Configuring Wired Dynamic PVLAN

The following sections provide information about configuring wired dynamic PVLAN:

- Restrictions for Wired Dynamic PVLAN, on page 1
- Information About Wired Dynamic PVLAN, on page 1
- Configuring Wired Dynamic PVLAN, on page 3
- Feature History for Wired Dynamic PVLAN, on page 6

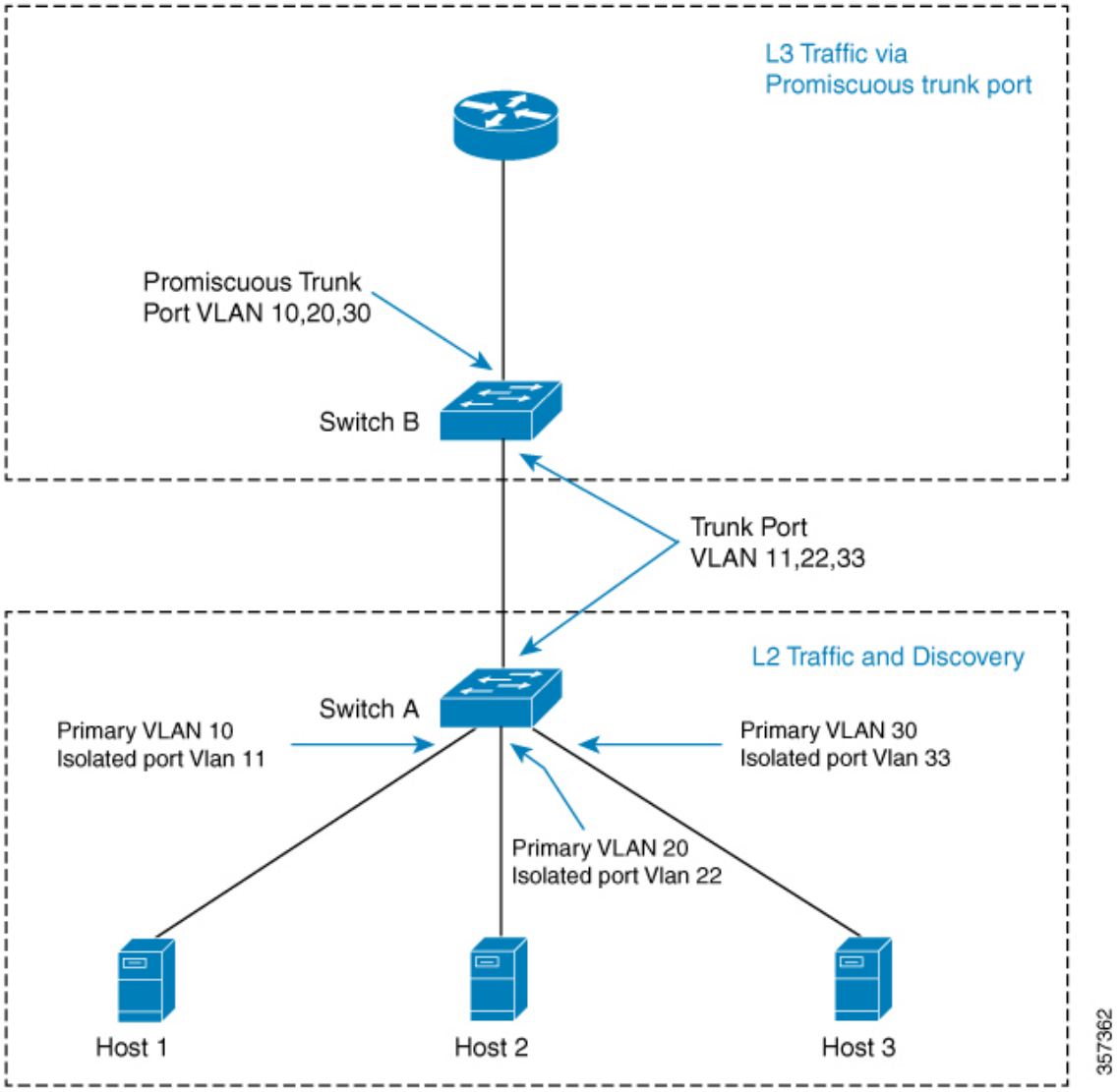
Restrictions for Wired Dynamic PVLAN

- High availability is not supported with Wired Dynamic PVLAN.
- Voice VLAN configuration cannot co-exist with this feature.
- Local Web Authentication (LWA) and Central Web Authentication (CWA) cannot be used with this feature.
- All wired clients using the dynamic PVLAN interface template will be programmed as data clients.
- Only interfaces with existing Access or PVLAN Host switchport mode support PVLAN template.
- Identity Based Networking Services 2.0 (IBNS 2.0) must be used for dynamic template support.

Information About Wired Dynamic PVLAN

Wired Dynamic PVLAN is a feature that uses a private VLAN with AAA authorization to isolate clients and provide Zero-Trust. It is a method to block peer to peer communications within a subnet/VLAN. Here, the client is assigned to a PVLAN which isolates a wired client connected on one port from all other ports on Layer 2 while the Layer 3 communication occurs via the promiscuous port. In this feature, a single wired data client is supported per port interface, to ensure point-to-point blocking.

Note Traffic from multiple clients on the same interface will not be blocked.



In this topology, the hosts are connected to Switch A and they can communicate only with the promiscuous trunk port on the switch. The PVLAN can be extended to span across multiple switches by adding intermediate switches. If there is a switch (Switch C) between Switch A and Switch B in the above topology, then layer 2 trunk ports need to be configured on the intermediate links. If case of a community VLAN, it allows packets to be seen on other hosts within the same community VLAN.

When a host is connected to a switch port with a cable, it is placed into an Isolated PVLAN where it cannot discover any other hosts. The host is then authenticated by the RADIUS server. Another scenario is when the port is placed in closed mode, and if the port is not authenticated, only Extensible Authentication Protocol over LAN (EAPoL) packets are allowed. Once the port is authenticated it is placed into an Isolated VLAN dynamically. As the host first authenticates with the RADIUS server, it sends the name of a dynamic interface template to be applied to the host's port. This interface template contains the configurations to enable the PVLAN Primary and Secondary VLANs on the port. With the template applied to the host, the switchport mode will be changed which will cause the port to flap from access mode to PVLAN mode.

Note The interface template with the same name as referred by AAA Authorization needs to be configured on the switch.

When the interface template is being applied, the port will physically go down for a time period set by the sticky timer and come up again. When the RADIUS server sends the interface template a second time, it is ignored as the conversion has been completed. The port is then assigned to a PVLAN which keeps it isolated. The host completes authorization and comes up to ready state.

Configure the keep time for which the interface template information is retained before it is removed from the port using the **access-session interface-template sticky timer** *time* command.

Configuring Wired Dynamic PVLAN

To configure Wired Dynamic PVLAN, perform these steps on the user device (Switch A in the above topology):

Before you begin

Ensure that the dot1x aaa is configured on the user device.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vlan** *vlan-id* **Example:** `Device(config)# vlan 200`	(Optional) Enters VLAN configuration mode and designates or creates a VLAN that will be an isolated VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.
Step 4	**private-vlan isolated** **Example:** `Device(config-vlan)# private-vlan isolated`	Designates the VLAN as an isolated VLAN.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-vlan)# exit`	Returns to global configuration mode.
Step 6	**vlan** *vlan-id* **Example:** `Device(config)# vlan 100`	Enters VLAN configuration mode and designates or creates a VLAN that will be the primary VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.
Step 7	**private-vlan primary** **Example:** `Device(config-vlan)# private-vlan primary`	Designates the VLAN as the primary VLAN.
Step 8	**private-vlan association** [**add** | **remove**] *secondary_vlan_list* **Example:** `Device(config-vlan)# private-vlan association 200`	Associates the secondary VLANs with the primary VLAN. It can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs. • The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs. • The *secondary_vlan_list* parameter can contain multiple community VLAN IDs but only one isolated VLAN ID. • Enter a *secondary_vlan_list*, or use the **add** keyword with a *secondary_vlan_list* to associate secondary VLANs with a primary VLAN. • Use the **remove** keyword with a *secondary_vlan_list* to clear the association between secondary VLANs and a primary VLAN. • The command does not take effect until you exit VLAN configuration mode.
Step 9	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-vlan)# exit`	
Step 10	**template** *template-name* **Example:** `Device(config)# template PVLAN100_200_CFG`	Creates a user template and enters template configuration mode.
Step 11	**switchport mode private-vlan host** **Example:** `Device(config-template)# switchport mode private-vlan host`	Configures a Layer 2 port as a PVLAN host port on the template.
Step 12	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id* **Example:** `Device(config-template)# switchport private-vlan host-association 100 200`	Configures the association of a Layer 2 port with a PVLAN on the template.
Step 13	**exit** **Example:** `Device(config-template)# exit`	Returns to global configuration mode.
Step 14	**access-session interface-template sticky timer** *time* **Example:** `Device(config)# access-session interface-template sticky timer 60`	Configures the keep time of the template globally. Once the last client leaves, the template will be removed from the port after the configured keep time. **Note** It is recommended that you set the sticky timer to 60 seconds.
Step 15	**interface** *interface-id* **Example:** `Device(config)# interface GigabitEthernet1/0/1`	Enters interface configuration mode and specifies the interface.
Step 16	**access-session interface-template sticky timer** *time* **Example:**	Configures the keep time of the template on the interface. Once the last client leaves, the template will be removed from the port after the configured keep time.

	Command or Action	Purpose
	`Device(config-if)# access-session interface-template sticky timer 60`	**Note** It is recommended that you set the sticky timer to 60 seconds.
Step 17	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

What to do next

After the above steps, configure the Identity Services Engine (ISE) or any other RADIUS server to assign the template to the client's port interface after the client has been authenticated successfully.

Figure 1: Configuring the ISE to Assign the Interface Template

If you are using the ISE, go to the **Policy** > **Policy Elements** > **Authorization** > **Authorization Profile** page. Check the **Interface Template** check box and enter the name of the template to be assigned to the client interface.

If you are using a different RADIUS server, the attribute **Cisco-AVpair="interface:template=name"** must be pushed to the switch after the initial client authentication has been completed.

Feature History for Wired Dynamic PVLAN

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.5.1	Wired Dynamic PVLAN (Whitelist P2P Blocking)	Wired Dynamic PVLAN feature uses a private VLAN to isolate the clients and provide Zero-Trust. This methods blocks peer to peer communication within a subnet/VLAN. The client is assigned to a PVLAN which isolates a single wired client connected on a port from other ports.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.