

Configuración básica del VMCP.

Resultados de Aprendizaje.	
RdA1	Comprender La Estructura de la red.
RdA2	Aplicar los conocimientos de interconexión de redes.
RdA3	Opera equipamiento de Capa 2 y 3.
RdA4	Aplicar los conceptos de VLAN.
RdA5	Interactuar con otras personas relacionadas al área.

INTRODUCCIÓN

VCMP son las siglas de VLAN Trunking Protocol, un protocolo usado para configurar y administrar VLANs las cuales operan en 3 modos distintos: Servidor, Cliente o Transparente.

Servidor: Debe haber al menos un Servidor. Desde él se pueden crear, eliminar o modificar VLANs.

Cliente: Desde la CLI no se pueden crear, eliminar o modificar VLANs.

Transparente: Desde él no se puede crear, eliminar o modificar VLANs (que afecten a los demás switches), las VLANs que se creen en el switch mediante CLI serán sólo locales para este switch.

Los administradores cambian la configuración de las VLANs en el switch en modo servidor, después de que se realiza algún cambio, estos son distribuidos a todos los demás dispositivos en el dominio VCMP a través de los enlaces que permiten el Trunk. Los dispositivos que operan en modo transparente no aplican las configuraciones VLAN que reciben, ni envían las suyas a otros dispositivos.

El VCMP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El VCMP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN, denominada vlan.dat.

PROCEDIMIENTO:

En esta actividad, se efectuarán las configuraciones básicas del switch, se configurará el VCMP, se establecerán los enlaces troncales, se aprenderá sobre los modos de VCMP, se creará y distribuirá información VLAN y se asignarán puertos a la VLAN. La red inicial se abre en un estado seguro con todos los puertos desactivados administrativamente.

Diagrama de topología

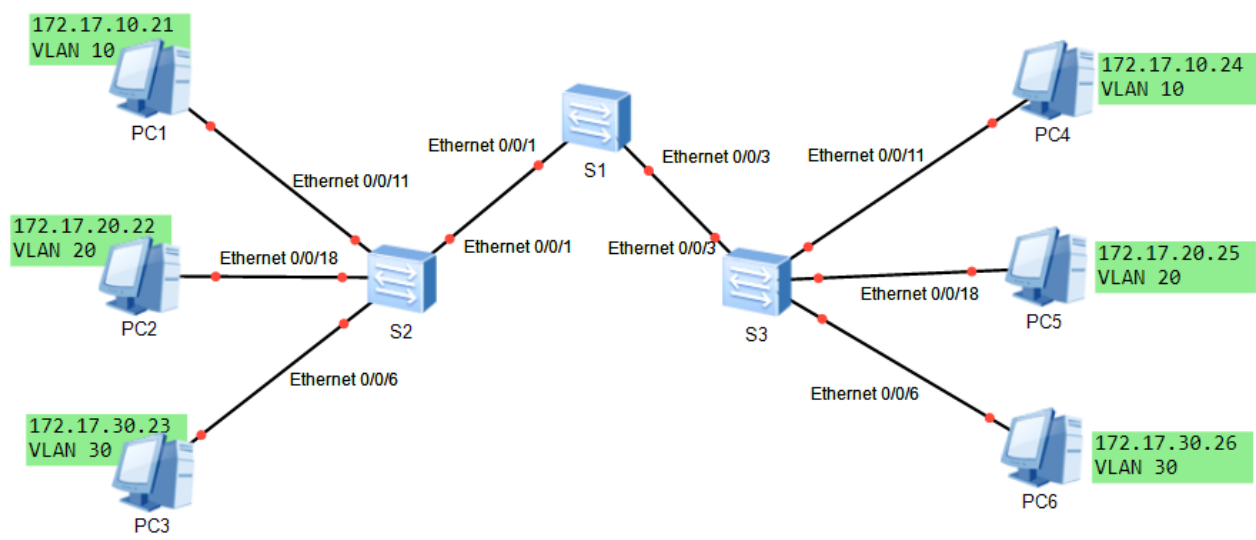


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de enlace) predeterminada
S1	VLAN 99	172.17.99.11	255.255.255.0	No aplicable
S2	VLAN 99	172.17.99.12	255.255.255.0	No aplicable
S3	VLAN 99	172.17.99.13	255.255.255.0	No aplicable
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

Asignación de puertos (S1 y S2).

Puertos	Asignaciones	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN nativa 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Invitados	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Facultad	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Estudiantes	172.17.20.0 /24

Realizar configuración básica.

Configure los switches S1, S2 y S3 según las siguientes pautas y guarde todas las configuraciones:

- Configure el nombre de host del switch, según se indica en la topología.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de class en el Modo EXEC.
- Configure una contraseña de cisco para las conexiones de consola.
- Configure una contraseña de cisco para las conexiones vty.

Configurar las interfaces Ethernet en los equipos PC host.

Configure las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 y PC6 con las direcciones IP y las gateways por defecto indicadas en la tabla de direccionamiento.

Configurar VTP y seguridad en los switches.

Habilitar los puertos del usuario en S2 y S3.

Configure los puertos del usuario en el modo de acceso. Consulte el diagrama de topología para determinar los puertos que están conectados a los dispositivos del usuario final.

```
[S2]interface Ethernet 0/0/6
[S2 interface Ethernet0/0/6]port link-type access
[S2 interface Ethernet0/0/6]port default vlan 30
[S2 interface Ethernet0/0/6]quit
```

```
[S2]interface Ethernet 0/0/11
[S2 interface Ethernet0/0/11]port link-type access
[S2 interface Ethernet0/0/11]port default vlan 10
[S2 interface Ethernet0/0/11]quit
```

```
[S2]interface Ethernet 0/0/18
[S2 interface Ethernet0/0/18]port link-type access
[S2 interface Ethernet0/0/18]port default vlan 20
[S2 interface Ethernet0/0/18]quit
```

Comprobar la configuración VCMP actual en los tres switches..

Con la ayuda de la siguiente tabla que compara con VTP de CISCO.

Table 4-9 Differences in command formats

Function	Command on Huawei Switches	Command on Cisco Switches	Description
----------	----------------------------	---------------------------	-------------

Configure the device role or mode.	vcmp role { client server silent transparent }	vtp mode { client off server transparent }	A switch used as a VCMP silent in a Huawei VCMP domain is similar to the switch in off mode in a Cisco VTP domain, and directly discards received protocol packets.
Configure the domain name.	vcmp domain <i>domain-name</i>	vtp domain <i>domain-name</i>	-
Configure the domain ID.	vcmp device-id <i>device-id</i>	Not supported	Cisco VTP does not support the configuration.
Configure an authentication password for the domain.	vcmp authentication sha2-256 password <i>password</i>	vtp password <i>password</i>	-
Configuring the protocol version number.	Not supported	vtp version <i>number</i>	Huawei VCMP does not support the configuration.
Check the protocol status.	display vcmp status	show vtp status	-

3.3. Configurar el modo de funcionamiento, el nombre de dominio y la contraseña de VTP en los tres switches.

Establezca el nombre de dominio de VTP en Lab4 y la contraseña de VTP en cisco en los tres switches. Configure S1 en el modo de servidor, S2 en el modo cliente y S3 en el modo transparente.

[S1]**vcmp role server**

[S1]**vcmp domain** Lab4

[S1]**vcmp authentication sha2-256 password** huawei

[S2]**vcmp role client**

[S2]**vcmp domain** Lab4

```
[S2]vcmp authentication sha2-256 password huawei
```

```
[S3]vcmp role transparent
```

```
[S3]vcmp domain Lab4
```

```
[S3]vcmp authentication sha2-256 password huawei
```

Configurar enlaces troncales

Los enlaces troncales son conexiones entre los switches que permiten que los switches intercambian información para todas las VLAN. Por defecto, un puerto de enlace troncal pertenece a todas las VLAN, a diferencia de un puerto de acceso, que sólo puede pertenecer a una única VLAN. Si el switch admite encapsulación de VLAN ISL y 802.1Q, los enlaces troncales deben especificar el método que se usa.

Configurar S1 Eth 0/0/1 y Eth 0/0/3 para enlaces troncales y para usar VLAN 99 como la VLAN nativa.

```
[S1]interface Ethernet 0/0/1
```

```
[S1-interface Ethernet0/0/1]port link-type trunk
```

```
[S1-interface Ethernet0/0/1]port trunk allow-pass vlan 99
```

```
[S1-interface Ethernet0/0/1]quit
```

```
[S1]interface Ethernet 0/0/3
```

```
[S1-interface Ethernet0/0/3]port link-type trunk
```

```
[S1-interface Ethernet0/0/3]port trunk allow-pass vlan 99
```

```
[S1-interface Ethernet0/0/3]quit
```

Verificar que los enlaces troncales estén habilitados en S2 y configurar VLAN 99 como la VLAN nativa.

```
<S2> display interface Ethernet 0/0/1
```

Como práctica recomendada, el modo administrativo de la interfaz de enlaces troncales se debe configurar en modo de enlace troncal. De este modo, se garantiza que la interfaz estará configurada de manera estática como un puerto de enlace troncal y nunca negociará un modo diferente.

```
[S1]interface Ethernet 0/0/1
```

```
[S1-interface Ethernet0/0/1]port link-type trunk
```

```
[S1-interface Ethernet0/0/1]port trunk allow-pass vlan 99
```

```
[S1-interface Ethernet0/0/1]quit
```

Verificar que los enlaces troncales estén habilitados en S3 y configurar VLAN 99 como la VLAN nativa.

5. Configurar la seguridad del puerto en los switches de la capa de acceso S2 y S3.

Configure los puertos fa0/6, fa0/11 y fa0/18 de modo que permitan sólo un host y obtengan la dirección MAC del host dinámicamente.

```

[S2]interface Ethernet 0/0/6
[S2-interface Ethernet0/0/6]port-security enable
[S2-interface Ethernet0/0/6]port-security mac-address sticky
[S2-interface Ethernet0/0/6]port-security max-mac-num 1
[S2]interface Ethernet 0/0/11
[S2-interface Ethernet0/0/11]port-security enable
[S2-interface Ethernet0/0/11]port-security mac-address sticky
[S2-interface Ethernet0/0/11]port-security max-mac-num 1
[S2]interface Ethernet 0/0/18
[S2-interface Ethernet0/0/18]port-security enable
[S2-interface Ethernet0/0/18]port-security mac-address sticky
[S2-interface Ethernet0/0/18]port-security max-mac-num 1

```

```

[S3]interface Ethernet 0/0/6
[S3-interface Ethernet0/0/6]port-security enable
[S3-interface Ethernet0/0/6]port-security mac-address sticky
[S3-interface Ethernet0/0/6]port-security max-mac-num 1
[S3]interface Ethernet 0/0/11
[S3-interface Ethernet0/0/11]port-security enable
[S3-interface Ethernet0/0/11]port-security mac-address sticky
[S3-interface Ethernet0/0/11]port-security max-mac-num 1
[S3]interface Ethernet 0/0/18
[S3-interface Ethernet0/0/18]port-security enable
[S3-interface Ethernet0/0/18]port-security mac-address sticky
[S3-interface Ethernet0/0/18]port-security max-mac-num 1

```

6. Configurar las VLAN en el servidor VCMF. En esta práctica de laboratorio se requieren cuatro VLAN:

- VLAN 99 (Administración)
- VLAN 10 (Facultad)
- VLAN 20 (Estudiantes)
- VLAN 30 (Invitados)

Verificar si las vlans creadas se encuentran en los switches 2 y 3.

COMENTARIOS

_____A continuación exprese sus dificultades, problemas o percepción general con respecto a la guía.
