SOP-NET-003_Cisco_VLAN_v1.0.0

SOP-NET-003_Cisco_VLAN_v1.0.0

SOP-NET-003: Cisco Device VLAN Configuration

1.0 Document Control

ID	SOP-NET-003
Version	1.1
Status	Final
Author	OberaConnect IT
Date	2025-12-02
Approved By	

2.0 Purpose

To define the standard procedure for configuring, verifying, and managing Virtual Local Area Networks (VLANs) on Cisco switches to ensure network segmentation and security.

3.0 Scope

This SOP applies to all network administration personnel responsible for configuring and managing Cisco network infrastructure within the organization.

4.0 Prerequisites

- **Access:** Administrative access to the target Cisco switch via console cable or SSH.
- **Credentials:** Valid username and password with privileges to make configuration changes.
- **Network Knowledge:** Understanding of the network design, including required VLAN IDs, names, and port assignments.

5.0 Procedure

5.1 Access the Switch

1. Connect to the switch using your preferred method (console or SSH). `bash ssh admin@<switch-ip-address>`
2. Enter your credentials when prompted.

5.2 Enter Global Configuration Mode

1. Enter privileged EXEC mode. `enable`
2. Enter global configuration mode. `configure terminal`

5.2.1 Configure VTP Mode (CRITICAL)

> **IMPORTANT:** Always set VTP mode to prevent unintended VLAN propagation across the network.

1. Set VTP mode to transparent (recommended for most deployments):

```
    vtp mode transparent
    ```

Or disable VTP entirely (Cisco IOS 15.x+):

vtp mode off
```
```

VTP Mode Options:

Mode	Description	Use Case
`transparent`	Does not participate in VTP but passes VTP messages	Recommended default
`off`	Completely disables VTP	Highest security
`server`	Can create/modify VLANs, propagates to clients	Only in controlled environments
`client`	Receives VLAN info from servers	Legacy deployments

> **WARNING:** Using `server` or `client` mode in an uncontrolled environment can cause VLAN database overwrites if a switch with a higher revision number is connected.

5.3 Create and Name VLANs

1. Create a new VLAN and enter the VLAN configuration sub-mode.

   ~~~
       vlan <VLAN_ID>
       ```

   *Example:*

   vlan 10
   ```
   ~~~

2. Assign a descriptive name to the VLAN.

   ~~~
       name <VLAN_Name>
       ```

   *Example:*

   name VLAN_SALES
   ```
   ~~~

3. Exit the VLAN configuration sub-mode. `exit`

4. Repeat steps 5.3.1 - 5.3.3 for each required VLAN. *Example:* `vlan 20 name VLAN_HR exit`

5.4 Assign Access Ports to VLANs

1. Select the interface or range of interfaces to configure.

   ~~~
       interface range <interface_type> <port_range>
       ```

   *Example:*

   interface range fastEthernet 0/1 - 12
   ```
   ~~~

2. Set the port mode to `access`. `switchport mode access`

3. Assign the port to the desired VLAN.

   ~~~
       switchport access vlan <VLAN_ID>
       ```

   *Example:*

   switchport access vlan 10
   ```
   ~~~

4. **Enable Spanning-Tree PortFast** (allows immediate port activation for end devices): `spanning-tree portfast`

5. **Enable BPDU Guard** (protects against rogue switches): `spanning-tree bpduguard enable`

6. Exit the interface configuration sub-mode. `exit`

Complete Access Port Configuration Example:

```
interface range gigabitEthernet 0/1 - 24
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
 exit
```

> **NOTE:** PortFast and BPDU Guard should ONLY be enabled on access ports connected to end devices (PCs, printers, phones). Never enable on ports connecting to other switches.

5.5 Configure Trunk Ports (If Required) *This step is necessary when connecting to another switch or a device that needs to handle traffic from multiple VLANs.*

1. Select the interface to configure as a trunk.

   ~~~
       interface <interface_type> <port>
       ```
   *Example:*

   interface gigabitEthernet 0/1
   ```
   ~~~

2. Set the port mode to `trunk`. `switchport mode trunk`
3. **Disable DTP negotiation** (security best practice): `switchport nonegotiate`
4. **Change native VLAN from default** (security - prevents VLAN hopping attacks):

   ~~~
       switchport trunk native vlan <unused_vlan_id>
       ```
   *Example (use an unused VLAN like 999):*

   switchport trunk native vlan 999
   ```
   ~~~

5. Specify which VLANs are allowed on the trunk (always limit to required VLANs):

   ~~~
       switchport trunk allowed vlan <vlan_list>
       ```
   *Example:*

   switchport trunk allowed vlan 10,20,30
   ```
   ~~~

6. Exit the interface configuration sub-mode. `exit`

Complete Trunk Port Configuration Example:

```
interface gigabitEthernet 0/48
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30
 exit
```

> **SECURITY NOTE:** - `nonegotiate` prevents DTP attacks where an attacker could negotiate a trunk - Changing native VLAN from 1 prevents VLAN hopping attacks - Always limit allowed VLANs to only those required

5.6 Configure Management VLAN and IP Address Set up switch management access via a dedicated VLAN.

1. Create a management VLAN (if not already created): `vlan 99 name MGMT exit`
2. Configure the Switch Virtual Interface (SVI) for management: `interface vlan 99 ip address 10.0.99.10 255.255.255.0 no shutdown exit`
3. Set the default gateway: `ip default-gateway 10.0.99.1`
4. Restrict management access to specific VLANs (optional but recommended):

   ```
   line vty 0 15
   access-class MGMT-ACCESS in
   exit

   ip access-list standard MGMT-ACCESS
   permit 10.0.99.0 0.0.0.255
   deny any
   exit
   ```

   > **NOTE:** Using a dedicated management VLAN (not VLAN 1) is a security best practice. Management traffic should be isolated from user traffic.

6.0 Verification

Use the following commands from privileged EXEC mode to verify the configuration.

1. **Display VLAN Information:**
   - Check that VLANs are created and ports are assigned correctly.

```
show vlan brief
```

2. **Display Trunk Port Information:**
   - Verify that trunk ports are active and allowing the correct VLANs.

```
show interfaces trunk
```

7.0 Save Configuration

To ensure the configuration persists after a device reboot, save the running configuration to the startup configuration.

1. From privileged EXEC mode, execute one of the following commands:

~~~
    write memory
    ```
~~~

````
*or*
````

~~~
copy running-config startup-config
```
~~~

2. Confirm the save when prompted.

8.0 Contingency/Rollback

- **To remove a VLAN:**

```
configure terminal
no vlan <VLAN_ID>
exit
```

- **To reset a port to its default state:**

```
configure terminal
default interface <interface_type> <port>
exit
```

- **To revert all changes:** If changes have not been saved, reboot the switch without saving the configuration.

8.1 Troubleshooting

Issue	Cause	Resolution
VLAN not showing in `show vlan brief`	VLAN not created or VTP client mode	Create VLAN manually. Check VTP mode (`show vtp status`). Set to transparent if needed.
Port not in correct VLAN	Access VLAN not set or port in trunk mode	Verify with `show interface switchport`. Set `switchport mode access` and `switchport access vlan X`.
Trunk not passing VLANs	VLANs not allowed on trunk	Check `show interface trunk`. Add VLANs with `switchport trunk allowed vlan add X`.
Devices can't communicate across VLANs	No inter-VLAN routing	Requires Layer 3 switch with SVIs or external router. Configure routing between VLANs.
STP blocking port unexpectedly	Loop detected or BPDU received on portfast port	Check `show spanning-tree`. If BPDU guard triggered, remove unauthorized switch and `shut`/`no shut` port.
Native VLAN mismatch	Different native VLANs on trunk ends	Verify native VLAN matches on both ends (`show interface trunk`). Set same native VLAN.
VTP not syncing VLANs	VTP domain mismatch or password	Check `show vtp status`. Ensure domain name and password match. Consider transparent mode.
Cannot access switch management	Wrong VLAN or no IP on SVI	Verify management VLAN SVI has IP (`show ip interface brief`). Check default gateway.
Port err-disabled	Security violation, BPDU guard, or port security	Check `show interface status err-disabled`. Fix cause, then `shut` / `no shut`.
Slow network performance	Spanning-tree convergence or duplex mismatch	Check `show spanning-tree` for blocking ports. Verify duplex/speed with `show interface status`.

Diagnostic Commands:

```
! View all VLANs
show vlan brief

! Check port VLAN assignment
show interface <interface> switchport

! View trunk status
```

```
show interface trunk

! Check spanning-tree
show spanning-tree vlan <vlan_id>

! View VTP status
show vtp status

! Check interface errors
show interface <interface> | include errors|CRC|collision

! View MAC address table
show mac address-table vlan <vlan_id>
```

9.0 Revision History

Version	Date	Author	Description
1.0	2025-12-02	OberaConnect IT	Initial document creation from source.
1.1	2025-12-29	Jeremy Smith	SME Review: Added VTP mode configuration (5.2.1). Added Spanning-Tree PortFast and BPDU Guard for access ports. Added trunk security (nonegotiate, native VLAN change). Added Management VLAN section (5.6). Added Section 8.1 (Troubleshooting) with common issues and diagnostic commands.