



Acceso a la Red

Creacion de VLANs

Entrar al modo privilegiado:

```
Switch>enable
```

Entrar al modo de configuración global:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Crear una VLAN con un ID valido:

```
Switch(config)#vlan 10
```

Nombrar la VLAN para fácil identificación:

```
Switch(config-vlan)#name ventas
```

Asignar una interface del switch a una VLAN:

```
Switch(config)#interface fastethernet 0/1
Switch(config)#switchport mode access
Switch(config)#switchport access vlan 10
```

Validar la configuracion de asignacion de la VLAN con comando show:

```
Switch#show vlan
```

Puertos de acceso y puertos con Voice VLAN:

Ingresar al modo configuración global:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Entrar al modo de configuración global:

```
Switch#configure terminal
Switch(config)#
```

Seleccionar interface y configurarla en modo acceso:

```
Switch(config)#interface gigabitEthernet 0/1
```

```
Switch(config-if)#switchport mode access
```

Asignar VLAN de datos:

```
Switch(config-if)#switchport access vlan vlan-id
```

De manera opcional si tienes VLAN de voz, acá la asignar VLAN de voz:

```
Switch(config-if)#switchport voice vlan vlan-id
```

Verificación:

En el modo privilegiado, usar el commando:

```
Switch#show vlan
```

VLAN Nativa:

Asignar VLAN de datos como vlan nativa:

```
Switch(config-if)#Switchport trunk native vlan vlan-id (VLAN Datos)
```

Verificación:

```
Switch#show vlan  
Switch#show vlan brief  
Switch#show interfaces gigabitEthernet 0/1 Switchport
```

Creacion y asignacion de interfaces TRUNKs o troncales

Ingresar al modo configuración global:

```
Switch#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.
```

Ingresar a la interface deseada:

```
Switch(config)#Interface fastEthernet 0/24
```

Habilitar el puerto en modo trunk:

```
Switch(config-if)#switchport mode trunk
```

Verificacion. Mostrar las interfaces que estan en modo trunk:

```
Switch#show interfaces trunk
```

Verificacion. Mostrar los detalles de una interface especifica:

```
Switch#show interfaces fastEthernet 0/24 switchport
```

SVIs

Crear la VLAN:

Ingresar al modo configuración global:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 100
Switch(config)#vlan 100
```

Ingresar la primera interface LAN, asignar la IP y activarla:

```
Switch(config)#interface vlan 100
Switch(config-if)#ip address 10.1.1.254 255.255.255.0
Switch(config)#no shutdown
```

Ingresar la segunda interface VLAN, asignar la IP y activarla:

```
Switch(config)#interface vlan 200
Switch(config-if)#ip address 10.2.1.254 255.255.255.0
Switch(config)#no shutdown
```

CDP

Habilitar CDP en el modo de configuración global:

```
Switch(config)#cdp run
```

Verificación:

```
Switch#show cdp neighbors
```

Para obtener información más detallada del vecino:

```
Switch#show cdp neighbors detail
```

LLDP

Activar LLDP en el modo de configuración global:

```
Switch(config)#lldp run
```

Verificación:

```
Switch#show lldp
Switch#show lldp neighbors
```

Etherchannel

Se crea una interfaz de tipo port-channel y se asigna un número.

```
Switch# configure terminal
Switch (config)# interface port-channel 1
```

Generalmente, en un etherchannel se busca transmitir más de una VLAN, por tanto, los puertos se configuran como trunk, pero es posible también hacerlo como access si así se requiere.

```
Switch(config)# interface range GigabitEthernet 0/1
Switch(config-if)# Switchport mode trunk
Switch(config-if)# Switchport trunk vlan-id,vlan-id
```

Se asigna el puerto al port-channel, y el modo.

Podemos configurar Etherchannel de tres formas en Switches Cisco. Port Aggregation Protocol (PAgP) tiene dos Channel modes y ellos son "Desirable" y "Auto". Link Aggregation Control Protocol (LACP) tiene dos Channel modes y ellos son "Active" y "Passive". Manual, tiene solamente el modo: on.

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

Verificación:

```
Switch# show interface port-channel channel-number
Switch# show port-channel summary
```

Spanning Tree Protocol (STP):

Activar spanning tree:

```
Switch(config)#spanning-tree mode stp
```

Comando para configurar el root bridge de forma manual (default: 32768):

```
Switch(config)#spanning-tree priority priority
```

Definir costo de spanning tree en las interfaces:

```
Switch(config)#interface gigabitEthernet 1/1
Switch(config-if)#spanning-tree cost cost
```

Verificación:

```
Switch# show spanning-tree
Switch# show spanning-tree brief
```

PVST

Este es el modo por default de spanning-tree en Switches Cisco.

```
Switch(config)#spanning-tree mode pvst
```

Configurar primary y secondary root bridges para cada VLAN:

```
Switch(config)#spanning-tree vlan vlan-id root primary
Switch(config)#spanning-tree vlan vlan-id root secondary
```

Verificación:

```
Switch#show spanning-tree
Switch#show spanning-tree vlan vlan-id
```

MST

Activar MST.

```
Switch(config)# spanning-tree mode mst
```

Configurar parámetros requeridos para MST:

```
Switch(config)# spanning-tree mst configuration
```

Nombre de la region MST:

```
Switch(config-mst)# name name
```

Número de la revisión, puede ser de 0 a 65535:

```
Switch(config-mst)# revision 5
```

Número de la instancia y el rango de VLAN a incluir en la misma:

```
Switch(config-mst)# instance instance-id vlan vlan-range
```

Las VLAN que no se incluyan en la instancia creada, pasarán automáticamente a ser parte de la instancia por default (instancia 0).

Conectividad IP

Rutas estáticas

Entrar al modo privilegiado:

```
Router>enable
```

Entrar al modo de configuración global:

```
Router#configure terminal
Router(config)#
```

Existen dos comandos para crear una ruta estática:

Por IP de próximo salto:

```
Router(config)#ip route red_destino [máscara]  
IP_address_próximo_salto [distancia_administrativa]
```

Por interfaz de salida:

```
Router(config)#ip route red_destino [máscara] interface_de_salida  
[distancia_administrativa]
```

Verificación:

```
Router#show ip route
```

OSPF Single Area

Activar OSPF:

```
Router(config)#router ospf process_ID
```

El process_ID es significativo solo de forma local, y puede estar entre 1 y 65,535.

Definir las interfaces que van a participar en el proceso OSPF:

```
Router(config-router)# network IP_network [wildcard mask] area  
area_number
```

La wildcard mask es diferente a la máscara de sub-red. La wildcard mask le dice al proceso OSPF la parte de la red que debe coincidir en la interfaz.

El router-ID es un identificador único del router OSPF. A diferencia del ID de proceso, este tiene importancia en toda la red OSPF, no solo de forma local. Se escribe en el mismo formato que las direcciones IPv4. Si no se define manualmente, el router la asignará de forma automática.

```
Router(config-router)#router-id ip_address_format
```

Verificación:

```
Router#show ip protocols  
Router#show ip ospf  
Router#show ip ospf neighbor
```

OSPF Multi Area

Activar OSPF:

```
Router(config)# router ospf process_ID
```

Definir las interfaces que van a participar en el proceso OSPF. Importante fijar el área donde se encuentra la interfaz:

```
Router(config-router)# network IP_network [wildcard mask] area  
area_number
```

Definir router-ID:

```
Router(config-router)#router-id ip_address_format
```

Verificación:

```
Router#show ip protocols
Router#show ip ospf
Router#show ip ospf neighbor
```

HSRP

Seleccionar interfaz primaria e interfaz secundaria:

```
Router(config)#interface Interface-id
```

Configurar el grupo y la IP primaria o secundaria:

```
Router(config-if)#standby [group-number] ip [ip-address [secondary]]
```

Configurar prioridad HSRP, rango de 1 a 255, default es 100, el número más alto representa la mayor prioridad:

```
Router(config-if)#standby [group-number] priority priority
```

Cambiar de estado a activo cuando el router tiene una interfaz con una prioridad más alta:

```
Router(config-if)#standby [group-number] preempt
```

Verificación:

```
Router#show standby [interface-id [group]]
```

VRRP

Seleccionar la interfaz:

```
Router(config)#interface interface-id
```

Habilitar VRRP en la interfaz, y establecer prioridad (opcional):

```
Router(config-if)# vrrp group description text
Router(config-if)# vrrp group priority level
```

Cambiar de estado a activo cuando el router tiene una interfaz con una prioridad más alta:

```
Router(config-if)# vrrp group preempt [delay minimum seconds]
```

Configurar intervalo entre cada aviso sucesivo del router master. Tiene que ser igual en todos los routers del mismo grupo VRRP:

```
Router(config-if)# vrrp group timers advertise [sec] interval
```

Configurar router virtual backup para aprender el tiempo de aviso del router master:

```
Router(config-if)# vrrp group timers learn
```

Servicios IP

ACL STANDARD

Configurar ACL. Las ACL estándar usan los números 1 a 99 y 1300 a 1999.:

```
Router(config)#access-list acl_number permit|deny IP_address  
wildcard_mask
```

Si la ACL afecta solo a un host, se puede utilizar el siguiente comando:

```
Router(config)#access-list acl_number permit|deny host IP_address
```

Aplicar ACL en la interfaz y el sentido requerido:

```
Router(config)#interface Interface-id  
Router(config-if)#ip access-group acl_number in|out
```

Verificación:

```
Router#show ip access-lists
```

ACL EXTENDED

Configurar ACL extendida.

```
Router(config)#access-list acl_number permit|deny protocol  
IP_origen      IP_destino
```

Verificación:

```
Router#show ip access-lists
```

ACL NAMED

Puede ser estándar o extendida:

```
Router(config)#ip access-list standard|extended acl_name  
Router(config)#permit|deny protocol [source source-wildcard] {any |  
host {address | name} {destination [destination-wildcard] {any | host  
{address | name} [log]
```

Verificación:

```
Router#show ip access-lists  
Router#show ip access-lists acl_name
```

NAT STATICO

Configurar manualmente el “mapa” de las direcciones IP a traducir:

```
Router(config)#ip nat inside source static [inside local ip address]
[inside global IP address]
```

Aplicar en las interfaces según corresponda:

```
Router(config)#interface Interface-id
Router(config-if)#ip nat inside
```

```
Router(config)#interface Interface-id
Router(config-if)#ip nat outside
```

Verificación:

```
Router#show ip nat translations
```

NAT DINAMICO

Primero configurar ACL estándar para definir redes internas locales a traducir:

```
Router(config)# access-list ACL_Identifier_number permit/deny
matching-      parameters
```

Definir pool de IP internas globales:

```
Router(config)#ip nat pool [Pool Name] [Start IP address] [End IP
address] netmask [Subnet mask]
```

Configurar NAT usando los parámetros definidos anteriormente:

```
Router(config)#ip nat inside source list [access list name or number]
pool [pool name]
```

Aplicar en las interfaces según corresponda:

```
Router(config)#interface Interface-id
Router(config-if)#ip nat inside
```

```
Router(config)#interface Interface-id
Router(config-if)#ip nat outside
```

Verificación:

```
Router#show ip nat translations
Router#show ip access-lists
```

NTP

Definir zona horaria:

```
Router(config)#clock timezone name time_zone
```

Definir servidor NTP:

```
Router(config)#ntp server server_IP
```

Verificación:

```
Router#show clock  
Router#show ntp status
```

DHCP

Nombre del pool de DHCP:

```
Router(config)#ip dhcp pool POOL_NAME
```

Definir red:

```
Router(dhcp-config)#network IP_address Mask
```

Definir gateway:

```
Router(dhcp-config)#default-router IP_Gateway
```

Definir dirección IP del DNS:

```
Router(dhcp-config)#dns-server IP_DNS
```

Direcciones IP excluidas del pool de DHCP:

```
Router(config)#ip dhcp excluded-address IP_address_inicio  
IP_address_fin
```

Verificación:

```
Router#show ip dhcp
```

DNS

Habilitar la traducción de host a IP (este comando viene habilitado por default):

```
Router(config)# ip domain-lookup
```

Configurar la/las direcciones IP de el o los servidores DNS:

```
Router(config)# ip name-server ip_address  
Router(config)# ip name-server ip_address
```

Verificación:

```
Router# ping
```

SYSLOG

Configurar IP del servidor:

```
Router(config)#logging host server_IP
```

Definir el tipo de logs que se enviarán al servidor:

```
Router(config)#logging trap severity_level
```

Verificación:

```
Router#debug ip protocolo
```

SSH

Configurar un hostname al router:

```
Router(config)#hostname Cisco
```

Configurar un nombre de dominio:

```
Cisco(config)#ip domain-name cisco.com
```

Crear un usuario y contraseña:

```
Cisco(config)#username ccna password cisco123
```

Generar llave RSA pública y privada:

```
Cisco(config)#crypto key generate rsa
```

Habilitar acceso por SSH:

```
Cisco(config)#line vty 0 10  
Cisco(config-line)#login local  
Cisco(config-line)#transport input ssh
```

Habilitar password de modo privilegiado:

```
Cisco(config)#enable password cisco123
```

Verificación:

```
Cisco#show ip ssh
```

Seguridad

Port security

El puerto debe estar en modo acceso.

```
Switch(config-if) # Switchport mode access
```

Activar port-security en el puerto:

```
Switch(config-if) # Switchport port-security
```

Máximo número de direcciones MAC seguras (default: 1):

```
Switch(config-if) # Switchport port-security maximum valor
```

Acción a tomar en caso de violación de seguridad:

```
Switch(config-if) # Switchport port-security violation {restrict | shutdown}
```

Verificación:

```
Switch#show port-security interface
```

DHCP snooping

Activar DHCP Snooping:

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

Seleccionar la VLAN que se desea proteger:

```
Switch(config) # ip dhcp snooping vlan vlan-id
```

Configurar el trusted port, el puerto que está directamente conectado al servidor DHCP.

```
Switch(config) # interface GigabitEthernet 0/1  
Switch(config-if) # ip dhcp snooping trust
```

Verificación:

```
Switch#show ip dhcp snooping
```

Dynamic ARP inspection

ARP inspection funciona con la base de datos de DHCP Snooping.

En el caso de que los dos Switches involucrados soporten ARP inspection y DHCP Snooping:

Activar la inspección ARP:

```
Switch(config) # ip arp inspection vlan vlan-id  
Switch(config) # interface GigabitEthernet 0/1  
Switch(config-if) # ip arp inspection trust
```

```
Switch(config-if)#end
```

Verificación:

```
Switch#show ip arp inspection vlan vlan-id  
Switch#show ip dhcp snooping binding
```

En el caso de que los dos Switches involucrados no soporten ARP inspection o DHCP Snooping:

```
Switch(config)#arp access-list access-list-name
```

Asociar manualmente la dirección IP del host a su dirección MAC y guardarla en la base de datos del Switch:

```
Switch(config-arp-nacl)#permit ip host 1.1.1.1 mac host 0001.0001.0001
```

Aplicar el filtro a la vlan-id requerida:

```
Switch(config)#ip arp inspection filter access-list-name vlan vlan-id
```

Verificación:

```
Switch#show arp access-list  
Switch#show ip arp inspection vlan 1  
Switch#show ip arp inspection statistics vlan 1
```