Comandos para Cisco

Deniso Xocuis

15 de abril del 2024

1 Configuración básica del router

```
Router(config) #hostname [NAME]
```

Contraseñas:

```
Router(config) #enable secret [PASSWORD]
Router(config) #service password-encryption
Router(config) #line console 0
Router(config-line) #loggin synchronous
Router(config-line) #password [PASSWORD]
Router(config-line) #login
Router(config)#line vty 0 4
Router(config-line) #password [PASSWORD]
Router(config-line)#login (y exit)
Router(config) #no service password-encryption
```

Conf de un mensaje de bienvenida:

```
Router(config)#banner motd # MESSAGE #
```

Configuración de una interfaz

```
Router(config)#interface [TYPE NUMBER]
Router(config-if)#ip address [IP] [MASK]
Router(config-if) #no shu
```

No interactuar con el DNS

```
no ip domain-lookup
```

Guardar cambios realizados: `Router#copy run start`

Verificación de la configuración básica:
```
Router#show run conf
Router#show ip route
Router#show ip int br
Router#show interfaces
show ip protocols
```

Análisis de interfaces del router: `show ip route`
```
show int
show ip int br
show run
```

Historial de comandos
Almacena temporalmente la lista de comandos ejecutados que se deben recuperar
```
terminal history size 200
show history
```

1.1 Enrutamiento estático

1. Agregar conf básica ;)
```
Router(config)#ip route [IP RED DESCONOCIDA][MASK][PUERTA ENLACE]
```

1.2 Enrutamiento dinámico

1.2.1 RIPv2

1. Agregar conf básica ;)
```
Router(config)#router rip
Router(config-router)#version 2
Router (config-router)#network [IP] (clase completa nomas)
Router(config-router)#passive-interface [NAME]
Router(config-router)#no auto-summary
```

1.2.2 EIGRP

1. Agregar conf básica ;)
```
Router(config)#router eigrp 100
Router(config-router)#no auto-summary
Router(config-router)#eigrp log-neighbor-changes
Router(config-router)#network [IP] (clase completa nomas)
```

1.3 ACCESS LIST

1. Agregar conf básica ;)
2. Enrutamiento estático o dinámico
Creación
`access-list [ID][deny|permit][ip][wildcard][log]`

Aplicación:
Para permitir el resto del tráfico `R2(config)#access-list [ID] permit any`
Para aplicar la ACL a una interfaz: `R2(config)# int [NAME]`
`R2(config-if)#ip access-group [ID] (in|out)`

Verificar:
`show ip interface`
`show access-lists`

ACL ESTÁNDAR
`access-list [ID] [deny|permit][IP][WILDCARD]`
or
`access-list [ID] [deny|permit] host [IP]`

ACL ESTENDIDA
`access-list [ID] [permit|deny][PROTOCOL][IP][IP destino wildcard][TCP APPLICATION]`

Sintaxis
Protocolo: ip — tcp — udp — icmp
Comparación: gt — it — eq
Origen de una sola ip: host
Origen de cualquier ip: any
Máscara wildcard: el inverso de la máscara
¿Dónde se aplican?
Las ESTÁNDAR se colocan cerca del destino
Las EXTENDIDAS se deben colocar cerca de la fuente
IN : El tráfico que llega a la interfaz y luego pasa por el router.
OUT: El tráfico que ya ha pasado por el router y está saliendo de la interfaz
EJEMPLO:
La red 192.168.11.0/24 (R2) no tiene permiso para acceder al DNS en la red 192.168.20.0/24. Se permite el resto de los tipos de acceso.
Se debe crear una ACL en R2, la lista de acceso se debe colocar en la interfaz de salida hacia el DNS. Se debe crear una segunda regla en el R2 para permitir el resto del tráfico.
La red 192.168.10.0/24(R3) no tiene permiso para comunicarse con la red 192.168.30.0/24. Se permite el resto de los tipos de acceso

Para restringir el acceso de la red 192.168.10.0/24(R3) a la red 192.168.30/24 sin interferir con otro tráfico, se debe crear una lista de acceso en el R3. La ACL se debe colocar en la interfaz de salida hacia la PC3. Se debe crear una segunda regla en el R3 para permitir el resto del tráfico.

2 VLAN

3 VTP

VTP: protocolo troncal de vlan (solo se usa en cisco)
mode access: recibe la info del servidor
mode trunk: manda toda la info para el resto de los clientes(switches)

4 INTER VLAN