Configure VLAN Trunking

Feature History for VLAN Trunks

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 Name and Description	Supported Platform
VLAN Trunks	A trunk is a point-to-point link between one or more Ethernet interfaces and another networking device such as a router or a controller. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Release	Feature Name and Description	Supported Platform
Dynamic Trunking Protocol (DTP)	Dynamic Trunking Protocol (DTP) is a Cisco proprietary Layer 2 protocol. It operates between Cisco switches to negotiate the formation of a trunk link. A trunk link is a point-to-point connection that carries traffic for multiple Virtual Local Area Networks (VLANs).	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

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

Information About VLAN Trunks

The following sections provide information about VLAN Trunks:

Trunking Overview

A trunk is a point-to-point link between one or more Ethernet interfaces and another networking device such as a router or a controller. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

IEEE 802.1Q— Industry-standard trunking encapsulation is available on all Ethernet interfaces.

Trunking Modes

Ethernet trunk interfaces support different trunking modes. You can set an interface as trunking or nontrunking or to negotiate trunking with the neighboring interface. To autonegotiate trunking, the interfaces must be in the same VTP domain.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Point-to-Point Protocol (PPP). However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.

Layer 2 Interface Modes

Table 1: Layer 2 Interface Modes

Mode	Function
switchport mode access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface.
switchport mode dynamic auto	Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk** or **desirable** mode. The default switchport mode for all Ethernet interfaces is **dynamic auto**.
switchport mode dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.
switchport nonegotiate	Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.
switchport mode private-vlan	Configures the private VLAN mode.

Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk.

To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), DTP, and VTP in VLAN 1.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port will be added to VLAN 1, regardless of the **switchport trunk allowed** setting. The same is true for any VLAN that has been disabled on the port.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

Load Sharing on Trunk Ports

Load sharing divides the bandwidth supplied by parallel trunks connecting devices. To avoid loops, STP normally blocks all but one parallel link between the devices. Using load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same device. For load sharing using STP path costs, each load-sharing link can be connected to the same device or to two different devices.

Network Load Sharing Using STP Priorities

When two ports on the same device form a loop, the device uses the STP port priority to decide which port is enabled and which port is in a blocking state. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

Network Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs, blocking different ports for different VLANs. The VLANs keep the traffic separate and maintain redundancy in the event of a lost link.

Feature Interactions

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the device propagates the setting that you entered to all ports in the group:
  - Allowed-VLAN list.
  - STP port priority for each VLAN.
  - STP Port Fast setting.
  - Trunk status:

    If one port in a port group ceases to be a trunk, all ports cease to be trunks.
- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, the port mode is not changed.

Prerequisites for VLAN Trunks

The IEEE 802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco devices connected through IEEE 802.1Q trunks, the devices maintain one spanning-tree instance for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco device to a non-Cisco device through an IEEE 802.1Q trunk, the Cisco device combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco IEEE 802.1Q device. However, spanning-tree information for each VLAN is maintained by Cisco devices separated by a cloud of non-Cisco IEEE 802.1Q devices. The non-Cisco IEEE 802.1Q cloud separating the Cisco device is treated as a single trunk link between the devices.

- Make sure the native VLAN for an IEEE 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.

- Disabling spanning tree on the native VLAN of an IEEE 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an IEEE 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure your network is loop-free before disabling spanning tree.

Restrictions for VLAN Trunks

The following are restrictions for VLAN trunks:

- A trunk port cannot be a secure port.

- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the device propagates the setting that you entered to all ports in the group:

  - Allowed-VLAN list.
  - STP port priority for each VLAN.
  - STP Port Fast setting.
  - Trunk status:

    If one port in a port group ceases to be a trunk, all ports cease to be trunks.

- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.

- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, the port mode is not changed.

- Dynamic Trunking Protocol (DTP) is not supported on tunnel ports.

- When native VLAN and management VLAN is configured with the same VLAN ID and a new VLAN is added as trunk port, both the new VLAN and native VLAN shifts between active and suspend state for a duration of 15 seconds. This duration is the time taken for STP to resolve all inconsistencies.

How to Configure VLAN Trunks

To avoid trunking misconfigurations, configure interfaces connected to devices that do not support DTP to not forward DTP frames, that is, to turn off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Configuring an Ethernet Interface as a Trunk Port

This section provides information about configuring an Ethernet Interface as a trunk port:

Configuring a Trunk Port

Because trunk ports send and receive VTP advertisements, to use VTP you must ensure that at least one trunk port is configured on the device and that this trunk port is connected to the trunk port of a second device. Otherwise, the device cannot receive any VTP advertisements.

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	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/2`	Specifies the port to be configured for trunking, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**} **Example:** `Device(config-if)# switchport mode dynamic desirable`	Configures the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or tunnel port or to specify the trunking mode). • **dynamic auto**—Sets the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. This is the default. • **dynamic desirable**—Sets the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode. • **trunk**—Sets the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
Step 5	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 200`	(Optional) Specifies the default VLAN, which is used if the interface stops trunking.
Step 6	**switchport trunk native vlan** *vlan-id* **Example:** `Device(config-if)# switchport trunk native vlan 200`	Specifies the native VLAN for IEEE 802.1Q trunks.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 8	**show interfaces** *interface-id* **switchport** **Example:** `Device# show interfaces gigabitethernet 1/0/2 switchport`	Displays the switch port configuration of the interface in the *Administrative Mode* and the *Administrative Trunking Encapsulation* fields of the display.
Step 9	**show interfaces** *interface-id* **trunk** **Example:**	Displays the trunk configuration of the interface.

	Command or Action	Purpose
	`Device# show interfaces gigabitethernet 1/0/2 trunk`	
Step 10	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Defining the Allowed VLANs on a Trunk

VLAN 1 is the default VLAN on all trunk ports in all Cisco devices, and it has previously been a requirement that VLAN 1 always be enabled on every trunk link. You can use the VLAN 1 minimization feature to disable VLAN 1 on any individual VLAN trunk link so that no user traffic (including spanning-tree advertisements) is sent or received on VLAN 1.

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	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Specifies the port to be configured, and enters interface configuration mode.
Step 4	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the interface as a VLAN trunk port.

	Command or Action	Purpose
Step 5	**switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list* **Example:** `Device(config-if)# switchport trunk allowed vlan remove 2`	(Optional) Configures the list of VLANs allowed on the trunk. The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport** **Example:** `Device# show interfaces gigabitethernet 1/0/1 switchport`	Verifies your entries in the *Trunking VLANs Enabled* field of the display.
Step 8	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect.

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet0/1`	Selects the trunk port for which VLANs should be pruned, and enters interface configuration mode.
Step 4	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan* [,*vlan* [,,,]]	Configures the list of VLANs allowed to be pruned from the trunk. For explanations about using the **add**, **except**, **none**, and **remove** keywords, see the command reference for this release. Separate non-consecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are 2 to 1001. Extended-range VLANs (VLAN IDs 1006 to 4094) cannot be pruned. VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport** **Example:** `Device# show interfaces gigabitethernet 1/0/1 switchport`	Verifies your entries in the *Pruning VLANs Enabled* field of the display.
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the device forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

The native VLAN can be assigned any VLAN ID.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the device sends the packet with a tag.

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	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/2`	Defines the interface that is configured as the IEEE 802.1Q trunk, and enters interface configuration mode.
Step 4	**switchport trunk native vlan** *vlan-id* **Example:** `Device(config-if)# switchport trunk native vlan 12`	Configures the VLAN that is sending and receiving untagged traffic on the trunk port. For *vlan-id*, the range is 1 to 4094.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport** **Example:** `Device# show interfaces gigabitethernet`	Verifies your entries in the *Trunking Native Mode VLAN* field.

	Command or Action	Purpose
	`1/0/2 switchport`	
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Trunk Ports for Load Sharing

The following sections provide information about configuring trunk ports for load sharing:

Configuring Load Sharing Using STP Port Priorities

If your switch is a member of a switch stack, you must use the **spanning-tree** [**vlan** *vlan-id*] **cost** *cost* interface configuration command instead of the **spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority* interface configuration command to select an interface to put in the forwarding state. Assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last.

These steps describe how to configure a network with load sharing using STP port priorities.

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 on Device A.
Step 3	**vtp domain** *domain-name* **Example:** `Device(config)# vtp domain workdomain`	Configures a VTP administrative domain. The domain name can be 1 to 32 characters.
Step 4	**vtp mode server** **Example:**	Configures Device A as the VTP server.

	Command or Action	Purpose
	`Device(config)# vtp mode server`	
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**show vtp status** **Example:** `Device# show vtp status`	Verifies the VTP configuration on both Device A and Device B. In the display, check the *VTP Operating Mode* and the *VTP Domain Name* fields.
Step 7	**show vlan** **Example:** `Device# show vlan`	Verifies that the VLANs exist in the database on Device A.
Step 8	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 9	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet1/0/1`	Defines the interface to be configured as a trunk, and enters interface configuration mode.
Step 10	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the port as a trunk port.
Step 11	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 12	**show interfaces** *interface-id* **switchport** **Example:**	Verifies the VLAN configuration.

	Command or Action	Purpose
	`Device# show interfaces gigabitethernet 1/0/1 switchport`	
Step 13	Repeat the above steps on Device A for a second port in the device.	
Step 14	Repeat the above steps on Device B to configure the trunk ports that connect to the trunk ports configured on Device A.	
Step 15	**show vlan** **Example:** `Device# show vlan`	When the trunk links come up, VTP passes the VTP and VLAN information to Device B. This command verifies that Device B has learned the VLAN configuration.
Step 16	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode on Device A.
Step 17	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Defines the interface to set the STP port priority, and enters interface configuration mode.
Step 18	**spanning-tree vlan** *vlan-range* **port-priority** *priority-value* **Example:** `Device(config-if)# spanning-tree vlan 8-10 port-priority 16`	Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.
Step 19	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 20	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/2`	Defines the interface to set the STP port priority, and enters interface configuration mode.

	Command or Action	Purpose
Step 21	**spanning-tree vlan** *vlan-range* **port-priority** *priority-value* **Example:** `Device(config-if)# spanning-tree vlan 3-6 port-priority 16`	Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.
Step 22	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 23	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 24	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Load Sharing Using STP Path Cost

These steps describe how to configure a network with load sharing using STP path costs.

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 on Device A.

	Command or Action	Purpose
Step 3	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Defines the interface to be configured as a trunk, and enters interface configuration mode.
Step 4	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the port as a trunk port.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 6	Repeat Steps 2 through 4 on a second interface in Device A or in Device A stack.	
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Device# show running-config`	Verifies your entries. In the display, make sure that the interfaces are configured as trunk ports.
Step 9	**show vlan** **Example:** `Device# show vlan`	When the trunk links come up, Device A receives the VTP information from the other devices. This command verifies that Device A has learned the VLAN configuration.
Step 10	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 11	**interface** *interface-id* **Example:**	Defines the interface on which to set the STP cost, and enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface gigabitethernet 1/0/1`	
Step 12	**spanning-tree vlan** *vlan-range* **cost** *cost-value* **Example:** `Device(config-if)# spanning-tree vlan 2-4 cost 30`	Sets the spanning-tree path cost to 30 for VLANs 2 through 4.
Step 13	**end** **Example:** `Device(config-if)# end`	Returns to global configuration mode.
Step 14	Repeat Steps 9 through 13 on the other configured trunk interface on Device A, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.	
Step 15	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 16	**show running-config** **Example:** `Device# show running-config`	Verifies your entries. In the display, verify that the path costs are set correctly for both trunk interfaces.
Step 17	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Dynamic Trunking Protocol

Dynamic Trunking Protocol (DTP) is a Cisco proprietary Layer 2 protocol. It operates between Cisco switches to negotiate the formation of a trunk link. A trunk link is a point-to-point connection that carries traffic for multiple Virtual Local Area Networks (VLANs). DTP automates the process of configuring trunk ports. This automation allows switches to dynamically agree on whether a link should operate as an access port (carrying traffic for a single VLAN) or a trunk port.

DTP simplifies switch administration. It removes the need for you to manually configure trunking on each port. When DTP is enabled on a port, it sends DTP frames to the connected device. These frames advertise the port's trunking capabilities and negotiate the link's operational mode.

Limitations and restrictions of DTP

- Cisco proprietary: DTP is a Cisco-specific protocol. It does not function with non-Cisco switches. If you connect a Cisco switch port configured for DTP to a non-Cisco switch, the link typically defaults to an access port. Trunking will not establish in this scenario. To establish a trunk with non-Cisco devices, manually configure both ends as trunk.
- Security risk: DTP can pose a security risk. By default, many Cisco switch ports are configured in a DTP mode that attempts to form a trunk (dynamic auto or dynamic desirable). An attacker can connect a device to such a port. By sending DTP frames, the attacker can force the port into trunking mode. This action grants access to multiple VLANs and potentially sensitive network traffic.
- Misconfiguration potential: If you do not manage DTP carefully, it can lead to unintended trunk links or access links. This can cause network connectivity issues or VLAN hopping vulnerabilities. For example, if both ends are set to dynamic auto, they will not form a trunk.
- Resource consumption: DTP exchanges frames. This consumes a minimal amount of network bandwidth and switch Central Processing Unit (CPU) resources.

Modes of DTP

DTP operates in various modes. These modes determine how a switch port behaves when negotiating a trunk link.

- switchport mode access:
  - Meaning: Configures the port as a permanent non-trunking (access) port. It belongs to a single VLAN and does not send DTP frames.
  - Negotiation: The port will not form a trunk, regardless of the connected port's DTP mode.
- switchport mode trunk:
  - Meaning: Configures the port as a permanent trunking port. It carries traffic for multiple VLANs and sends DTP frames.
  - Negotiation: The port attempts to form a trunk. If the connected port is access or nonegotiate, the trunk will not form.
- switchport mode dynamic desirable:
  - Meaning: Makes the port actively attempt to convert the link into a trunk link. It sends DTP frames and tries to negotiate.
  - Negotiation: It forms a trunk with trunk, desirable, or auto modes.
- switchport mode dynamic auto:
  - Meaning: Makes the port willing to convert the link into a trunk link if the connected port actively requests it. It sends DTP frames but does not actively try to negotiate a trunk.

- Negotiation: It forms a trunk only with trunk or desirable modes. It does not form a trunk with another auto port.

- switchport nonegotiate:
  - Meaning: Configures the port as a permanent trunking port but prevents it from sending DTP frames. You often use this for manually configured trunks, especially when connecting to non-Cisco devices or for security reasons.
  - Negotiation: The port operates as a trunk, but it does not participate in DTP negotiation. The connected port must also be configured as a trunk (for example, switchport mode trunk).

Configure DTP

DTP configuration occurs on a per-interface basis. Follow these steps to configure DTP:

Procedure

Step 1 Enter privileged EXEC mode.

Example:

```
Switch> enable
```

Step 2 Enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 EEnter interface configuration mode for the desired interface.

Example:

```
Switch(config)# interface <interface_type> <interface_number>
```

Step 4 Set the switchport mode.

Example:

```
Switch(config-if)# switchport mode {access | trunk | dynamic desirable | dynamic auto}
```

Step 5 (Optional) Disable DTP negotiation.

Use this command with switchport mode trunk to prevent the port from sending DTP frames.

Example:

```
Switch(config-if)# switchport nonegotiate
```

Step 6 Exit interface configuration mode.

Example:

Switch(config-if)# end

Step 7 Verify the configuration

Example:

```
Switch# show interface <interface_type> <interface_number> switchport
```

To configure interface GigabitEthernet1/0/1 to actively seek to become a trunk:

```
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
```

To configure interface GigabitEthernet1/0/2 as a permanent trunk without DTP negotiation:

```
Switch(config)# interface GigabitEthernet1/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
Switch(config-if)# end
```

Where to Go Next

After configuring VLAN trunks, you can configure the following:

- VLANs
- Voice VLANs
- Private VLANs

Additional References

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2