IP
O DHCP	Static	Obtener una dirección IP automática	mente
IP Address	192.168.10.10	Usar la siguiente dirección IP:	
Subnet Mask	255.255.255.0	Dirección IP:	192.168.10.10
Default Gateway	192,168,10,1	Máscara de subred;	255 . 255 . 255 . 0
DN3 JEIVEI		Puerta de enlace predeterminada:	192.168.10.1
IPv6 Configuration		Obtener la dirección del servidor DN	S automáticamente
O DHCP O A	uto Config 🧕 Static	Usar las siguientes direcciones de se	rvidor DNS:
IPv6 Address		Servidor DNS preferido:	- H. H. H.
Link Local Address	FE80::230:A3FF:FE75:AA34	Servidor DNS alternativo:	1 (4 F)
IPv6 Gateway		and the second s	<i>i</i>
IPv6 DNS Server		Valdar configuración al salir	Opciones avanzadas
Configuración	en packet tracer	Configuración PC Re	Aceptar Cancelar

Figura 7. Configuración de gateway o puerta de enlace Fuente: propia Una vez configurado el *gateway* en todos los equipo o *host*, realizar nuevamente la comprobación de *ping* entre las máquinas de diferente red.

### ¿Pasan los paquetes?

En el PC0 C:\>ping.10.10.10.10 En el PC2 C:\>ping 192.168.10.10

Como nos damos cuenta, ahora **si** pasan los paquetes entre diferentes redes, es decir el *router* está cumpliendo con su labor de interconectar redes y encaminar los paquetes.

¿Pero por qué pasan los paquetes si no hemos creado tablas de rutas en el router?

Si no fijamos bien, No se han creado tablas de rutas ni configurado un protocolo de enrutamiento que permita la generación dinámica de tablas de rutas.

La razón para que las máquinas del ejemplo anterior siendo de diferente red se conecten entre sí sin haber creado tablas de rutas, es porque las dos redes están directamente conectadas al mismo router y generará enrutamiento entre las redes conectadas directamente al él.



**Reto 2**: interconectar por medio de dos router 1941 dos redes remotas que no comparten conexión al mismo *router*.

Requerimientos: dos *router* 1941 con tarjeta de red serial, dos switch 2960, cuatro máquinas terminales PC.

- Desarrolle en Packet Tracer el montaje de la topología de acuerdo a la figura.
- Agregue la interfaz serial EHWIC a la ranura del lado derecho de los router.
- Configure los PC de acuerdo al direccionamiento mostrado en la figura.
- Interconecte los dispositivos con el tipo de cable apropiado (PC Sw cable UTP, Sw *Router* cable UTP, *Router* Router cable serial tipo DCE al R1).



Figura 8. Topología con dos router - reto 2 Fuente: propia

- Conecte el PC1 al *router* 1, con cable de consola para poder ingresar por medio terminal al IOS del router.
- Una vez haya ingresado al sistema operativo del router 1 configure los parámetros básicos del dispositivo. (nombre R1; Password= CISCO; password en la línea de consola = CISCOCON; Password en la línea VTY=CISCOVTY; IP interfaz Giga0/0 = 192.168.10.1 255.255.255.0) y encienda la interfaz.
- Configure la interfaz S0/0/0 con la dirección 20.20.20.1 255.255.255.0
- Configure el clock rate 128000 en esta interfaz (DCE).
- Encienda el puerto serial.
- Conecte ahora el PC2 al *router* 2 con cable de consola para poder ingresar por medio terminal al IOS del *router*.
- Una vez haya ingresado al sistema operativo del router 2 configure los parámetros básicos del dispositivo. (nombre R2; Password= CISCO; password en la línea de consola = CISCOCON; Password en la línea VTY=CISCOVTY; IP interfaz G0/0 =10.10.10.1 255.255.255.0) y encienda las interfaces.

- Configure la interfaz S0/0/0 del R2 con la dirección 20.20.20.2 255.255.255.0
- En esta interfaz no se configura el clock rate pues es de tipo DTE.
- Encienda el puerto serial.

Atención la configuración básica es la misma descrita en el Reto 1, repita los pasos.

Después de desarrollar la configuración básica de los *router* procederemos a configurar la interfaz serial.

R1(config)#interface serial S0/0/0 R1(config-if)# ip address 20.20.20.1 255.255.255.0 R1(config-if)# clock rate 128000 R1(config-if)# no shutdown

Ahora configuramos las interfaces en R2 (previamente configurar los elementos básicos de *router*).

R2(config)#interface Giga0/0 R2(config-if)# ip address 10.10.10.1 255.255.255.0 R2(config-if)# no shutdown R2(config)#interface serial S0/0/0 R2(config-if)# ip address 20.20.20.2 255.255.255.0 R2(config-if)# no shutdown

Notemos que en esta interfaz no se configura *clock rate*, ya que está conectada por cable DTE.

## Analicemos

 Haga ping de cada máquina a la dirección del router, ¿responden los pings? y ¿por qué?

En el PC0 C:\>ping 192.168.10.1 En el PC1 C:\>ping 192.168.10.1 En el PC2 C:\>ping 10.10.10.1 En el PC3 C:\>ping 10.10.10.1  Haga ping entre las máquinas conectadas al mismo switch, ¿responden los pings? y ¿por qué?

En el PC0 C:\>ping 192.168.10.11 En el PC2 C:\>ping 10.10.10.11

• Haga *ping* entre las direcciones de las interfaces seriales de los *router* conectados, ¿responden los *pings*? y ¿por qué?

R1# ping 20.20.20.2 R2# ping 20.20.20.1

• Haga ping entre las máquinas de diferente red, ¿responden los pings? y ¿por qué?

En el PC0 C:\>ping.10.10.10.10 En el PC1 C:\>ping.10.10.10.11 En el PC2 C:\>ping 192.168.10.10 En el PC3 C:\>ping 192.168.10.11

Una vez emitidos los *pings* notamos que entre los dispositivos de la misma red los *pings* responden, entre las máquinas del mismo segmento, entre el *router* y la máquina perteneciente a la red y entre los *router* el *ping* responde.

Pero entre las máquinas de diferente red los *pings* **no** responden.

 Verificar que la puerta de enlace esté correctamente configurada (para el ejercicio ya la configuramos correctamente). ¿Por qué no se ven las máquinas entre distintas redes si ya configuramos correctamente todo?

La respuesta es sencilla, como las dos redes que contienen host no están conectadas al mismo router, por lo que no generarán un enrutamiento local, entonces es necesario configurar una tabla de rutas que permita encaminar los paquetes.

Como lo vimos anteriormente la tabla de rutas se puede configurar de forma estática o dinámica.

## Configuración enrutamiento estático



Existen dos tipos de rutas estáticas, ruta estática específica (se configura para llegar a una red específica y ruta estática predeterminada (se configura para llegar a cualquier red no especifica).

Las tablas de rutas se configuran en los router en el modo de configuración global, para crear enrutamiento estático específico se requiere conocer la dirección de la red o las redes de destino (redes que no estén directamente conectadas al router), la máscara de la red de destino y el *next hop* o próximo salto, el cual será la dirección IP de la interfaz del router que recibirá el paquete.

Con el comando "ip route" se creará la ruta de la siguiente forma. R1(config)#ip route dirección IP destino máscara de red, destino próximo salto.

## Para nuestro ejemplo: R1(config)# ip route 10.10.10.0 255.255.255.0 20.20.20.2

Quiere decir que R1 no está conectado directamente a la red 10.10.10.0 pero puede llegar a ella por intermedio de la interfaz serial del siguiente *router* R2 la cual tiene como dirección 20.20.20.2, a esta interfaz se le denomina *next hop* o siguiente salto de R1 porque a R2 le entregará el paquete para que sea entregado a su destino final.

Otra manera de configurar la tabla de ruta estática específica es conocer la dirección de la red o las redes de destino, la máscara de la red de destino y la interfaz de salida del *router* que emite el mensaje siempre y cuando esta interfaz sea serial (*point to point*).

R1(config)#ip route dirección IP destino máscara de red, destino interfaz salida. R1(config)#ip route 10.10.10.0 255.255.255.0 serial 0/0/0

## j ;Impor tante!

Cuando una ruta se define por próximo salto e interfaz de salida se le denomina ruta completamente definida. Ahora bien, si la interfaz de salida es tipo *Ethernet* no se recomienda configurar por interfaz de salida ya que este tipo de interfaz es multipunto y generará problemas de rendimiento en la red.

Ya configurada la tabla de rutas en el router R1, procederemos a configurar la tabla de rutas en el *router* R2.

R2(config)#ip route 192.168.10.0 255.255.255.0 20.20.20.1 R2(config)#ip route 192.168.10.0 255.255.255.0 serial 0/0/0

Una vez terminado el proceso de configuración de la tabla de rutas en todos los *router*, se verifica conectividad emitiendo un *ping* desde la red de origen a la red de destino.

 Haga ping entre las máquinas de diferente red, ¿responden los pings? y ¿por qué?

En el PC0 C:\>ping.10.10.10.10 En el PC1 C:\>ping.10.10.10.11 En el PC2 C:\>ping 192.168.10.10 En el PC3 C:\>ping 192.168.10.11

Efectivamente los pings ya responden porque se creó la tabla de rutas en cada *router*. Para verificar la tabla de rutas en el router imita el comando "show ip route" en el modo privilegiado y obtendrá el resultado que nos muestra la siguiente figura.

#### R1#show ip route

La tabla de códigos nos muestra que la letra **S** significa enrutamiento estático, al observar la tabla de rutas vemos que aparece en el segundo renglón.

#### S 10.10.10.0/24 {1/0} vía 20.20.20.2

Explicación del resultado obtenido:

S (estático) tipo de enrutamiento que descubrió la red.

10.10.10.0/24 (red de destino y mascara), {1/0} distancia administrativa de ruta estática DA = 1 y métrica = 0 (no realiza cálculo de métrica por ser ruta estática), vía 20.20.20.2 significa la vía por la que tomo o el próximo salto (*next hop*). En la siguiente figura observamos la tabla de rutas que se ha creado:

```
R1#show ip route
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
     10.0.0.0/24 is subnetted, 1 subnets
s
        10.10.10.0/24 [1/0] via 20.20.20.2
                      is directly connected, Serial0/0/0
C
        20.20.20.0/24 is directly connected, Serial0/0/0
        20.20.20.1/32 is directly connected, Serial0/0/0
L
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C
        192.168.10.0/24 is directly connected, GigabitEthernet0/0
L
        192.168.10.1/32 is directly connected, GigabitEthernet0/0
```

Figura 10. Tabla de rutas – ruta estática Fuente: propia

Otros elementos que podemos interpretar de la figura de la tabla de rutas es que se encuentran dos redes conectadas directamente.

C 20.20.20.0/24 directly connected, Serial 0/0/0

C 192.168.10.0/24 directly connected, Gigabit 0/0

C conectada directamente.

20.20.20.0/64 Dirección de red y mascara de la red conectada.

Serial 0/0/0 interfaz por la cual está conectada esa red.



Video cápsula: "rutas predeterminadas" Autor: José Luis Usero Vílchez

## Ruta estática predeterminada



representará a cualquier red que no esté en la tabla de rutas. Al crear la ruta estática predetermina-

La ruta estática predeterminada es la ruta que coincide con todos los paquetes y

da se crea un *gateway* de último recurso y cualquier paquete que no encuentre la red destino en la tabla de rutas será enviado a dicho gateway de último recurso.

Su configuración es similar a cualquier ruta estática con la diferencia que la red de destino es 0.0.0.0 y la máscara 0.0.0.0

Figura 11 Fuente: propia.

R1(config)#ip route 0.0.0.0 0.0.0.0 20.20.20.2 R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0

R2(config)#ip route 0.0.0.0 0.0.0.0 20.20.20.1 R2(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0

Este tipo de rutas se utiliza comúnmente cuando se conecta una red interna al ISP, o cuando conecta un *router* con otro único *router*.

Al crear la ruta estática esta se anunciará en la tabla de rutas como S\* en donde "S" indica que es una ruta estática y "\*" indica que es una ruta estática predeterminada por defecto y se seleccionara como *gateway* de último recurso, como se ve en la siguiente figura:



Figura 12. Tabla de rutas - ruta estática predeterminada Fuente: propia



## Instrucción

Los invito a desarrollar la actividad de repaso rutas estáticas.

### Rutas estáticas IPv6

Las rutas estáticas para IPv6 se configuran con el comando "*ipv6 route*" y al igual que IPv4 se pueden configurar por siguiente salto o por interfaz de salida.



Video cápsula: rutas estáticas Autor: Juan Carlos Cabeza Frías **Reto 3:** configurar direccionamiento IPv6 y el enrutamiento estático IPv6.

- Utilice el mismo montaje del reto dos para desarrollar direccionamiento y enrutamiento IPv6.
- Asigne direcciones IPv6 a las máquinas de acuerdo a las direcciones mostradas en la figura, utilice como puerta de enlace la dirección FE80::1 para R1 y FE80::2 para R2.
- Configure *router* R1 y R2 con el direccionamiento IPv6 de acuerdo a las direcciones asignadas en la gráfica.
- S0/0/0 2001:DB8:20::1/64 S0/0/0 2001:DB8:20::2/64 FE80::1 FE80::2  $\mathbf{O}$ Router 1941-1 💧 Router 1941-2 G0/0 2001:DB8:10::1/64 S0/0/0 2001:DB8:30::1/64 FE80::1 FE80::2 ( )SW 2960-0 SW 2960 PC0 PC1 PC2 PC3 2001:DB8:10::10/64 2001:DB8:10::11/64 S0/0/0 2001:DB8:10::11/64 S0/0/0 2001:DB8:10::11/64 FE80::1 FE80::1 FE80::1 FE80::1
- Cree las tablas de rutas estáticas IPv6 con el comando "ipv6 route".

Figura 13. Topología con dos *router* en IPv6 Fuente: propia

- Verifique la tabla de rutas IPv6 de cada router por medio del comando "show ipv6 route".
- Compruebe conectividad por medio de *ping* entre los *hosts* de las diferentes redes.
  - R1(config)#ipv6 unicast-routing (habilita el protocolo IPv6 en el router).
  - R1(config)#interface Giga 0/0
  - R1(config-if)#ipv6 address 2001:db8:10::1/64 (asigna dirección IPv6 y prefijo).
  - R1(config-if)#ipv6 address FE80::1 Link-local (asigna dirección link-local).
  - R1(config-if)#no shutdown
  - R1(config-if)#exit
  - R1(config)#interface serial 0/0/0

R1(config-if)#ipv6 address 2001:db8:20::1/64 R1(config-if)#ipv6 address FE80::1 Link-local R1(config-if)#clock rate 128000 (asigna tasa de transferencia a la interfaz DCE). R1(config-if)#no shutdown R1(config-if)#exit

Configurando tabla de rutas IPv6.

R1(config)# ipv6 route 2001:db8:30::/64 2001:db8:20::2 (ruta estática siguiente salto).
R1(config)# ipv6 route 2001:db8:30::/64 S0/0/0 (ruta estática por interfaz de salida).
R1(config)# ipv6 route ::/0 2001:db8:20::2 (ruta estática predeterminada).
R1(config)# ipv6 route ::/0 S0/0/0 (ruta estática predeterminada por interfaz de salida).
R1(config)# ipv6 route ::/0 S0/0/0 (ruta estática predeterminada por interfaz de salida).
R1(config)#exit
R1# show IPv6 route (muestra las tablas de rutas IPv6).

Ahora proceda a configurar el R2 (el mismo proceso que R1) con los datos de direccionamiento que aparecen en la figura, recuerde que la puerta de enlace va a ser FE80::2.

En la siguiente figura observamos el resultado de emitir el comando "show ipv6 route" el cual nos mostrará la tabla de rutas IPv6 para R1:

**IOS Command Line Interface** R1#show ipv6 route IPv6 Routing Table - 7 entries Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP U - Per-user Static route, M - MIPv6 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -OSPF ext 2 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 S ::/0 [1/0] via 2001:DB8:20::2 via Serial0/0/0, directly connected via GigabitEthernet0/0, directly connected L 2001:DB8:10::1/128 [0/0] via GigabitEthernet0/0, receive 2001:DB8:20::/64 [0/0] via Serial0/0/0, directly connected 2001:DB8:20::1/128 [0/0] 14 Jeria10/0/0, 1 2001:DB8:30::/64 [1/0] S via 2001:DB8:20::2 via Serial0/0/0, directly connected

> Figura 14. Tabla de rutas – ruta estática predeterminada IPv6 Fuente: propia

Observemos que en IPv6 las redes predeterminadas no llevan el símbolo "\*" solo llevan el identificador de tipo de ruta S (estática), pero se muestran como S ::/0.

Una vez configurados los router emita ping entre los hosts de diferente red.

En el PC0 C:\>ping 2001:DB8:30::10 En el PC1 C:\>ping 2001:DB8:30::10 En el PC2 C:\>ping 2001:DB8:10::11 En el PC3 C:\>ping 2001:DB8:10::11

Observamos que los paquetes pasan sin problema, es decir se ha creado enrutamiento estático IPv6.



## Enrutamiento dinámico

Para empezar, los invito a realizar la lectura complementaria:



Lectura recomendada

Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF, leer protocolos de enrutamiento.

Fernando Boronat Seguí y Mario Montagud Climent.

La cual explica que son los protocolos de enrutamiento, tipo de protocolos e introduce al protocolo RIP, definiendo características y funcionalidades.



### No olvides que

La creación dinámica de las tablas de rutas es la mejor alternativa en redes grandes y en continuo cambio y/o actualización, pues se actualizarán de forma automática sin necesidad que intervenga el administrador de red, al igual son adecuadas en topologías que requieren varios *router*.

El enrutamiento dinámico busca el mejor y más confiable camino y si esta falla es capaz de tomar una ruta alterna, garantizando la entrega y optimizando el tiempo de respuesta.

El enrutamiento dinámico presenta algunas desventajas, dentro de las cuales tenemos: mayor tráfico en la red, mayor consumo de ancho de banda, requerirán de mayores recursos de *router* (memoria, procesador, etc.), son más inseguros y la configuración puede ser más compleja.

Cuando hablamos de rutas dinámicas debemos hablar de protocolos de enrutamiento pues estos son los encargados de generar la tabla de rutas en el *router*. en la siguiente tabla observamos las principales características de los diversos tipos de protocolos de enrutamiento.

Tipo de protocolo	Protocolo	Características
Vector distancia	Rip,RipV2, RipNg, IGRP, EIGRP	Las rutas se publican de acuerdo a la distancia métrica y número de saltos, se publica periódicamente la tabla de enrutamiento, lo cual genera un tráfico innecesario en la red. Utiliza el próximo salto para la entrega del paquete. Útil en redes simples y planas. La mayoría de estos protocolos están descontinuados.
Estado de enlace	ospf, IS-IS	ldeal en redes grandes y complejas dentro de sistemas autónomos SA, optimiza la entrega de paquetes ya que crea un mapa global de la red, adecuado en redes jerár- quicas, convergen de forma rápida y optimizan los recursos de la red. El OSPF es el protocolo de pasarela interior más utilizado en las redes actuales.
Vector camino	BGP	Protocolo de pasarela exterior encargado de interconectar sistemas autónomos SA, generando caminos entre dichos SA. El protocolo utilizado por Internet, en la actualidad se denomina BGP4.

Tabla 2 protocolos de enrutamiento Fuente: propia El estudio de los protocolos de vector distancia, estado de enlace, vector camino, están fuera del alcance de este curso, sin embargo, daremos una mirada introductoria al protocolo RIP.

## **Protocolo RIP**



El protocolo RIP (*Routing Information Protocol*) es un protocolo de pasarela interior IGP (*Internal Gateway Protocol*), su algoritmo de encaminamiento se basa en vector distancia, es decir que su métrica son únicamente los saltos, lo cual lo hace lento e inoperante, por esta misma razón el protocolo está en desuso, pero es útil en la academia para el entendimiento de la formación de la tabla de rutas dinámicas.

La primera versión de RIP alcanzaba 15 saltos máximo, es decir que a partir del 16 se consideraban redes inalcanzables. RIPv1 es un protocolo con clase, no soporta <u>VLSM</u> y <u>CIDR</u>, lo cual resultaba poco eficiente, por último RIP se considera inseguro pues no incluye mecanismos de autenticación.

RIPv1 es un protocolo que no es utilizado en redes de producción.

La segunda versión de RIP denominada RIPv2 es una versión mejora RIPv1, esta versión soportar redes VLSM, CIDR, y autenticación, pero sigue manteniendo su número máximo de 15 saltos.

RIP es un protocolo obsoleto y de poco uso en redes de producción.

RIPng (*Rip Next Generation*) la siguiente generación está desarrollada para soportar el protocolo IPv6.

**Reto 4:** configurar enrutamiento estático RIPv2 y RIPng en modo *Dual Stack* en la topología dada.

<u>\_\_\_\_\_</u>

Mascara de subred de tamaño variable.

<u>CIDR</u> mascara de subred de tamaño variable.

## j ;Importante!

Dual stack es un mecanismo de transición a IPv6 que consiste en la asignación de direcciones IPv4 e IPv6 a cada dispositivo (el tema no hace parte del ámbito de la materia, pero se nombra para desarrollar en un solo montaje de red, el doble enrutamiento RIPv2 y RIPng.

#### Desarrollo:

- 50/0/0 20.20.20.1/24 50/0/0 20.20.20.1/24 2001:DB8:20::1/64 2001:DB8:20::2/64 FE80::1 FE80::2 Ø Router 1941-1 Router 1941-2 G0/0 2001:DB8:10::1/64 50/0/0 10.10.10.1/24 FE80::1 2001:DB8:30::1/64 FF80::2  $\mathbf{C}$ SW 2960-0 SW 2960 PC0 PC2 PC1 PC3 192.168.10.10/24 50/0/0 10.10.10.10/24 192.168.10.11/24 50/0/0 10.10.10.11/24 2001:DB8:10::10/64 2001:DB8:30::10/64 2001:DB8:10::11/64 2001:DB8:30::11/64 FE80::1 FE80::1 FE80::2 FE80::2
- Elabore en Packet Trace y el montaje de dispositivos de acuerdo a la figura dada.

Figura 16. Topología de red IPv6 Fuente: propia

- Asigne direccionamiento IPv4 e IPv6 a cada equipo de acuerdo al direccionamiento presentado en la figura.
- Configure los parámetros de cada *router* (Nombre, *password*, seguridad de línea con, mensaje, direccionamiento IPv4 e IPv6 a cada interfaz).
- Una vez todo configurado y encendidas las interfaces, procedemos a configurar el enrutamiento dinámico RIP, para lo cual se emitirá en modo de configuración global el comando "router rip".

Para IPv4 emitiremos los comandos:

- R1(config)#router rip (configuración enrutamiento RIP).
- R1(config-router)# version 2 (configuración versión 2 de RIP).
- R1(config-router)#network 192.168.10.0 (red directamente conectada al router R1).
- R1(config-router)# network 20.20.20.0 (red directamente conectada al router R1).

Para IPv6 emitiremos los comandos:

R1(config)# ipv6 unicast-routing (habilita protocol lpv6).

R1(config)#ipv6 router rip ANDINA (habilita RIP en IPv6 con una palabra clave para nuestro ejemplo ANDINA, pero puede ser cualquier palabra).

- R1(config-rtr)# exit
- R1(config)# interface Giga 0/0
- R1(config-if)# ipv6 rip ANDINA enable (habilita enrutamiento RIP en la interfaz G0/0 con la palabra clave que habíamos creado para el ejemplo ANDINA).
- R1(config-if)# exit
- R1(config)# interface serial 0/0/0
- R1(config-if)# ipv6 rip ANDINA enable
- R1(config-if)# exit

Con este listado de comandos hemos configurado el R1 para enrutamiento RIP IPv4 e IPv6.

## j ilmpor tante!

Notemos que para configurar RIP en IPv4 es necesario registrar cada red conectada directamente al *router* dentro del protocolo RIP. Para configurar RIPng no se necesitan registrar redes, pero sí en cambio, se debe habilitar cada interfaz para que permita el paso de RIPng.

- Configure el enrutamiento RIP y RIPng, en el router R2 de forma similar a lo configurado en el R1.
- Una vez configurado el R2 emita el comando "show ip route" y el comando "show ipv6 router" en R1 y en R2.

Se obtendrá un resultado similar al de la siguiente figura, en donde R representa las rutas descubiertas por el protocolo RIP.



Figura 17. Tabla de rutas – protocolo de enrutamiento RIPng Fuente: propia Bellido, Q. (2014). Equipos de interconexión y servicios de red (UF1879). Madrid, España: IC Editorial.

Bermúdez, L. (2012). Montaje de infraestructuras de redes locales de datos: UF1121. Madrid, España: IC Editorial.

Boronat, S., y Montagud, C. (2013). Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. Valencia, España: Editorial de la Universidad Politécnica de Valencia.

Calvo, G. (2014). Gestión de redes telemáticas (UF1880). Madrid, España: IC Editorial.

Feria, G. (2009). Modelo OSI. Córdoba, Argentina: El Cid Editor | apuntes.

García, M. (2012). Mantenimiento de infraestructuras de redes locales de datos (MF0600\_2). Málaga, España: IC Editorial.

Hillar, G. (2004). *Redes: diseño, actualización y reparación*. Buenos Aires, Argentina: Editorial Hispano Americana HASA.

Íñigo, G., Barceló, O., y Cerdà, A. (2008). Estructura de redes de computadores. Barcelona, España: Editorial UOC.

Martínez, Y., y Riaño, V. (2015). IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6. Madrid, España: Servicio de Publicaciones. Universidad de Alcalá.

Molina, R. (2014). Implantación de los elementos de la red local. Madrid, España: RA-MA Editorial.

Mora, J. (2014). Desarrollo del proyecto de la red telemática (UF1870). Madrid, España: IC Editorial.

Purser, M. (1990). Redes de telecomunicación y ordenadores. Madrid, España: Ediciones Díaz de Santos.

Roa, B. (2013). Seguridad informática. Madrid, España: McGraw-Hill España.

Robledo, S. (2002). Redes de computadoras. Ciudad de México, México: Instituto Politécnico Nacional.

Esta obra se terminó de editar en el mes de Septiembre 2018 Tipografá BrownStd Light, 12 puntos Bogotá D.C,-Colombia.

# **AREANDINA** Fundación Universitaria del Área Andina

# MIEMBRO DE LA RED