

# QinQ (Provider Bridging)

---

## Contents

<b>Overview</b> .....	8-2
<b>Introduction</b> .....	8-3
How QinQ Works .....	8-4
Features and Benefits .....	8-4
Terminology .....	8-5
Operating Rules and Guidelines .....	8-6
Enabling QinQ and Configuring QinQ Modes .....	8-6
QinQ Mixed Vlan Mode .....	8-7
Configuring VLANs .....	8-7
Operating Notes and Restrictions .....	8-9
<b>Configuring QinQ</b> .....	8-12
General Configuration Steps .....	8-12
Enabling QinQ .....	8-13
Setting up S-VLANs .....	8-13
Configuring Per-Port S-VLAN Membership .....	8-14
Configuring Port-Types .....	8-15
<b>Configuration Example</b> .....	8-16
<b>Updating QinQ Configurations</b> .....	8-21
Changing QinQ Modes .....	8-21
Disabling QinQ .....	8-21
Changing VLAN Port Memberships (Mixed Vlan Mode) .....	8-21
Moving Ports between C-VLANs and S-VLANs (Mixed Vlan Mode) .	8-22
<b>Displaying QinQ Config and Status</b> .....	8-23
Show Commands for QinQ .....	8-23
Show Commands for VLANs .....	8-24
Displaying Spanning Tree Status .....	8-26

<b>Effects of QinQ on Other Switch Features</b> .....	8-27
<b>Event Log Messages and SNMP Support</b> .....	8-32
SNMP Support and MIB Objects .....	8-32

## Overview

This chapter describes how to enable QinQ operations on the switch and how to configure provider bridge S-VLANs and port assignments.

For information on how to configure and use static, port-based and protocol-based VLANs, refer to chapter 2, “Static Virtual LANs (VLANs)”.

For information on how to configure dynamic VLANs on the switch, refer to chapter 3, “GVRP”.

---

### **License Requirements**

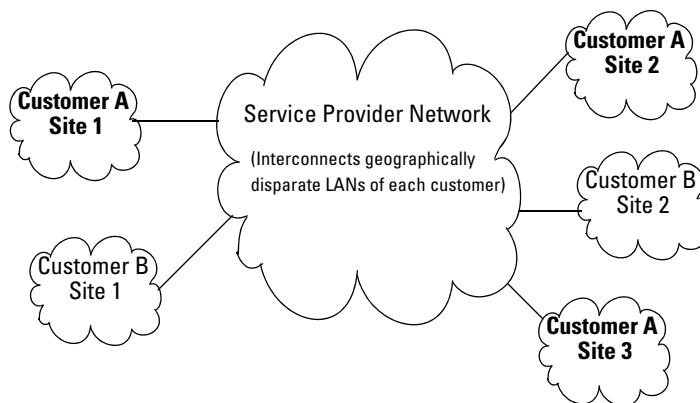
---

In the 3500yl, 5400zl, 6600 and 8200zl switches, QinQ is included with the Premium License. In the 6200yl switches, this feature is included with the base feature set.

## Introduction

The IEEE 802.1ad specification, commonly known as QinQ or provider bridging, extends the IEEE 802.1Q standard by providing for a second tier of VLANs in a bridged network. The general purpose of QinQ is to allow frames from multiple customers to be forwarded (or tunneled) through another topology (provider network) using service VLANs or S-VLANs. The provider bridge, which may comprise multiple devices in the service provider domain, looks like a simple bridge port to the customer's traffic and maintains the customer's VLANs.

Figure 8-1 shows a sample QinQ topology and use model. Customer A has LANs spread across multiple site locations and may want to link them together in a single logical LAN. To do this, the customer could have a cable laid out for the entire distance interconnecting the three sites. A more cost-effective and scalable alternative, however, would be to tunnel frames through the provider's network to interconnect all the sites subscribing to the service. This solution can be delivered using QinQ.



**Figure 8-1. QinQ Network Diagram**

---

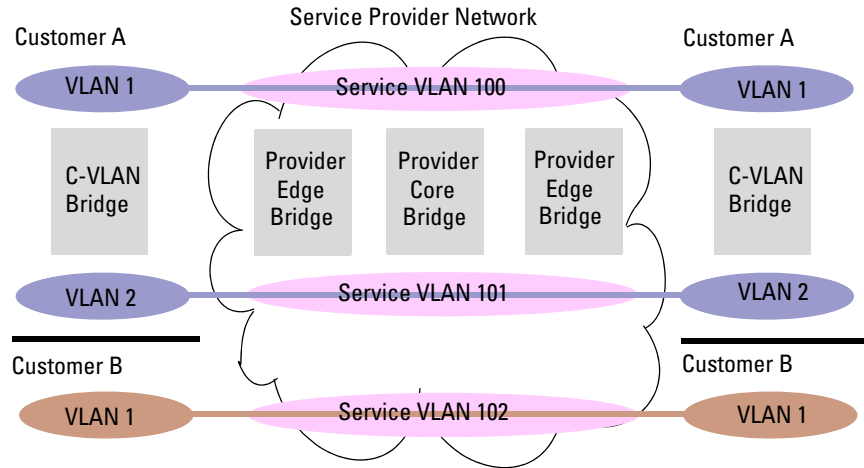
**Note**

The so-called 'Service Provider' and 'Customers' may belong to the same business entity, as in the case where a single enterprise uses QinQ to help segregate local networks and increase the scalability of their backbone infrastructure.

---

## How QinQ Works

Under QinQ, the provider network operates on a different VLAN space, independent of the VLANs that are used in the customer network as shown in Figure 8-2.



**Figure 8-2. Example of VLANs in a QinQ Configuration**

Customer VLANs (referred to as C-VLANs by the IEEE 802.1ad specification) are not used to make any forwarding decisions inside the provider network where customer frames get assigned to service VLANs (S-VLANs). Inside the provider cloud, frames are forwarded based on the S-VLAN tag only, while the C-VLAN tag remains shielded during data transmission. The S-VLAN tag is removed when the frame exits the provider network, restoring the original customer frame.

## Features and Benefits

- Increases the VLAN space in a provider network or enterprise backbone.
- Reduces the number of VLANs that a provider needs to support within the provider network for the same number of customers.
- Enables customers to plan their own VLAN IDs, without running into conflicts with service provider VLAN IDs.
- Provides a simple Layer 2 VPN solution for small-sized MANs (Metropolitan Area Networks) or intranets.
- Provides for customer traffic isolation at Layer 2 within a Service Provider network.

## Terminology

**C-VLANs.** Customer network VLANs that can exist across multiple locations. These are assigned and managed by each customer and are local to the customer space.

**C-VLAN bridge.** A customer-owned device operating regular 802.1Q VLANs.

**Customer.** The consumer of network services delivered by a service provider.

**Customer-network port.** Customer-facing port on a provider edge device. The equivalent of 'CN' ports of the IEEE 802.1ad standard.

**Customer VLAN.** See **C-VLAN**.

**IEEE 802.1ad.** Specification that allows a service provider to assign a unique VLAN identifier (called the Service VLAN ID or S-VID) to customers using multiple VLANs, thereby extending the total number of VLANs that can be supported within the provider network.

**Mixed vlan mode device.** Device that supports both C-VLANs and S-VLANs. A device configured in **qinq mixedvlan** mode can do regular CVLAN switching/routing (standard bridge behavior) and can also serve as a provider edge device tunneling frames into and out of the provider network.

**Port-based interface.** Untagged customer-network ports or trunks on a QinQ enabled device. See also **S-tagged interface**.

**Provider-network port.** Port on an S-VLAN bridge that connects to the provider network. This equates to 'PN' ports of the IEEE 802.1ad standard.

**QinQ.** A feature that enables service providers to use a single VLAN-ID to support multiple customer VLANs by encapsulating the 802.1Q VLAN tag within another 802.1Q frame. See also **IEEE 802.1ad**.

**Service Provider.** The provider of the network that provides one or more service instances to a customer.

**S-tagged interface.** Tagged customer-network ports or trunks on a QinQ enabled device. See also **port-based interface**.

**Service VLAN.** See **S-VLAN**.

**S-VLAN.** Service VLANs that are used to tunnel customer frames through the provider network to customer sites. These are managed by the service provider who can assign each customer a unique S-VLAN ID.

**S-VLAN bridge.** Provider-owned device configured in **qinq svlan** mode that uses S-VLANs only to forward frames in the provider network. This bridge can be further sub-classified as:

- **Provider edge bridge.** An svlan bridge that has customer network ports configured on the device.
- **Provider core bridge.** A device in the core of the provider network that does not interface with any customer bridges. All ports on the device are provider network ports, and the S-VLAN bridge only receives and forwards S-tagged frames.

**Tunnel VLAN.** See **S-VLAN**.

## Operating Rules and Guidelines

This section provides an overview of QinQ operations and restrictions on the switch. For details of CLI commands and configuration procedures, refer to “Configuring QinQ” on page 8-13.

### Enabling QinQ and Configuring QinQ Modes

By default, QinQ is disabled. When QinQ is enabled via the CLI, an operating mode is globally configured on the switch. Two QinQ modes are supported:

- **qinq mixedvlan:** C-VLANs and S-VLANs are both supported, with regular switching/routing based on C-VLAN tags in the C-VLAN domain, while S-VLANs are used for QinQ tunneling through the provider network.
- **qinq svlan:** C-VLANs are NOT supported on the device. All configured VLANs on the switch must be S-VLANs.

Table 8-1 shows how the various QinQ modes and operations impact VLAN configuration options on the switch.

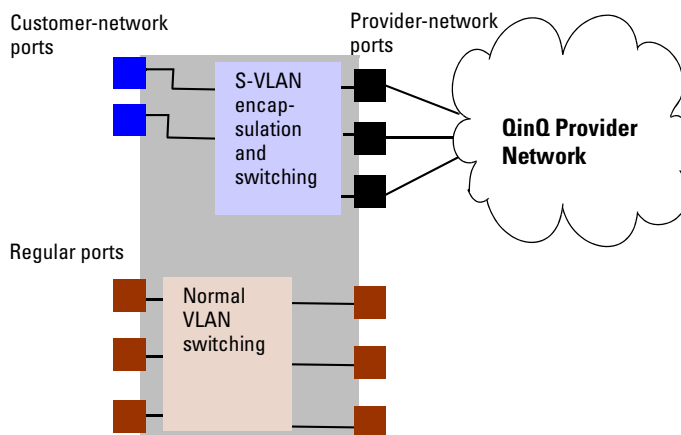
**Table 8-1. Relationship of QinQ Operating Modes to VLAN Environments**

QinQ Operation	CLI Command	VLAN Options
QinQ disabled		
No QinQ support (Default)	<b>no qinq</b>	Only regular VLAN commands are available. If QinQ is disabled, S-VLAN commands are not available.
QinQ enabled		
QinQ mixed vlan mode	<b>qinq mixedvlan</b>	Both S-VLAN and regular VLAN commands (known as C-VLANs in a mixed vlan environment) are available.
QinQ svlan mode	<b>qinq svlan</b>	No regular VLAN commands are available. All VLANs configured on the switch are S-VLANs only.

## QinQ Mixed Vlan Mode

The QinQ mixed vlan mode configuration supports both C-VLAN and S-VLAN operations on the same device. This allows the use of S-VLAN member ports for QinQ tunneling, while regular ports can still do switching or routing within the C-VLAN space. To tunnel customer frames through the provider network, you can externally connect a regular port to a customer-network port, eliminating the need for a separate S-VLAN bridge device to perform such operations. When configuring VLANs on a mixed vlan mode device, a separate **svlan <vid>** command is used to distinguish the S-VLAN type from regular VLANs.

The main advantage for QinQ mixed vlan mode is that users do not have to dedicate the entire switch as a QinQ access switch. For a high density chassis switch such as the 5400zl or 8200zl series, customers can use regular ports for normal LAN switching, while S-VLAN member ports can be configured to access the QinQ provider network (see Figure 8-3). There are some additional restrictions in mixed-VLAN mode (see “Operating Notes and Restrictions” on page 8-10 for details).



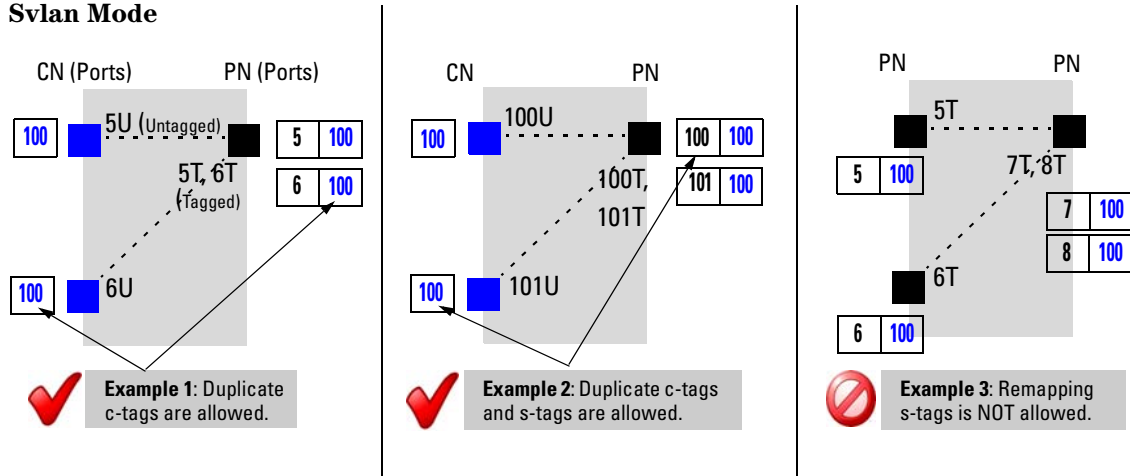
**Figure 8-3. ProCurve Switch in Mixed-VLAN mode**

## Configuring VLANs

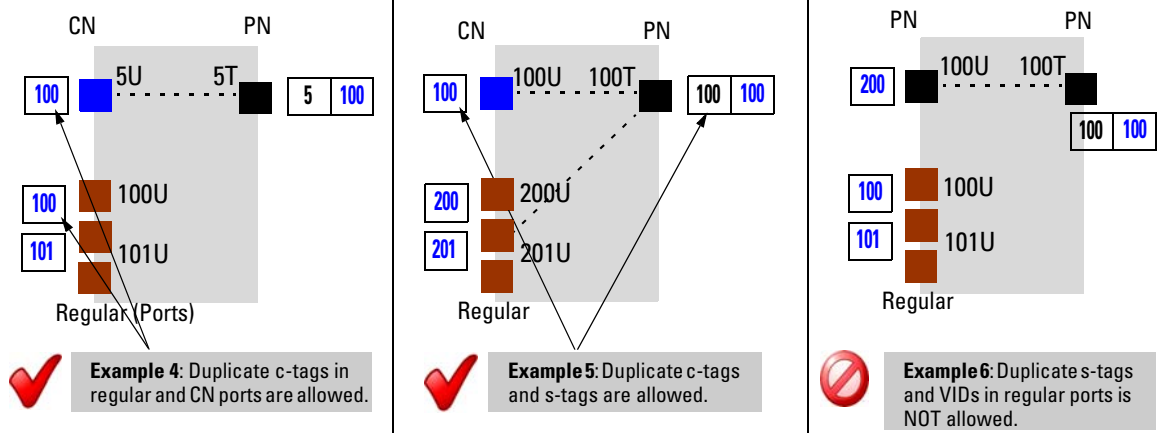
- A VLAN created on a QinQ mixed vlan mode device can be either a regular VLAN (C-VLAN) or a tunnel VLAN (S-VLAN). C-VLANs have no mapping/ relation whatsoever to the S-VLANs on the device.
- VLANs created on a QinQ svlan mode device can be S-VLANs only. S-VLANs provide QinQ tunneling of customer frames and behave like a port-based/s-tagged interface (see “Setting up S-VLANs” on page 8-14 for configuration details).

**QinQ and Duplicate VID's.** Duplicate VID's for c-tagged and s-tagged VLANs (for example, C-VID=100; S-VID=100) are allowed in certain cases and disallowed in others. Customer-network ports are essentially S-VLAN ports: they simply read the C-tags in the customer frame to insert them into the appropriate untagged S-VLAN for that port. Once this double-tagging occurs, frames are forwarded based on the S-VLAN tag only, while the C-VLAN tag remains shielded during data transmission. See Figure 8-4 for examples of allowed configurations.

**Svlan Mode**



**Mixed Mode**



**Figure 8-4. QinQ and Duplicate VID's: Examples of Allowed Configurations**

**Assigning Ports to VLANs.** In mixed vlan mode, a port can be a member of a C-VLAN or of an S-VLAN but not both. For details, on assigning membership to provider-based VLANs, see “Configuring Per-Port S-VLAN Membership” on page 8-15.

**Configuring Port-Types.** The IEEE 802.1ad standard requires that every svlan member port be configured as either a provider-network or as a customer-network port. In a typical deployment scenario, customer-network ports will be configured as untagged members of S-VLANs while provider-network ports will be configured as tagged members of S-VLANs. Note the following configuration rules and guidelines:

- All ports of a device that is QinQ enabled (in svlan mode or mixed vlan mode) are provider-network ports by default—if there are any ports that connect to a customer device, they must be manually configured as customer-network ports.
- Configuring a port-type is only applicable if the device is QinQ enabled and the port is a member of an svlan. In QinQ mixed mode, ports that are members of C-VLANs cannot be configured to any port-type.

For more information, see “Configuring Port-Types” on page 8-16.

---

## Note

If a device running in QinQ svlan mode has one or more ‘customer-network’ ports, it is considered to be a provider edge and not a provider core bridge. This may impact certain operations, such as meshing, UDLD, and stacking. This is because at the edge of the provider network such proprietary protocols are filtered out at customer network ports. This prevents the intermix of stacking/meshing/udld protocols in the customer and provider domains (since they use the same dst-mac address in either domain).

---

## Operating Notes and Restrictions

- **Changing bridge modes requires a reboot.** When changing the operating mode (to/from: QinQ svlan mode, QinQ mixed vlan mode, or QinQ disabled), you will be prompted to restart the system before the changes can take effect. Upon reboot, *all configuration information for the prior QinQ mode will be lost*. Any configurations created will be erased, and the device will boot up with a default configuration for the new QinQ mode.
- **Provider edge devices at Layer 2 only.** QinQ does not provide Layer 3 capabilities of complete network isolation between customers. In a mixed VLAN configuration, there is no switching/routing between C-VLANs and S-VLANs. S-VLANs are essentially Layer 2 VLANs that switch packets based on S-VIDs.

- **IP support.** Regular VLANs support IP and can be routing enabled. S-VLANs of mixed vlan mode devices cannot be ip enabled. S-VLANs of svlan mode devices can be ip enabled, though routing related features (such as ip routing) are not supported.
- **Double-tagging causes frame size increases.** Since there is both a provider VLAN tag and customer VLAN tag in each QinQ frame, the size of each 'double-tagged' frame increases by 4 bytes. To accommodate the frame size increase, ProCurve recommends that you configure all port-based S-VLANs to accept jumbo frames. See the section on “Jumbo Frames” in the *Management and Configuration Guide* for details.
- **S-VLAN configuration restrictions:**
  - S-VLAN commands are not available when QinQ is disabled on the switch.
- **VLAN configuration restrictions in mixed vlan mode:**
  - Both C-VLANs and S-VLANs can be configured on the switch. In a mixed mode device, the default VLAN is always a C-VLAN.
  - VLAN types cannot be updated dynamically. A VLAN can only be classified as an S-VLAN or a C-VLAN at the time its created. Once created, the VLAN cannot be moved between being a C-VLAN and an S-VLAN. If a VID that was initially created as a regular VLAN needs to be used for an S-VLAN, the VID must be deleted and recreated as an S-VLAN.
  - If a VLAN being configured as an S-VLAN already exists as a GVRP C-VLAN or a static C-VLAN on the switch, the S-VLAN creation is blocked. Similarly, a C-VLAN creation is blocked if the same VID exists as a static S-VLAN on the device.
  - S-VLANs in a mixed vlan device cannot be configured as a voice-VLAN, primary-VLAN, or management-VLAN.
  - S-VLANs cannot be configured with ip-layer functionality, except for ip-acls.
- **VLAN configuration restrictions in svlan mode:**
  - Only S-VLANs are supported—the keyword on all vlan-related command syntax changes from **vlan** to **svlan**.
  - Routing related features such as ip-routing, RIP, OSPF, PIM, and VRRP are NOT supported in svlan mode.
- **Port-based restrictions:**
  - In QinQ mixed vlan mode, a port must be explicitly GVRP-disabled before it can be assigned to the S-VLAN space (see page 8-15 for details).

- In QinQ mixed vlan mode, only ports that are members of S-VLANs can be configured as customer network or provider network ports; ports that are members of C-VLANs cannot be configured to any port-type.
  - QinQ mixed vlan mode devices cannot be connected in an S-VLAN mesh topology. This is because STP cannot be run in the S-VLAN space, and so a mesh topology (or the presence of any redundant links) would result in loops.
  - A port can only either be a member of S-VLANs or C-VLANs, but not a combination of both.
  - A port cannot be configured as a ‘Customer-Edge’ as specified in Section 12.13.3 of the IEEE 802.1ad specification. In the current software release, such ‘C-tagged interfaces’ are not supported—only port-based/S-tagged interfaces are supported.
  - Moving ports between C-VLANs and S-VLANs may cause conflicts. For example, if a port has any mirroring/monitoring sessions set up, they will not be allowed to change VLAN domains until these sessions are unconfigured. Refer to “Changing VLAN Port Memberships (Mixed Vlan Mode)” on page 8-22 for additional details.
- **Interoperating with Other Vendor Devices.** When enabling QinQ, you can configure a unique tpid value, such as 0x8100, to allow the device to interoperate with devices that require this value for the inner and outer VLAN-tag. If the provider tag-type is configured as 0x8100, then:
- customer-network ports cannot be configured as tagged-SVLAN members; and
  - tagged-SVLAN members cannot be configured as customer-network ports.
- **Configuring QinQ with Other Network Protocols.** The networks for both the customer and provider can be complex. For information on how QinQ may impact other network protocols (such as spanning tree, LLDP, and GVRP), refer to “Effects of QinQ on Other Switch Features” on page 8-28.

## Configuring QinQ

QinQ must be configured on all the devices and ports participating in the provider bridge. Typically, customer facing ports are configured as untagged members of S-VLANs and provider facing ports are configured as tagged members of S-VLANs. Per the IEEE 802.1ad specification, there is no condition binding port types (customer or provider) to untagged or tagged S-VLAN memberships. Therefore, when configuring QinQ tunnelling on the switch, you would first configure per-port S-VLAN membership (tagged or untagged), and then configure the port type as ‘customer-network’ or ‘provider-network’ depending on the device to which the switch port is connected.

---

### Note

A customer-network port can receive S-VLAN tagged frames if the customer and provider agree upon the S-VID association for that customer and the customer device is capable of sending S-VLAN tagged frames.

---

## General Configuration Steps

To configure QinQ, you would take the following steps on all participating provider switches (see the following sections for details and refer to page 8-17 for a configuration example):

1. Enable QinQ on the device, selecting the appropriate qinq mode (svlan or mixed vlan mode).
2. Save the configuration and reboot the switch.
3. Configure S-VLANs and assign per port VLAN membership.
4. Configure port-types for all of the switch ports that carry QinQ traffic across the network.
5. (Optional) Verify the configuration (see “Displaying QinQ Config and Status” on page 8-24).

---

### Caution

A reboot is required to enable/disable QinQ operations on the switch. When moving between qinq modes (**qinq mixedvlan** to **qinq svlan** or vice versa), the switch boots up with a default configuration for the new qinq mode and the configuration parameters of the current mode will be erased out. Refer to “Updating QinQ Configurations” on page 8-22 for details.

---

## Enabling QinQ

By default, QinQ is disabled on the switch. To enable QinQ, the switch must be put into either QinQ mixed vlan mode or QinQ svlan mode by issuing one of the following commands from configuration mode on the CLI.

**Syntax:** `qinq mixedvlan <tag-type[tpid]>`

*From config mode, globally enables QinQ mixed mode, an environment that supports both S-VLAN and C-VLAN traffic on the same device. This command requires a reboot to take effect.*

*Default: Disabled.*

**Syntax:** `qinq svlan <tag-type[tpid]>`

*From config mode, globally enables QinQ svlan mode, an S-VLAN only environment that supports port-based or s-tagged interfaces of the standard. Requires a reboot to take effect.*

*Default: Disabled.*

## Setting up S-VLANs

S-VLANs can be created via the CLI using the **svlan** `<vid>` command.

**Syntax:** `svlan < vid / ascii-name-string >`  
`[no] svlan < vid >`

*If < vid > does not exist in the switch, this command creates a port-based S-VLAN with the specified < vid >. If the command does not include options, the CLI moves to the newly created S-VLAN context. If you do not specify an optional name, the switch assigns a name in the default format: **svlann** where **n** is the < vid > assigned to the S-VLAN. If the S-VLAN already exists and you enter either the **vid** or the **ascii-name-string**, the CLI moves to the specified S-VLAN's context.*

*The **[no]** form of the command deletes the S-VLAN as follows:*

- *If one or more ports belong only to the S-VLAN to be deleted, the CLI notifies you that these ports will be moved to the default VLAN and prompts you to continue the deletion. For member ports that also belong to another S-VLAN, there is no “move” prompt.*

---

### Note

When QinQ is disabled, all VLANs must be C-VLANs. When QinQ is enabled in svlan mode, all VLANs must be S-VLANs. When QinQ is enabled in mixed vlan mode, VLANs can be configured as either C-VLANs or S-VLANs. For more on S-VLAN configuration constraints, refer to the restrictions on page 8-10.

---

## Configuring Per-Port S-VLAN Membership

The **svlan** <vid> command supports tagged and untagged options to configure per-port S-VLAN memberships. You can use these options from the configuration level by beginning the command with **svlan** < vid >, or from the context level of the specific VLAN by just typing the command option.

**Syntax:** svlan < vid >

tagged < port-list >

*Configures the indicated port(s) as **Tagged** for the specified S-VLAN. The “no” version sets the port(s) to either **No** or (if GVRP is enabled) to **Auto**.*

untagged < port-list >

*Configures the indicated port(s) as **Untagged** for the specified S-VLAN. The “no” version sets the port(s) to either **No** or (if GVRP is enabled) to **Auto**.*

forbid < port-list >

*QinQ svlan mode only. Used in port-based S-VLANs to configure < port-list > as “forbidden” to become a member of the specified VLAN, as well as other actions. The “no” version sets the port(s) to either **No** or (if GVRP is enabled) to **Auto**. Refer to chapter 3, “GVRP”, in this guide.*

auto < port-list >

*QinQ svlan mode only. Available if GVRP is enabled on the switch. Returns the per-port settings for the specified S-VLAN to **Auto** operation. Note that **Auto** is the default per-port setting for a static VLAN if GVRP is running on the switch. Refer to chapter 3, “GVRP”, in this guide.*

**Note:** Since provider-gvrp is not supported in a QinQ mixed vlan mode environment, the **forbid** and **auto** configurations are only available in QinQ svlan mode. For more information on dynamic VLAN and GVRP operation, refer to chapter 3, “GVRP” in this guide.

**In QinQ mixed vlan mode.** An interface (port or trunk) must be explicitly GVRP-disabled before it can be assigned to the S-VLAN space. When you first attempt to configure a port as tagged for an S-VLAN, the CLI will issue a message disallowing the configuration. For example:

```
<config #> svlan 200 tagged a1,a2
GVRP enabled ports cannot be members of svlans. Disable
the interface level gvrp configuration.
```

To disable gvrp at the interface, you would issue the following command:

```
<config #> interface a1,a2 unknown-vlans disable
```

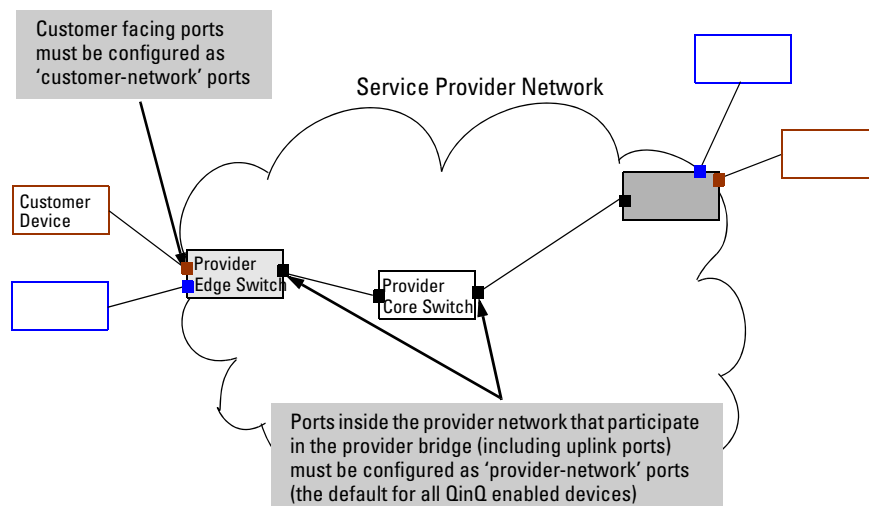
Now when you configure the port, the CLI will issue a warning prompt:

```
<config #> svlan 200 tagged a1,a2
Ports a1, a2 will lose their cvlan memberships if any.
Do you want to continue? [y/n] y
```

Press **[Y]** to continue and automatically configure both ports as port-type 'provider-network' (the default for all S-VLAN member ports).

## Configuring Port-Types

When QinQ is enabled on the switch all S-VLAN member ports must be categorized as either port-type customer-network or provider-network (see Figure 8-5).



**Figure 8-5. Example of Customer or Provider Ports in the Provider Network**

All ports of a QinQ enabled device default to 'provider-network'. Any ports participating in the provider bridge that are used to connect to customer equipment, must be manually configured as port-type 'customer-network'. In a mixed mode device, ports that are members of C-VLANs and that do not participate in the provider-bridge cannot be configured to any port-type.

The following command allows you to configure the appropriate port-type.

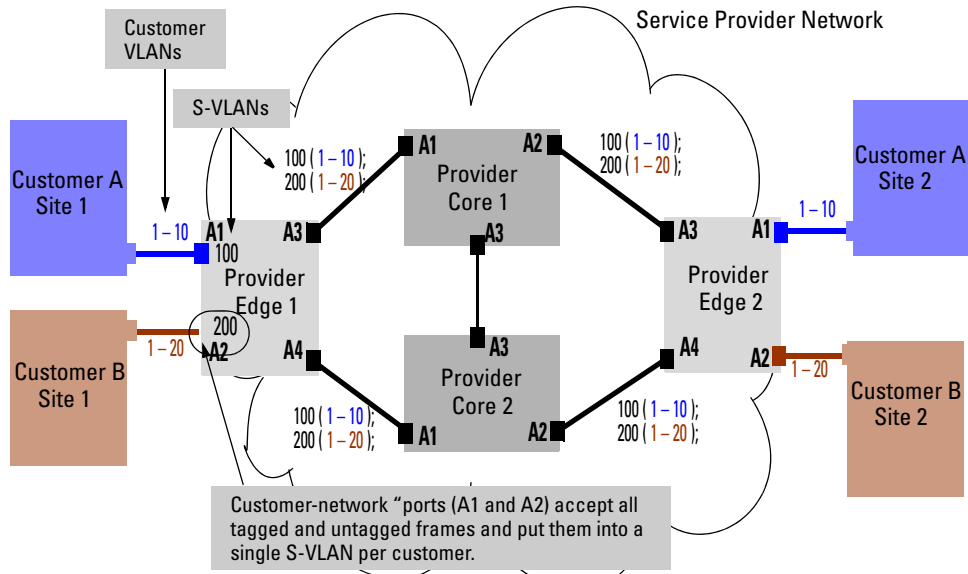
**Syntax:** [no] interface <port-list | Trk> qinq port-type <customer-network | provider-network>

*Configures the specified ports/trunks as a customer network port or provider network port.*

*Default: port-type provider (for QinQ svlan mode)*

## Configuration Example

Figure 8-6 shows a configuration example that uses four ProCurve switches to establish a QinQ tunnel through the provider network.



**Figure 8-6. QinQ Configuration Example**

The design parameters for this example are as follows:

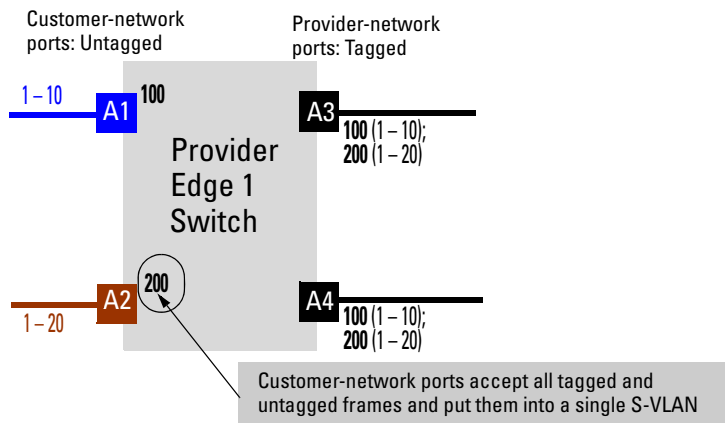
- The provider edge bridge and the provider core bridge are configured in svlan mode.
- Each customer is associated with a single S-VLAN connecting two separate sites: customer A's VLANs (C-VLANs 1-10) are associated with S-VLAN 100; and customer B's VLANs (C-VLANs 1-20) are associated with S-VLAN 200.

### Notes

- The VLANs of customers A and B can overlap: this will not result in intermixing of customer frames in the provider cloud because the S-VLANs associated with each customer are different.
- Core devices are not mandatory to establish a QinQ tunnel. For example, two edge-bridges can be connected directly to create a provider bridge network.

- The relationship between S-VLANs and C-VIDs is typically one to many. An alternative configuration might associate a single customer's C-VIDs with more than one S-VLAN. Such a configuration would most likely be used to tunnel distinct C-VIDs through various S-VLANs, but seldom be used to send the same C-VID through multiple S-VLANs.

**Configure Provider Edge 1 Switch.** Figure 8-7 shows the configuration details for “Edge 1” switch.



**Figure 8-7. Configuration Example: Edge Switch 1**

At the end of the configuration, the following settings will apply:

- All customer A site traffic received on port A1 will be associated with S-VLAN 100. This is independent of the C-VLAN tag information that the customer frames may carry.
- All customer B Site 1 traffic will be associated with S-VLAN 200 and be switched out to the core (uplinks A3, A4) with the S-VLAN tag-id of 200.
- The frame size will increase by 4 since ports A3 and A4 are tagged members of S-VLAN 100 and 200.

To configure the switch, you would do the following steps:

1. Enable QinQ.  

```
Edge 1(config)# qinq svlan tag-type 88a8
```
2. Reboot the box with the configuration saved to transfer into svlan bridge mode.

---

**Note**

A reboot is required for the QinQ enable command to take effect.

3. Configure S-VLANs and ports connected to the customer network.

```
Edge1 (config)# svlan100
Edge1(svlan-100)# untagged A1
Edge1(svlan-100)# exit
Edge1(config)# int A1 qinq port-type customer-network
Edge1(config)# svlan 200
Edge1(svlan-200)# untagged A2
Edge1(svlan-200)# exit
Edge1(config)# int A2 qinq port-type customer-network
```

---

**Note**

In this example, customer A is assigned S-VLAN 100 and customer B is assigned S-VLAN 200. However, the same customer can be associated with more than one S-VLAN. Also, interfaces A1 and A2 are configured as customer network ports because they are linked to customer bridges.

4. Configure the provider ports leading to the core of the provider network.

```
Edge1(config)# svlan 100 tagged A3, A4
Edge1(config)# svlan 200 tagged A3, A4
Edge1(config)# interface A3,A4 qinq port-type
provider-network
```

---

**Note**

As recommended by IEEE 802.1ad specification, uplink ports should generally be configured as tagged ports for S-VLANs that are used to carry customer traffic. However, this is not a mandatory requirement on ProCurve switches—S-VLANs that are used for internal provider network use (not carrying customer traffic but for management of the provider network devices) can have untagged port memberships.

**Configure Provider Edge 2 Switch.** The configuration details for the “Edge 2” switch mirrors the configuration for the Edge 1 switch. All customer traffic received on port A1 from customer A’s site 2 will be associated with S-VLAN 100. Similarly, all customer B’s site 2 traffic will be associated with S-VLAN 200.

To configure the switch, you would do the following steps:

1. Enable QinQ.

```
Edge 2(config)# qinq svlan tag-type 88a8
```

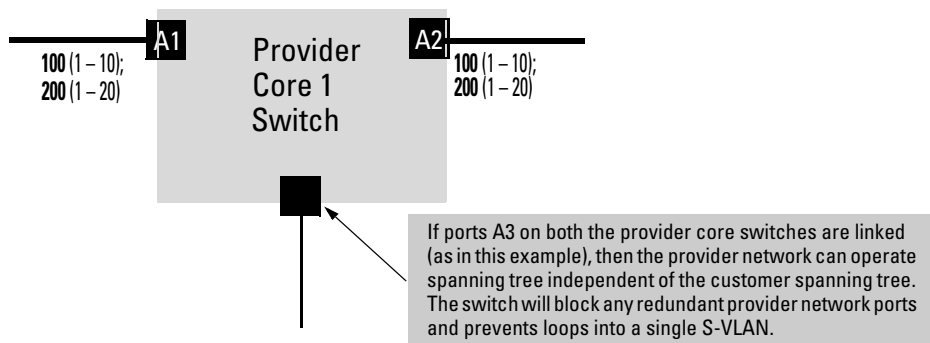
2. Reboot the box with the configuration saved to transfer into svlan bridge mode.
3. Configure S-VLANs and customer ports connected to the customer network.

```
Edge2(config)# svlan 100
Edge2(svlan-100)# untagged A1
Edge2(svlan-100)# exit
Edge2(config)# int A1 qinq port-type customer-network
Edge2(config)# svlan 200
Edge2(svlan-200)# untagged A2
Edge2(svlan-200)# exit
Edge2(config)# int A2 qinq port-type customer-network
```

4. Configure the provider ports leading to the core of the provider network.

```
Edge1(config)# svlan 100 tagged A3, A4
Edge1(config)# svlan 200 tagged A3, A4
Edge1(config)# interface A3,A4 qinq port-type
provider-network
```

**Configure Provider Core 1 Switch.** Figure 8-8 shows the configuration details for the “Core 1” switch..



**Figure 8-8. Configuration Example: Core Switch 1**

To configure the Core 1 switch, you would take the following steps:

1. Enable QinQ.

```
Core 1(config)# qinq svlan tag-type 88a8
```

2. Reboot the box with the configuration saved to transfer into svlan bridge mode.
3. Configure S-VLANs and port assignments.

```
Core 1(config)# svlan 100
Core 1(svlan-100)# tagged A1, A2
Core 1(svlan-100)# exit
Core 1(config)# svlan 200
Core 1(svlan-200)# tagged A1, A2
Core 1(svlan-200)# exit
Core 1(config)# interface A1,A2 qinq port-type
provider-network
```

---

**Note**

The S-VLAN configuration for the core devices is based on what VLANs the edge devices (Edge 1 and 2) can send. Per the 802.1ad specification, all ports carrying customer traffic will be tagged on the VLAN that the port carries customer frames on.

---

**Configure Provider Core 2 Switch.** To configure the Core 2 switch, you would take the following steps:

1. Enable QinQ.  
Core 2(config)# qinq svlan tag-type 88a8
2. Reboot the box with the configuration saved to transfer into svlan bridge mode.
3. Configure S-VLANs and port assignments.

```
Core 2(config)# svlan 100
Core 2(svlan-100)# tagged A1, A2
Core 2(svlan-100)# exit
Core 2(config)# svlan 200
Core 2(svlan-100)# tagged A1, A2
Core 2(svlan-100)# exit
Core 2(config)# interface A1,A2 qinq port-type
provider-network
```

**Verify the Configuration.** Once the edge and core switch configurations are completed, QinQ operations can begin. To verify operations, it should be possible to assign IP-addresses to customer A or B devices in site 1 and site 2 and ping them. If everything has been configured correctly, traffic will flow through the provider network cloud and reach the other site seamlessly. To verify the configuration, see also “Displaying QinQ Config and Status” on page 8-24.

## Updating QinQ Configurations

This section considers the impacts of updating QinQ modes and configuration settings on the switch.

### Changing QinQ Modes

Changing QinQ modes (and/or disabling QinQ operations) will result in the current configuration being erased. See the following Caution for details.

---

#### **Caution**

Configuring the switch to operate in a different bridge mode requires a reboot to take effect. Upon reboot, **all configuration information for the prior QinQ mode will be lost**. Any configurations created under the existing QinQ mode will be erased, and the device will boot up with a default configuration for the new QinQ mode.

For information on the effect of the different QinQ modes on switch protocols and operations, refer to Table 8-2 on page 8-28.

### Disabling QinQ

To disable QinQ once it has been enabled, you would issue the following commands from configuration mode on the CLI.

**Syntax:** no qinq

*This is the default mode when QinQ is disabled on the switch.*

*Moving into this configuration from another qinq configuration requires a reboot to take effect. Upon reboot, all configuration information for the prior QinQ mode will be lost.*

*Default setting. Standard VLAN operations apply.*

### Changing VLAN Port Memberships (Mixed Vlan Mode)

On mixed vlan mode devices, certain per-port features are not supported on S-VLANs that are supported on C-VLANs. Ports that are currently members of a regular VLAN can only move to an S-VLAN if there is no conflicting configuration.

---

**Note**

---

To avoid a misconfiguration, it is recommended that you use a default interface configuration when moving ports between C-VLANs and S-VLANs.

When configuring S-VLAN port memberships using the **svlan** command, the CLI issues a warning and prompt if any of the ports listed already belong to a regular VLAN. For example:

```
<config #> svlan 200 tagged a1,a2
Ports a1, a2 will lose their cvlan memberships if any.
Do you want to continue: y/n?
```

The warning prompt is displayed only when there is at least one port in the port list that needs to be moved out from the C-VLAN space to the S-VLAN domain. Similarly, if ports being added to the C-VLAN are already members of an S-VLAN, the CLI issues a warning that the port's membership with its existing VLANs will be removed and will prompt for a confirmation before continuing.

If all ports are just being added or removed from within the same VLAN type domain, no prompt will appear. For example, moving ports from S-VLAN 200 to S-VLAN 300, will not result in any warning as the ports are already part of the S-VLAN domain.

## Moving Ports between C-VLANs and S-VLANs (Mixed Vlan Mode)

A port (or trunk) that is a member of C-VLANs cannot be moved into the S-VLAN space with conflicting configurations for the S-VLAN mode. The list of conflicting protocols/features is listed below. If a port has any of these enabled, the feature must be disabled before the port can be moved in to the S-VLAN space.

- An interface has to be GVRP-disabled to move it from the C-VLAN to the S-VLAN space. This is because S-VLANs of mixed vlan mode do not support provider-GVRP, and also because a GVRP-enabled configuration (when the port is a C-VLAN member) is in the context of customer-GVRP which must be disabled before the port can operate in the S-VLAN space.
- Interface should not have any mirroring or monitoring sessions when moving between C-VLANs and S-VLANs. All mirror/monitor sessions that involve the port must be unconfigured.
- An interface that has auth-vid or unauth-vid configuration cannot move into the S-VLAN space. They have to be unset.
- Interfaces cannot have LACP enabled (active or passive modes) when moving into the S-VLAN space. They have to be disabled.

## Displaying QinQ Config and Status

The following section outlines changes and additions to existing show command outputs to display QinQ configuration and status.

### Show Commands for QinQ

The **show qinq** command displays QinQ configuration information.

**Syntax:** show qinq

*Shows QinQ global and port configurations on the switch.*

**Mode:** Shows the QinQ configuration mode that is operating on the switch.

- **cvlan bridge:** QinQ is disabled, normal VLANs apply.
- **mixedvlan bridge mode:** Both S-VLANs and regular C-VLANs are available in a mixed vlan mode environment.
- **svlan mode:** No regular VLAN commands are available. All VLANs configured on the switch are S-VLANs only.

**Tag-id:** Displayed only if QinQ is enabled on the switch.

**Port Type:** Displayed only if QinQ is enabled on the switch. On a mixed mode device, port type is only shown for svlan ports.

For example:

```
ProCurve (config)# show qinq

QinQ Global Configuration:
-----
Bridge-mode           : svlan bridge

QinQ Interface Configuration:
-----
interface             port-type
-----
A1                    provider-network
A2                    provider-network
Trk1                  customer-network
```

**Figure 8-9.** Example of “show qinq” Output (QinQ svlan mode)

## Show Commands for VLANs

The following show commands are a subset of those listed in the chapter on Static Virtual LANs (VLANs) highlighting the changes made to show the additional QinQ VLAN types (C-VLANs and S-VLANs). For a full listing of all command parameters, refer to the chapter on Static Virtual LANs (VLANs).

**Displaying the Switch’s VLAN Configuration.** The **show vlans** command lists the VLANs currently running in the switch, including the VID, VLAN name, and VLAN status. Once QinQ is enabled in mixed vlan mode, an additional field showing the VLAN type is added to the display output.

**Syntax:** show vlans

(Changes to parameters when QinQ is enabled:)

**VLAN ID:** *Field name changes from 802.1Q VLAN ID to VLAN ID only.*

**Type:** *In a QinQ mixed mode environment, the VLAN type can be either a regular customer VLAN **CVLAN**, or it can be a tunnel VLAN in the provider network **SVLAN**.*

For example:

```

ProCurve (config)# show vlans
Status and Counters - VLAN Information

Maximum VLANs to support : 256
Primary VLAN : DEFAULT_VLAN
Management VLAN : VLAN-100
  
```

VLAN ID	Name	Type	Status	Voice	Jumbo
1	DEFAULT_VLAN	CVLAN	Port-based	No	No
10	Vlan-10	SVLAN	Port-based	No	No
100	Vlan-100	CVLAN	Port-based	No	No
101	Vlan-101	SVLAN	Port-based	No	No

When QinQ is disabled (the default), S-VLANs do not exist on the switch and the VLAN Type field does not appear.

**Figure 8-10. Example of “show vlan” Output (QinQ Mixed VLAN Mode)**

**Displaying the Configuration for a Particular VLAN.** This command uses the VID to identify and display the data for a specific VLAN. Once QinQ is enabled in mixed vlan mode, an additional field showing the VLAN Type is added to the display output.

**Syntax:** show vlans < vlan-id >

(Changes to parameters when QinQ is enabled:)

**VLAN ID:** Field name changes from 802.1Q VLAN ID to VLAN ID only.

**Type:** In a QinQ enabled environment, the VLAN type can be either a regular customer VLAN **CVLAN**, or it can be a tunnel VLAN in the provider network **SVLAN**.

For example:

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

Status and Counters - VLAN Information - Ports - VLAN 10

VLAN ID : 10
Name     : Vlan-10
Type     : SVLAN ←
Status  : Port-based
Voice   : No
Jumbo   : No

Port Information   Mode           Unknown VLAN   Status
-----
1                 Untagged      Disable        Down
2                 Untagged      Disable        Down
3                 Untagged      Disable        Down
4                 Untagged      Disable        Down
5                 Untagged      Disable        Down
```

When QinQ is enabled, the VLAN Type field is displayed.

**Figure 8-11. Example of “Show VLAN” for a Specific VLAN (QinQ Enabled)**

**Displaying the VLAN Membership of One or More Ports.** This command shows to which VLAN a port belongs. Once QinQ is enabled, an additional field showing the VLAN Type is added to the display output.

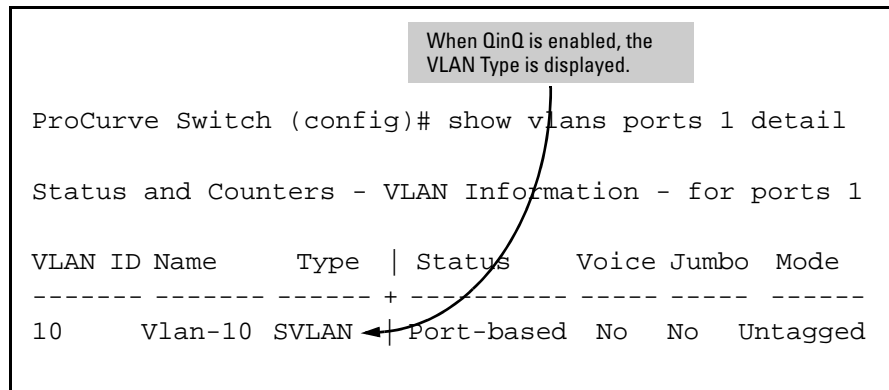
**Syntax:** show vlans < vlan-id >

(Changes to parameters when QinQ is enabled:)

**VLAN ID:** *Field name changes from 802.1Q VLAN ID to VLAN ID only.*

**Type:** *In a QinQ enabled environment, the VLAN type can be either a regular customer VLAN **CVLAN**, or it can be a tunnel VLAN in the provider network **SVLAN**.*

For example:



```
ProCurve Switch (config)# show vlans ports 1 detail
Status and Counters - VLAN Information - for ports 1
VLAN ID Name      Type | Status      Voice Jumbo  Mode
-----+-----
10      Vlan-10 SVLAN | Port-based  No   No   Untagged
```

When QinQ is enabled, the VLAN Type is displayed.

**Figure 8-12. Example of “Show VLAN Ports” Output (QinQ Enabled)**

## Displaying Spanning Tree Status

In QinQ mixed mode, only ports that are members of C-VLANs will be displayed in **show spanning tree** output. This is due to the fact that ports that are members of S-VLANs do not participate in C-VLAN spanning tree and will always be in forwarding state (treated as edge ports).

## Effects of QinQ on Other Switch Features

Per the IEEE standards, protocols such as STP and GVRP are assigned separate addresses for customer networks and provider networks, ensuring that QinQ has no impact on their operations. Bridge Protocol Data Units (BPDUs) that need to be tunneled through the provider network are treated as normal multicast frames at the provider bridge and forwarded out.

However, other protocols use common addresses for both customer and provider networks, and so are not supported when QinQ is enabled on the switch. Similarly, proprietary features such as meshing, discovery, UDLD, and loop-protect do not provide ‘tunneling’ support. In such cases, where provider networks could run an instance of the same protocol as a customer could run local to their site, these frames are dropped at the customer-network ports of the provider bridge.

---

### Note

The IEEE standards group are devising new addressing schemes that may support additional QinQ tunneling operations. Check the latest product release notes for implementation updates as they apply to ProCurve switches.

---

When QinQ is not enabled (the default setting), there are no impacts to the switch’s normal operations. Table 8-2 shows the impacts of QinQ on the operation of switch protocols and features based on the QinQ mode that is configured: QinQ mixed vlan mode (C-VLANs and S-VLANs are allowed) or QinQ svlan mode (S-VLANs only).

**Table 8-2. Impacts of QinQ Configurations on Other Switch Features**

Switch Feature	Impacts of QinQ Configurations and Allowed Operations
<b>ACLs</b>	<b>In QinQ mixed vlan or svlan modes:</b> <ul style="list-style-type: none"><li>On double-tagged frames, the VID applicable when applying ACLs will be the S-VLAN tag and not the C-VLAN tag.</li></ul>
<b>aaa</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>auth-vid/unauth-vid configuration is not supported on svlan ports; the auth-vid/unauth-vid cannot be an S-VLAN id.</li><li>If a port that is a member of C-VLANs is configured with auth-vid or unauth-vid and it needs to be added to the S-VLAN domain, the auth/unauth configuration must first be undone.</li></ul>
<b>arp-protect</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>arp-protect is NOT supported on SVLANs, nor on S-VLAN ports.</li></ul>

---

<b>CDP</b>	<b>In QinQ mixed vlan or svlan modes:</b> <ul style="list-style-type: none"><li>• CDP frames are consumed at customer network ports, if CDP is enabled on the device port, and the customer device shows up as a CDP neighbor on the customer-network port. If not, the frames are dropped.</li></ul>
<b>DHCP</b>	<b>In QinQ mixed vlan or svlan modes:</b> <ul style="list-style-type: none"><li>• dhcp relay only applies to C-VLANs.</li><li>• dhcp snooping is NOT supported on S-VLANs.</li></ul>
<b>directed-broadcast</b>	<b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>• directed-broadcast is NOT supported on provider core devices.</li></ul>
<b>GVRP</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>• S-VLAN ports cannot be GVRP enabled.</li><li>• Regular VLANs will participate in C-VLAN GVRP if enabled to do so. S-VLANs will tunnel all C-VLAN GVRP frames through.</li><li>• An explicit GVRP disable on a port is a prerequisite to moving the port to an S-VLAN domain.</li><li>• Port-based interfaces do not have support for provider-GVRP protocols. Provider GVRP frames received at S-VLAN interfaces will be dropped.</li><li>• If a VLAN being configured as an S-VLAN is already a GVRP VLAN on the switch, this S-VLAN creation would be blocked.</li></ul> <b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>• GVRP is supported on S-VLAN ports if the qinq mode is svlan.</li></ul>
<b>igmp-proxy</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>• igmp-proxy cannot be configured on S-VLANs.</li></ul> <b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>• igmp-proxy is NOT supported.</li></ul>
<b>IP</b>	See “Layer 3 Protocols (IP, IP+, DHCP, ARP, IGMP Layer 3, Layer 3 ACLs)” on page 8-30.
<b>IPv6</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>• IPv6 features are NOT supported on S-VLANs.</li></ul>
<b>ip-recv-mac</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>• ip-recv-mac cannot be configured on S-VLANs.</li></ul> <b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>• ip-recv-mac is NOT supported.</li></ul>
<b>Jumbo</b>	<b>In QinQ mixed vlan or svlan modes:</b> <ul style="list-style-type: none"><li>• No change in operations. It is recommended to jumbo-enable all SVLANs used for customer data tunneling to support the addition of the extra S-tag in each frame.</li></ul>

---

## QinQ (Provider Bridging)

### Effects of QinQ on Other Switch Features

---

<b>LACP/ Port Trunks</b>	<p><b>In QinQ mixed vlan mode:</b></p> <ul style="list-style-type: none"><li>• Dynamic-LACP is not supported on S-VLAN ports: LACP manual trunks alone are supported. The new trunk will be a member of C-VLANs (port types are not applicable).</li><li>• If two ports are added to a trunk, the resultant trunk will be a member of the default-vlan (vid-1) which is always a C-VLAN. The trunk can subsequently be manually assigned to an S-VLAN.</li><li>• Port-type and VLAN configurations are not mapped. If the port-type is updated through CLI or SNMP and the port is subsequently moved from the C-VLAN space to the S-VLAN space then back again, the last configured port-type is retained through each move.</li></ul> <p><b>In QinQ svlan mode:</b></p> <ul style="list-style-type: none"><li>• On svlan bridges, both manual and dynamic LACP trunks are supported. It is not recommended to configure dynamic trunks on 'customer' ports because they cannot become dynamic members of SVLANs (there is no provider-gvrp for a dynamic trunk to become a member of S-VLANs.)</li><li>• A newly formed trunk will by default be of type 'provider-network'. When the trunk is manually assigned to an S-VLAN for the first time after being created, the port-type is 'provider-network'.</li></ul>
<b>Layer 3 Protocols (IP, IP+, DHCP, ARP, IGMP Layer 3, Layer 3 ACLs)</b>	<p><b>In QinQ mixed vlan mode:</b></p> <ul style="list-style-type: none"><li>• There is no IP layer functionality on S-VLANs.</li><li>• No change in IP layer functionality on regular C-VLANs.</li><li>• S-VLANs cannot be configured as RIP, OSPF, PIM, or VRRP interfaces.</li></ul> <p><b>In QinQ svlan mode:</b></p> <ul style="list-style-type: none"><li>• S-VLANs can be ip enabled.</li><li>• IP routing is NOT supported.</li></ul>
<b>LLDP</b>	<p><b>In QinQ mixed vlan or svlan modes:</b></p> <ul style="list-style-type: none"><li>• LLDP is supported on the device (in both qinq modes). However, there is no provision for tunneling customer LLDP BPDUs through the provider-network.</li><li>• LLDP BPDUs received from a customer's network will be consumed at the customer-network ports of a provider device and the customer device will be displayed as an LLDP neighbor. Similarly the provider network device will show up as a neighbor on the customer's network if the customer-network ports send out LLDP advertisements.</li></ul>
<b>load-sharing</b>	<p><b>In QinQ svlan mode:</b></p> <ul style="list-style-type: none"><li>• Equal cost multi-path (ECMP) is NOT supported on provider core devices.</li></ul>
<b>management VLAN</b>	<p><b>In QinQ mixed vlan mode:</b></p> <ul style="list-style-type: none"><li>• The management VLAN cannot be an S-VLAN.</li></ul>
<b>Meshing</b>	<p><b>In QinQ mixed vlan mode:</b></p> <ul style="list-style-type: none"><li>• Meshing is NOT supported on the device.</li></ul> <p><b>In QinQ svlan mode:</b></p> <ul style="list-style-type: none"><li>• On an all provider-network ports of an svlan-bridge, meshing is supported.</li><li>• Meshing cannot be enabled on customer-network ports.</li></ul>

---

---

<b>Mirroring/ Monitoring</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>• Remote mirroring is not supported on S-VLANs.</li><li>• Cannot monitor a VLAN with mirror ports in the other VLAN domain. That is, an S-VLAN or an S-VLAN port cannot be monitored using a C-VLAN port as its mirror, and vice-versa.</li><li>• When a port is moved from the S-VLAN space to the C-VLAN space (or vice versa), all mirror/monitor sessions on the port must be unconfigured before the move will be allowed.</li></ul>
<b>multicast- routing</b>	<b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>• Multicast routing is NOT supported on provider core devices.</li></ul>
<b>QoS</b>	<b>In QinQ mixed vlan or svlan modes:</b> <ul style="list-style-type: none"><li>• It is not recommended to enable DSCP on S-VLANs used for tunneling as the customer ip-pkt will be modified in the S-VLAN space.</li></ul>
<b>Routing</b>	<b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>• Routing is NOT supported on provider core devices.</li></ul>
<b>source-binding</b>	<b>In QinQ mixed vlan or svlan modes:</b> <ul style="list-style-type: none"><li>• source-binding cannot be configured on S-VLANs.</li></ul>
<b>source-route</b>	<b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>• source-route is NOT supported on provider core devices.</li></ul>
<b>Spanning Tree</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>• Customer (C-VLAN) spanning tree is supported. All C-VLAN ports will receive/transmit customer STP BPDUs and participate in regular VLAN spanning tree as usual.</li><li>• When customer STP BPDUs are received at S-VLAN ports on the switch, they will be flooded out of the other ports on the S-VLAN. All such frames will be tunneled through the S-VLAN tunnel unscathed.</li><li>• Provider (S-VLAN) spanning tree is NOT supported on the switch. If S-VLAN STP frames are received on any S-VLAN enabled ports, they will be reforwarded out of the other ports on the S-VLAN.</li><li>• STP configuration on S-VLAN ports is not supported.</li><li>• If a port that is a member of C-VLANs is moved into being a member of S-VLANs, the port would, by default, tunnel customer STP BPDUs.</li><li>• If a C-VLAN port has been configured with any non-default STP parameters (such as <b>admin-edge</b>, <b>auto-edge</b>, and <b>bpdu-protect</b>) and is then moved into an S-VLAN, the port will be put into a forwarding state regardless of the STP configurations done when the port was a member of the C-VLAN.</li><li>• MSTP instances cannot include S-VLANs.</li></ul> <b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>• Provider (S-VLAN) spanning tree is supported—both provider-network ports and customer-network ports will receive/transmit provider STP BPDUs.</li><li>• Customer (VLAN) spanning tree tunneling is supported on S-VLAN interfaces—customer-network or provider-network ports will tunnel customer STP BPDUs through the appropriate S-VLAN.</li></ul>

---

## QinQ (Provider Bridging)

### Effects of QinQ on Other Switch Features

---

<b>Stacking</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>Stacking is only supported on C-VLANs. The device does not advertise itself (using the stack discovery protocol) in the S-VLAN space.</li></ul> <b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>Stacking discovery protocol frames will not be sent out of customer-network ports; similarly, any stacking discovery protocol frames received on customer-network ports will be dropped.</li></ul>
<b>UDLD</b>	<b>In QinQ mixed vlan or svlan modes:</b> <ul style="list-style-type: none"><li>UDLD frames received on udld-disabled customer network ports will be dropped. However, if the customer-network port is udld-enabled, it can peer with a customer device.</li><li>UDLD frames received on udld-disabled provider network ports will be reforwarded out of other udld-disabled provider network ports on the same VLAN.</li><li>UDLD reforwarding in the C-VLAN space (QinQ disabled or mixed vlan mode) will remain unaltered.</li></ul>
<b>udp-bcast-forward</b>	<b>In QinQ svlan mode:</b> <ul style="list-style-type: none"><li>udp-bcast-forward is NOT supported on provider core devices.</li></ul>
<b>unknown-vlans</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>GVRP (learn and disabled modes) not supported on S-VLAN ports.</li><li>A C-VLAN port that has GVRP enabled will need to disable it before it can be added to S-VLANs.</li></ul>
<b>Voice VLANs</b>	<b>In QinQ mixed vlan mode:</b> <ul style="list-style-type: none"><li>S-VLANs cannot be configured as voice-VLANs.</li></ul>
<b>VRRP</b>	<b>In QinQ mixed vlan or svlan modes:</b> <ul style="list-style-type: none"><li>VRRP is NOT supported on S-VLANs.</li></ul>

---

## Event Log Messages and SNMP Support

Table 8-3 shows the event log messages that may be generated when QinQ is enabled on the switch.

**Table 8-3. QinQ Event Log Messages**

Message	Meaning
system: Rebooting for qinq mode change	System reboot occasioned by a change in QinQ configuration mode.
QinQ: qinq mode - mixedvlan	The device is configured to operate in qinq mixed vlan mode.
QinQ: qinq mode - svlan	The device is configured to operate in qinq svlan mode.

---

### SNMP Support and MIB Objects

The switch SNMP agent can make use of certain variables that are included in a Hewlett-Packard proprietary MIB (Management Information Base) file. Table 8-4 on page 8-34 shows the MIB objects that can be used to configure the Q-in-Q (provider bridge) mode, the provider bridge port-type, and the QinQ outer tag ethertype.

The MIB objects listed in the following table may be subject to change. The **walkmib** *<OBJECT-STR>* CLI command can be used to verify the availability of the listed MIB objects on the device.

To download the latest version of the MIB file:

1. Go to the ProCurve Networking Web site at: [www.procurve.com](http://www.procurve.com)
2. Click on **software updates**, then **MIBs**.

**Table 8-4. MIB Objects for QinQ**

MIB Object	Notes and Descriptions
<b>Standard MIBs</b>	
dot1qVlanStaticTable	<p>VLANS (S-VLANs or C-VLANs) are created using the standard MIBs such as the dot1qVlanStaticTable defined by rfc2674_q MIB. To differentiate the VLAN as an S-VLAN or a C-VLAN, the dot1qVlanStaticTable is augmented by an HP proprietary MIB (hpicfVlanClassifierTable) that lets the user specify the VLAN type.</p>
dot1qVlanStaticEntry	<p>A port can be a member of C-VLANs or S-VLANs but not both. When changing port memberships using the SNMP dot1qVlanStaticEntry mib object, variable binding to add a port to the svlan and variable bindings to remove the port from all existing cvlans (that it is a member of) need to be sent in the same PDU (much like how the 'vlan &lt;vlan-id&gt; untagged &lt;port&gt;' CLI command works today). The same is applicable when moving a port from the S-VLAN space to the C-VLAN space.</p>
<b>HP Proprietary MIBs</b>	
hpicfProviderBridge	<p>This MIB module is the HP 'version' of the standard Provider Bridge MIB and the proprietary extensions to it.</p>
hpicfProviderBridgeType	<p>Configures a device to any one of the following bridge mode options:</p> <ul style="list-style-type: none"> <li>• <i>regular vlanBridge</i> (provider bridge feature disabled mode, all VLANs are C-VLANs);</li> <li>• <i>s-vlan bridge</i> (provider bridge mode with only S-VLANs);</li> <li>• <i>provider edge bridge</i> (provider bridge mode with C-VLANs and S-VLANs and mappings between them);</li> <li>• <i>vlanSvlanBridge</i> (provider bridge mode with independent C-VLANs and S-VLANs on the same device).</li> </ul>
hpicfProviderBridgeEtherType	<p>Defines the 2-byte ethertype for provider-tagged frames. It is applicable to the following bridge types: s-vlan bridge, provider edge bridge, or vlanSvlanBridge. The default value is 0x88a8. Changing from onetag-type to another with a given hpicfProviderBridgeType configuration will reboot the device and the new tag-type will take effect subsequently.</p>
hpicfProviderBridgeVlanType Table	<p>Augments the dot1qVlanStaticTable (see Standard MIBs above). Used to configure a VLAN as an S-VLAN or as a C-VLAN in vlanSvlanBridge mode. The absence of this variable binding would classify the new VLAN as a C-VLAN.</p>

<b>MIB Object</b>	<b>Notes and Descriptions</b>
hpicfProviderBridgePortTable	Used to configure each port as a 'provider' or 'customer'. This MIB object is only relevant when the device is QinQ enabled. On a non provider device (QinQ disabled), any SET operation on this MIB object is disallowed and an 'SNMP-GET' would not return any entry.
hpicfProviderBridgePortEntry	Used to specify the designated type of an externally accessible port on a Provider Bridge. These include the following options: <ul style="list-style-type: none"><li>• <i>customer-edge port</i> (reserved for future use);</li><li>• <i>customer-network port</i>: an S-VLAN component port on a provider bridge or within a provider edge bridge that receives and transmits frame for a single customer.</li><li>• <i>provider-network port</i>: an S-VLAN component port on a provider bridge that can transmit and receive frames for multiple customers.</li></ul>

**QinQ (Provider Bridging)**  
Event Log Messages and SNMP Support