Apuntes Packet Tracer

Utilidades

Comando	Función
Control + Shift + 6	Parar proceso corriendo
Control + z	Volver atrás
Shift + Insert	Pegar texto copiado
Tab	Autocompletar entrada
Flecha Arriba	Reinsertar comandos anteriores
?	Obtener documentación sobre un comando o parámetro
exit	Salir del modo actual, volver al anterior

Modos

Nota: Los modos (en general) van de menor a mayor permisos, y de menor a mayor especificidad.

Modo	Función	Para ingresar
[U] > Usuario	A penas entras, default	-
[P] # Privilegiado	Modo privilegiado	en
[CG] (config) Configuración Global	Configuración general	conf t
[CE] (config-X) Configuración Especifica	Configuraciones especificas	in [interfaz], entre otros

☑ *para identificar en qué modo va cada comando.*

Configuraciones

Nombre

```
[P] hostname [nombre]
```

Contraseña de [P]

```
[CG] enable password [contra]
```

Mostrar info

```
[P] show [cosa]
show r              | Running config
show in             | Interfaces
show in [interfaz] | Interfaz especifica
show v              | VLANs
show ac             | Access lists
show ip ro          | Tabla de rutas
show ip p           | Protocolo de enrutamiento
```

Interfaces

```
[P] interface f 0/0         | Interfaz especifica
[P] interface range f0/4-24 | Rango de interfaces
```

Output de "show interfaces"

Nota: show interface [interfaz] para ver solo una interfaz.

Output	Explicación
Interface is up	Está habilitado y tiene algo conectado
Interface is down	Está habilitado y no tiene algo conectado
Interface is administratively down	Deshabilitado. No se puede usar hasta que se habilite manualmente.

Seguridad de interfaz

Comando	Explicación
[Interfaz] switchport mode access	Configurar puerto en modo acceso
switchport port-security	Activar la seguridad del puerto
switchport port-security maximum 1	Numero máximo de MAC
switchport port-security mac-address [mac]	Asignar de MAC permitida
switchport port-security violation shutdown	Establecer acción ante violación. En este caso apagar puerto

Nota: Al hacer shutdown por una violation se pasa el puerto al estado administratively down.

IP administrativa

```
[CG] interface vlan 1     | Es la vlan por defecto
ip address [ip] [mascara] | Configurar IP y mascara
no shutdown               | Encender interfaz
```

Interfaz serial

Comando	Explicación
[CG] interface serial 0/0	Ingresar a interfaz
encapsulation ppp	Configurar protocolo de encapsulación
ip address [IP] [máscara]	Configurar IP y mascara
clock rate 2000000	Velocidad de reloj (SOLO en extremo DCE, icono relojito)
no shutdown	Encender interfaz

VLANs

Notas:

- Todos los switches involucrados deben tener configuradas las VLANs para poder direccionarlas correctamente.
- Por default todo está en la VLAN 1.

Crear VLANs

```
[CG] vlan [numero]
name [nombre]
```

Asignar un puerto a una VLAN

```
[Interfaz] switchport mode access
switchport access vlan [idVlan]
```

Trunk

```
[Interfaz] switchport mode trunk
```

Acceso remoto SSH

Notas: Existen 16 VTYs (Virtual Terminal). Desde 0 hasta 15.

Primero, activar acceso SSH en VTY 0.

Comando	Explicación
[CG] ip domain-name dominio.com	Configurar nombre de dominio

Comando	Explicación
crypto key generate rsa	Generar claves RSA (Se debe usar 1024, no el default)
ip ssh version 2	Configurar versión de SSH
line vty 0	Configurar terminal virtual (VTY) 0
transport input ssh	Configurar acceso SSH
login local	Configurar autenticación
[CG] username [user] privilege 15 password [pass]	Especificar user y pass

Por último, desactivar acceso en el resto de VTY.

Comando	Explicación
[CG] line vty 1 15	Configurar VTY 1 a 15
transport input none	Deshabilitar acceso remoto

Acceso remoto TELNET

Comando	Explicación
[CG] line vty 0 1	Configurar VTY 0 y 1
login	Configurar autenticación
password [contra]	Establecer contraseña
exec-timeout [minutos]	Timeout antes de terminar sesión

Spanning tree

Configurar este switch como root.

```
[CG] spanning-tree vlan [vlan1,vlanN] root primary
```

Enlace LACP

Este es un enlace que une dos puertos físicos lógicamente como si fueran el mismo. Esto se usa para evitar que spanning tree corte un bucle. Esto permite duplicar el ancho de banda de una conexion utilizando dos puertos a la vez.

```
port-channel load-balance {dst-mac | src-mac}
interface gigabitethernet 1/1
```

```
switchport mode trunk
channel-protocol LACP
```

Protocolo RIP

Comando	Descripción
[CG] router rip	Entra al modo de configuración del router para RIP
version 2	Version de RIP
network w.x.y.z	Especifica una red para incluirla en la tabla

*Nota: Las network deben estar en ip **CLASSFULL**. Es decir, la dirección de red (no subred) con la mascara default.*

Evitar la publicación de RIP en una interfaz

```
[Router rip] passive-interface [interfaz]
```

Establecer rutas sumarizadas CIDR

```
[CG] ip route [prefijo] [mascara] [interfaz]
```

Publico este prefijo, donde si una IP tiene el mismo prefijo, que me la manden porque ya la manejo.

Redistribuir rutas estáticas en el protocolo de ip dinámica

```
[Router rip] redistribute static
```

Para utilizar varios protocolos juntos

Supongamos que en un router tenemos los protocolos eigrp y rip. Entonces:

En la config de rip:

```
[Router rip] redistribute eigrp 99 metric 1
```

En la config de eigrp:

```
[Router eigrp] redistribute rip metric 10000 0 255 1 1500
```

Lista de acceso

Crear la acess list (Entrenar el patoba)

```
[CG] access-list [idAccessList] [accion] [origen] | Estandar
[CG] access-list [idAccessList] [accion] [protocolo] [origen] [destino] |
Extendida
```

idAccessList: Identificador de la access list

- 1-99 Estandar
- 100-199 Extendida

accion: Acción realizada si se matchea

- permit | Permitir
- deny | Denegar

protocolo: Protocolo a filtrar

- ip (siempre se usa ese, en primer parcial)

origen y destino: IPs a filtrar

- host [ip] | Una ip especifica
- any | Cualquier ip
- [ip] [wildcard] | Rango de IPs

wildcard: Es una "subnet mask inversa". Matchea bit a bit con la IP, solo donde la wildcard vale 0.

Activar la access list en una interfaz (Poner al patoba a laburar)

```
[Interfaz] ip access-group [idAccessList] [direccion]
```

direccion:

- in: Paquetes que entran
- out: Paquetes que salen

Sub-interfaces

Se utilizan para generar N interfaces virtuales en una interfaz física. Se utilizan para separar tráfico de diferentes VLANs en un router.

```
[CG] interface fX/X.[vlanId]
encapsulation dot1Q [vlanId]
```

```
ip address [ip] [mascara]
```

vlanId = ID de VLAN La IP elegida debe estar dentro de la VLAN en cuestion. Y debe ser configurada como el default gateway en los terminales.

Access list para evitar acceso entre VLANs

Una vez configuradas las subinterfaces, se puede acceder entre las difernetes VLANs a traves del router. Esto no es deseado. Por lo tanto, se deben configurar access lists para evitar estos accesos.

Crear access list

Se debe pensar en toda la combinatoria de accesos que se pueden producir entre las diferentes VLANs.

Ejemplo: Para las siguientes VLANs:

- 192.168.170.0/27
- 192.168.180.0/27
- 192.168.190.0/27 Las access list que se deben crear son:

```
access-list [idAccessList] deny ip 192.168.170.0 0.0.0.31 192.168.180.0
0.0.0.31
access-list [idAccessList] deny ip 192.168.170.0 0.0.0.31 192.168.190.0
0.0.0.31
access-list [idAccessList] deny ip 192.168.180.0 0.0.0.31 192.168.170.0
0.0.0.31
access-list [idAccessList] deny ip 192.168.180.0 0.0.0.31 192.168.190.0
0.0.0.31
access-list [idAccessList] deny ip 192.168.190.0 0.0.0.31 192.168.170.0
0.0.0.31
access-list [idAccessList] deny ip 192.168.190.0 0.0.0.31 192.168.180.0
0.0.0.31
access-list [idAccessList] permit ip any any
```

Nota: NO OLVIDAR el permit ip any any al final, porque sino todo lo que no matchee estas reglas se bloqueará, no es lo que queremos en este caso. Queremos hacer una lista negra (todo lo que no matchee es permitido).

Para 3 VLANs se debe crear:

- 1 -> 2
- 1 -> 3
- 2 -> 1
- 2 -> 3
- 3 -> 1
- 3 -> 2

Aplicar access list

Importante. Crear la access list no es suficiente. Se debe aplicar esta misma.

Ingresar a la configuracion de cada subinterfaz y aplicar la access list:

```
ip access-group [idAccessList] in
```

Túnel IPsec

Primero, definir (y anotar) estos datos:

- idCryptoPolicy (numero)
- idTransformSet (numero)
- idAccessList (numero)
- nombreMapa (string)
- claveSimetrica (string)

1) Configurar el IKE (Internet Key Exchange)

Comando	Descripción
[CG] crypto isakmp policy [idCryptoPolicy]	Configurar política de encriptación
encr AES	Algoritmo de encriptación
authentication pre-share	Método de autenticación. Clave pre-compartida
group 5	Grupo de Diffie-Helulman. Grupo 5, clave de 1536 bits
lifetime 900	Tiempo de vida de la clave (segundos)

2) Definir la clave simétrica con el otro extremo

```
[CG] crypto isakmp key [claveSimetrica] address [ip]
```

- claveSimetrica: Clave pre-compartida
- ip: IP del otro extremo

3) Configurar el IPSec modo túnel

```
[CG] crypto ipsec transform-set [idTransformSet] ah-sha-hmac esp-3des
```

- transform-set: Crea un mapa de transformación
- idTransformSet: Identificador del transform-set. Debe ser único
- ah-sha-hmac: Algoritmo de autenticación
- esp-3des: Algoritmo de encriptación

4) Configurar la lista de acceso

Nota: Esta lista de acceso determina que trafico se va a encriptar.

```
[CG] access-list [idAccessList] permit ip [ipOrigen] [wildcardOrigen]
[ipDestino] [wildcardDestino]
```

Nota: La wildcard es una "subnet mask inversa". Se matchean los valores en 0. Ejemplo:

```
access-list 100 permit ip 10.10.0.0 0.0.255.255 11.5.0.0 0.0.0.255
```

En este ejemplo, las ips cuyo origen matchee 10.10.X.X y su destino matchee 11.5.0.X, ingresará al túnel. (Será encriptado)

5) Configurar el mapa criptografico

Este determina la IP del otro extremo y el tráfico de interés que será encapsulado.

Comando	Descripción
crypto map [nombreMapa] [idCryptoPolicy] ipsec-isakmp	Crea un mapa criptográfico
set peer [ip]	IP del otro extremo
set security-association lifetime seconds 1800	Tiempo de establecimiento de la asociación de seguridad
set transform-set [idTransformSet]	Vincula el transform-set 50 creado anteriormente
match address [idAccessList]	Vincula la lista de acceso 101 creada anteriormente

6) Activar el túnel (Poner el patoba IPsec a trabajar)

```
[Interface] crypto map mymap
```

Nota: Recordar aplicar esta config en AMBOS extremos del tunel. Donde la UNICAS diferencias deben ser:

- Las access list deben estar al reves el origen y el destino.
- El "set peer" debe apuntar al OTRO extremo.
- El "crypto isakmp key" debe apuntar al OTRO extremo.

Wireless

Modos del AP

- Router: Es un Router inalámbrico. En este modo se crea una red independiente de la red cableada, y se realizan todas las funciones de un Router a la vez que de un AP.
- Bridge: Funciona como un puente inalámbrico. En este modo no se crea una red, se extiende la red existente. El AP reenvía los paquetes entre la red cableada y la inalámbrica, sin realizar funciones de router.

Modo Router

Para conectar el AP en este modo, se debe usar su puerto WAN (Internet). En este modo, el AP genera su propia WLAN, y además se conecta con otro router para tener acceso al resto de redes.

Ejemplo:

- RouterA usa su interfaz f0/0 para conectarse con el AP1, y el AP1 usa su interfaz Internet para conectarse con RouterA.
- Entre RouterA y AP1 usan la red 192.168.170.0/24 para conectarse entre sí.
- Entonces, el RouterA tiene configurada la IP 192.168.170.254/24 en f0/0. AP1 tiene la IP 192.168.170.253/24 en su interfaz Internet.
- Ademas, el AP creará la red 192.168.180.0/24 para su WLAN

Para configurar el AP, ingresar a la GUI:

```
**Pestaña Setup:**
Internet Setup:
Connection Type: Static IP
IP Address: IP de este router en la red con el otro router. En este ejemplo
192.168.170.253
Subnet Mask: Mascara de subred. En este ejemplo 255.255.255.0
Default Gateway: IP del otro router. En este ejemplo 192.168.170.254

Network Setup:
IP Adress: IP de este router en la red de la WLAN. En este ejemplo
192.168.180.1
Subnet Mask: Mascara de subred. En este ejemplo 255.255.255.0
Activar DHCP Server
Elegir la IP inicial y la cantidad de usuarios(IPs) maxima

**Pestaña Wireless:**
Configurar lo que se pida sobre la red en Basic Wireless Setttings y
Wireless Security
```

Luego ir a los dispositivos terminales de la WLAN y configurar:

- IP en DHCP.
- Credenciales de la red wireless.

Modo Bridge

Para conectar el AP en este modo, se debe usar alguno de sus puertos LAN (Ethernet). En este modo, el AP extiende la red LAN existente, creando su red WLAN. Actúa como un puente que conecta ambas. El AP se conecta a un switch.

Ejemplo:

- AP1 se conecta a SwitchA por su puerto LAN.
- SwitchA es parte de una red X.
- Entonces, el AP1 se conecta a la red X.
- El AP1 crea su red WLAN 192.168.168.64/27

Para configurar el AP, ingresar a la GUI:

```
**Pestaña Setup:**
Internet Setup:
Connection Type: Automatic Configuration - DHCP

Network Setup:
IP Address: IP de este router en la red WLAN. En este ejemplo
192.168.168.65
Subnet Mask: Mascara de subred. En este ejemplo 255.255.255.224 (/27)
Activar DHCP Server
Elegir la IP inicial y la cantidad de usuarios (IPs) maxima

**Pestaña Wireless:**
Configurar lo que se pida sobre la red en Basic Wireless Setttings y
Wireless Security
```

Luego ir a los dispositivos terminales de la WLAN y configurar:

- IP en DHCP.
- Credenciales de la red wireless.