Dell™ PowerConnect™ 34XX Systems

User's Guide Addendum

Notes, Notices, and Cautions

NOTE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

September 2006   Rev. A02

This document is an addendum to the PowerConnect 34XX user guide and includes the following topics:

- Configuring QinQ
- Defining STP Root Guard
- Configuring LLDP
- HTTP/HTTPS Upload/Download

Configuring QinQ

Configuring Customer VLANs Using the Web Interface

Customer VLANs are configured using QinQ. QinQ tagging allows network managers to add an additional tag to previously tagged packets. Adding additional tags to the packets helps create more VLAN space. The added tag provides an VLAN ID to each customer, this ensures private and segregated network traffic. The VLAN ID tag is assigned to a customer port in the service providers network. The designated port then provides additional services to the packets with the double-tags. This allows administrators to expand service to VLAN users.

To configure customer VLANs:

1 Click **Switch > VLAN > VLAN Membership**. The **VLAN Membership** page opens.

Figure 1-1.   VLAN Membership
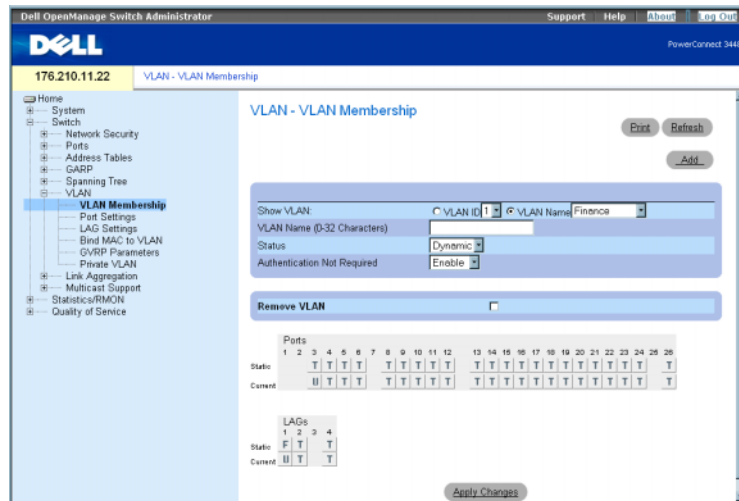
2 Click **Add**. The **Create New VLAN** page opens:

Figure 1-2.   Create New VLAN
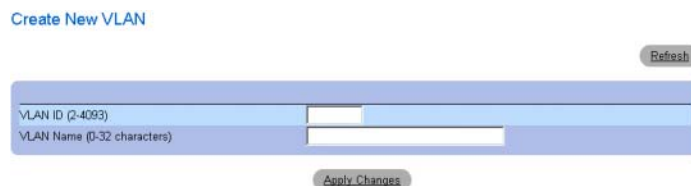
3 Define the **VLAN ID** and **VLAN Name** fields.

4 Click **Apply Changes** .

5 Click **Switch > VLAN > Port Settings**. The **VLAN Port Settings** page opens.

Figure 1-3. VLAN Port Settings
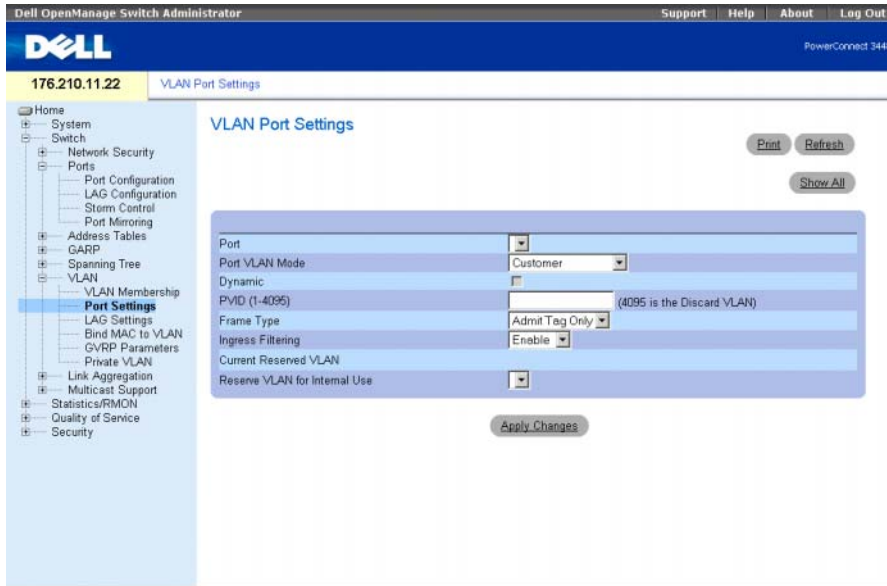
6 Select the interface.

7 Set the **Port VLAN Mode** field to **Customer**.

8 Define the remaining fields.

9 Click **Apply Changes** . The VLAN Port settings are saved, and the device is updated.

10 Click **Show All** . The **VLAN Port Table** opens.

Figure 1-4. VLAN Port Table

11 Select the Port VLAN Mode.

12 Click ⬚ Apply Changes ⬚ . The customer VLAN is defined, and the device is updated.

Configuring Customer VLANs using the CLI

To configure QinQ, perform the following:

1 Enter the global configuration mode.

```
Console>enable
Console#config
Console (config)#
```

2 Enter the VLAN configuration mode.

```
Console (config)# vlan database
Console (config-vlan)#
```

3 Create VLAN in the VLAN database.

```
Console (config-vlan)# vlan 100
Console (config-vlan)# exit
```

4 Configure port e5 as a customer port for VLAN 100.

```
Console (config)# interface ethernet 1/e5
Console (config-if)# switchport mode customer
Console (config-if)# switchport customer vlan 100
Console (config-if)# exit
Console (config)#
```

5 Configure port e10 as a trunked port, tagged for VLAN 100.

```
Console (config)# interface ethernet 1/e10
Console (config-if)# switchport mode trunk
Console (config-if)# switchport trunk allowed vlan add 100
Console (config-if)# exit
Console (config)#
```

The following is an example of the QinQ show commands:

```
console# show interfaces switchport ethernet 1/e5
Port: 1/e5
Port Mode: Customer
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 100
Protected: Disabled

Port is member in:

 Vlan            Name            Egress rule    Port Membership Type
 ----     ----------------------   ----------   -------------------
 100            100             Untagged       Static


Forbidden VLANS:
```

```
 Vlan              Name
 ----     ----------------------



Classification rules:

Protocol based VLANs:

 Group ID        Vlan ID
 --------    ------------------



Mac based VLANs:

 Group ID        Vlan ID
 --------    ------------------



Subnet based VLANs:

 Group ID        Vlan ID
 --------    ------------------


console#
```

QinQ Example

```
console# show ip igmp snooping cpe vlans


        inner VLAN          multicast TV VLAN
  ----------------------    --------------------
            3                   3001
            4                   3000
```
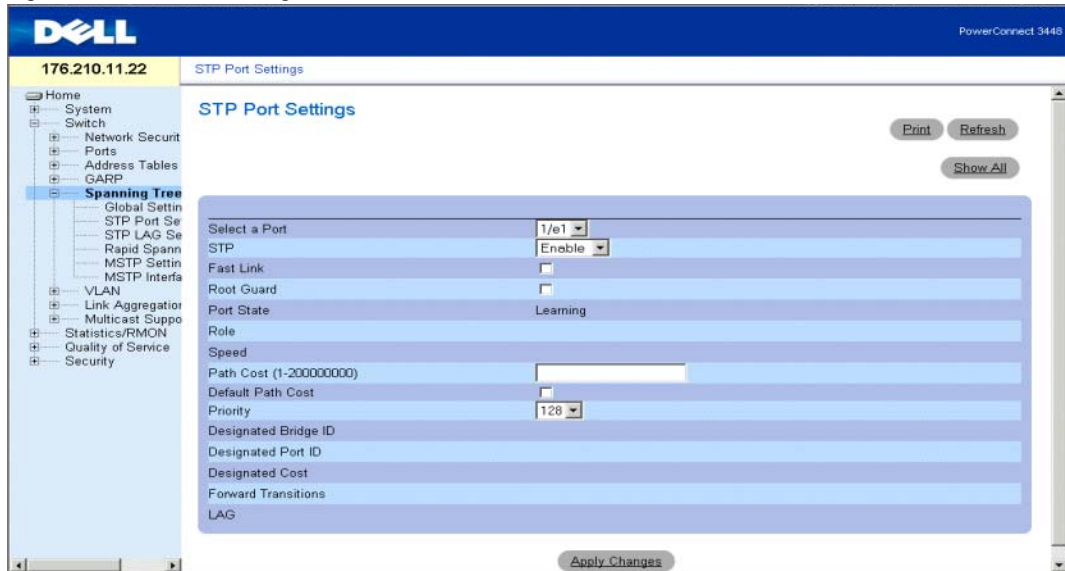
Defining STP Root Guard

Use the **STP Port Settings** page to assign Spanning Tree Port (STP) properties to individual ports.

To open the **STP Port Settings** page, click **Switch → Spanning Tree → STP Port Settings** in the tree view.

Figure 1-5.   STP Port Settings

Select a Port — Port number for which you want to modify STP settings.

STP — Enables or disables STP on the port.

Fast Link — When checked, enables Fast Link mode for the port. If Fast Link mode is enabled for a port, the **Port State** is automatically placed in the **Forwarding** state when the port link is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.

Root Guard — When checked, the port is never selected as the STP root interface.

Port State — Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:

> **Disabled —** STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.

> **Blocking —** The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.

Listening — The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses.

Learning — The port is currently in the learning mode. The port cannot forward traffic however it can learn new MAC addresses.

Forwarding — The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.

Role —Indicates the port role assigned by the STP algorithm that provides STP paths. The possible field values are:

Root — Provides the lowest cost path to forward packets to root switch.

Designated — Indicates the port via which the designated switch is attached to the LAN.

Alternate — Provides an alternate path to the root switch from the root interface.

Backup — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

Disabled — Indicates the port is not participating in the Spanning Tree.

Speed — Speed at which the port is operating.

Path Cost (1-200000000) — The port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.

Default Path Cost — The default path cost. The default values for long path costs are:

Ethernet - 2,000,000

Fast Ethernet - 200,000

Gigabit Ethernet - 20,000

The default values for short path costs are:

Ethernet - 100

Fast Ethernet - 19

Gigabit Ethernet - 4I

Priority — Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 -240. The priority value is provided in increments of 16.

Designated Bridge ID — The bridge priority and the MAC Address of the designated bridge.

Designated Port ID — The designated port's priority and interface.

Designated Cost — Cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

Forward Transmission — Number of times the port has changed from the **Forwarding** state to **Blocking**.
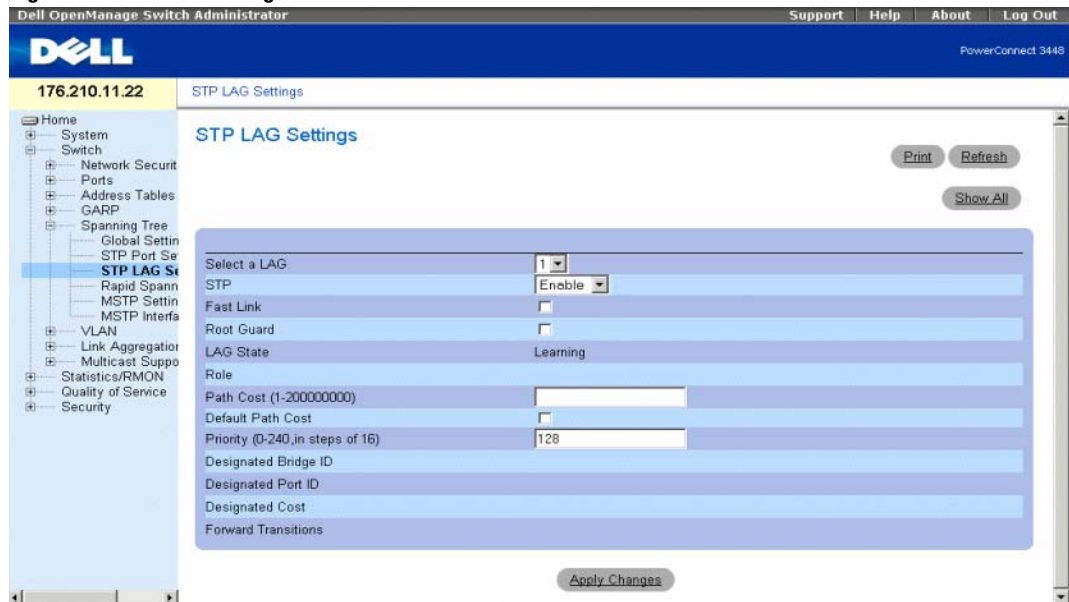
LAG — The LAG to which the port is attached.

Defining STP LAG Settings

Use the **STP LAG Settings** page to assign STP aggregating ports parameters.

To open the **STP LAG Settings** page, click **Switch → Spanning Tree → STP LAG Settings** in the tree view.

Figure 2.   STP LAG Settings

Select a LAG — The LAG number for which you want to modify STP settings.

STP — Enables or disables STP on the LAG.

Fast Link — Enables Fast Link mode for the LAG. If Fast Link mode is enabled for a LAG, the

Root Guard — When checked, the LAG is never selected as the STP root Interface.

LAG State is automatically placed in the **Forwarding** state when the LAG is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60

seconds in large networks.

LAG State — Current STP state of a LAG. If enabled, the LAG state determines what forwarding action is taken on traffic. If the bridge discovers a malfunctioning LAG, the LAG is placed in the **Broken** state. Possible LAG states are:

Disabled — STP is currently disabled on the LAG. The LAG forwards traffic while learning MAC addresses.

Blocking — The LAG is blocked and cannot be used to forward traffic or learn MAC addresses.

RSTP Discarding State — In this state the port does not learn MAC addresses and do not forward frames.

This state is union of Blocking, and Listening state introduced in STP (802.1.D).

Listening — The LAG is in the listening mode and cannot forward traffic or learn MAC addresses.

Learning — The LAG is in the learning mode and cannot forward traffic, but it can learn new MAC addresses.

Forwarding — The LAG is currently in the forwarding mode, and it can forward traffic and learn new MAC addresses.

Broken — The LAG is currently malfunctioning and cannot be used for forwarding traffic.

Role—Indicates the LAG role assigned by the STP algorithm that provides STP paths. The possible field values are:

Root — Provides the lowest cost path to forward packets to root switch.

Designated — Indicates that the via which the designated switch is attached to the LAN.

Alternate — Provides an alternate LAG to the root switch from the root interface.

Backup — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

Disabled — Indicates the LAG is not participating in the Spanning Tree.

Path Cost (1-200000000) — Amount the LAG contributes to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is being rerouted. The

path cost has a value of 1 to 200000000.

Default Path Cost — Indicates if the default path cost is used. The possible LAG path cost default values are:

    Long Method for LAG — 20,000

    Short Method for LAG — 4

Priority (0-240, in steps of 16) — Priority value of the LAG. The priority value influences the LAG choice when a bridge has looped ports. The priority value is between 0-240, in steps of 16.

Designated Bridge ID — The priority and the MAC Address of the designated bridge.

Designated LAG — The designated LAG's priority and interface.

Designated Cost — Cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

Forward Transitions — Number of times the LAG State has changed from the Forwarding state to a Blocking state.

Defining STP LAG Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for defining STP LAG settings.

Table 1-1.   STP LAG Settings CLI Commands

CLI Command	Description
spanning-tree	Enables spanning tree.
spanning-tree disable	Disables spanning tree on a specific LAG.
spanning-tree cost *cost*	Configures the spanning tree cost contribution of a LAG.
spanning-tree port-priority *priority*	Configures port priority.
spanning-tree guard root	Enables root guard on all the spanning tree instances on that interface.
show spanning-tree [**ethernet** *interface* | **port-channel** *port-channel-number*]	Displays spanning tree configuration.
show spanning-tree [**detail**] [**active** | **blockedports**]	Displays detailed spanning tree information on active or blocked ports.

The following is an example of the CLI commands:

```
console(config)# interface port-channel 1
console(config-if)# spanning-tree port-priority 16
```

Configuring LLDP

The Link Layer Discovery Protocol (LLDP) allows network managers to troubleshoot and enhance network management by discovering and maintaining network topologies over multi-vendor environments. LLDP discovers network neighbors by standardizing methods for network devices to advertise themselves to other system, and to store discovered information. Device discovery information includes:

- Device Identification
- Device Capabilities
- Device Configuration

The advertising device transmits multiple advertisement message sets in a single LAN packet. The multiple advertisement sets are sent in the packet Type Length Value (TLV) field. LLDP devices must support chassis and port ID advertisement, as well as system name, system ID, system description, and system capability advertisements.

To open the **LLDP Properties** page, click **System → LLDP → LLDP Properties** in the tree view.

Figure 1-1.   LLDP Properties
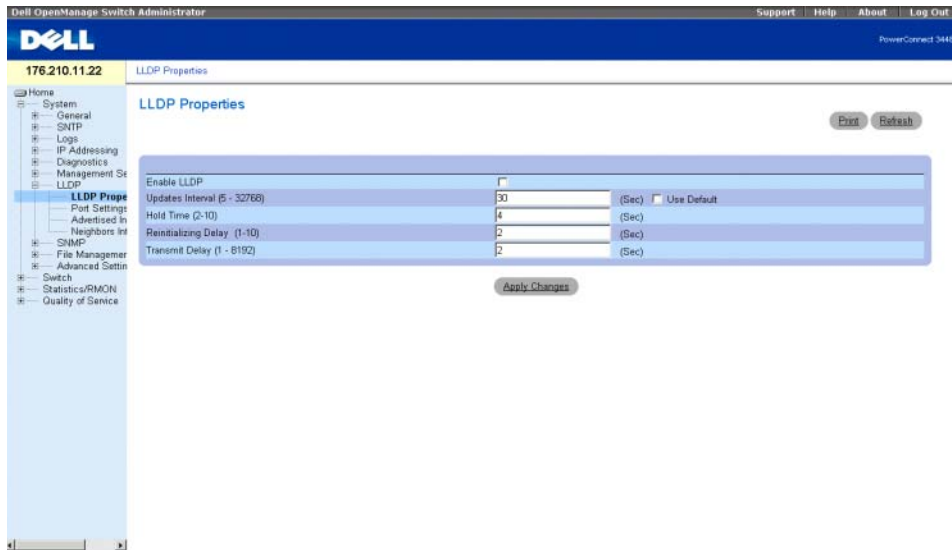
Enable LLDP — Indicates if LLDP is enabled on the device. The possible field values are:

Checked — Indicates that LLDP is enabled on the device.

Unchecked — Indicates that LLDP is disabled on the device. This is the default value.

Updates Interval (5-32768) — Indicates that rate at which LLDP advertisement updates are sent. The possible field range is 5 - 32768 seconds. The default value is 30 seconds.

Hold Time (2-10) — Indicates the amount of time that LLDP packets are held before the packets are discarded. The possible field range is 2 - 10 seconds. The field default is 4 seconds.

Reinitializing Delay (1-10) — Indicates the amount of time that passes between disabling LLDP and when reinitializing begins. The possible field range is 1 - 10 seconds. The field default is 2 seconds.

Transmit Delay (1-8192) — Indicates the amount of time that passes between successive LLDP frame transmissions due to changes in the LLDP local systems MIB. The possible field value is 1 – 8192 seconds. The field default is 2 seconds.

Configuring LLDP Using CLI Commands

The following table summarizes the equivalent CLI commands for defining LLDP.

Table 1-2.   LLDP Properties CLI Commands

| CLI Command	Description
`lldp enable (global)`	Enables enable Link Layer Discovery Protocol.
`lldp hold-multiplier` *number*	Specifies the time that the receiving device should hold a Link Layer Discovery Protocol (LLDP) packet before discarding it.
`lldp reinit-delay` *Seconds*	Specifies the minimum time an LLDP port will wait before reinitializing.
`lldp tx-delay` *Seconds*	Specifies the delay between successive LLDP frame tr.ansmissions.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# lldp enable
```

Defining LLDP Port Settings

The **LLDP Port Settings** page allows network administrators to define LLDP port settings, including the port number, the LLDP port number, and the type of port information advertised.

The **Port Settings** page contains fields for configuring LLDP.

To open the **Port Settings** page, click **System → LLDP → Port Settings** in the tree view.

Figure 1-2.   Port Settings
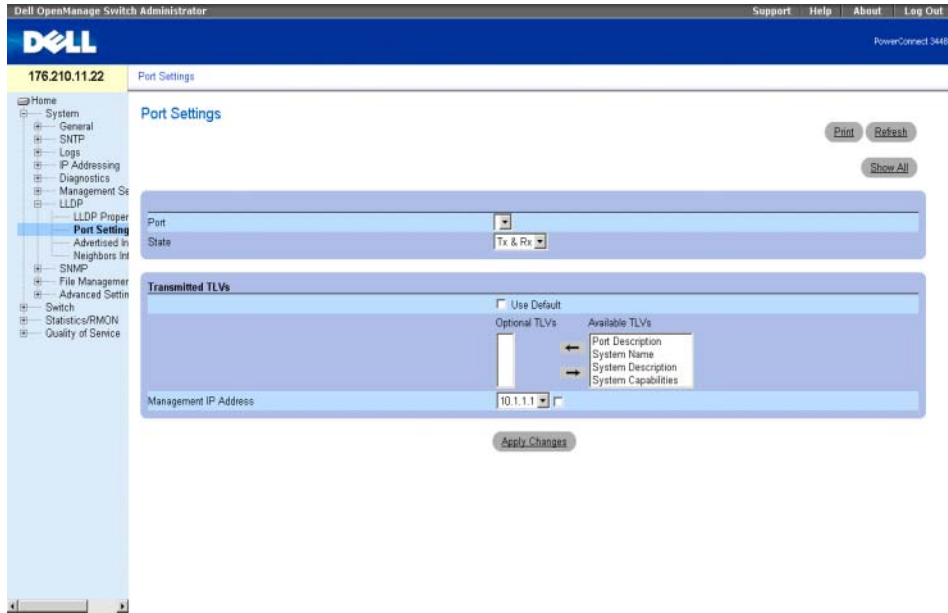
Port — Contains a list of ports on which LLDP is enabled.

State — Indicates the port type on which LLDP is enabled. The possible field values are:

> **Tx Only** — Enables transmitting LLDP packets only.

> **Rx Only** — Enables receiving LLDP packets only.

> **Tx & Rx** — Enables transmitting and receiving LLDP packets. This is the default value.

> **Disable** — Indicates that LLDP is disabled on the port.

Use Default — Indicates that information included in the TLVs is per the device defaults. The possible field values are:

> **Checked** — Enables sending the device default LLDP advertisements.

> **Unchecked** — Indicates that the device LLDP advertisement settings are disabled, and LLDP advertisement settings are user defined. This is the default value.

Optional TLVs — Contains a list of optional TLVs advertised by the port. For the complete list, see the **Available TLVs** field.

Available TLVs — Contains a list of available TLVs that can be advertised by the port. The possible field values are:

> **Port Description**— Advertises the port description.

> **System Name** — Advertises the system name.

System Description — Advertises the system description.

System Capabilities — Advertises the system capabilities.

Management IP Address — Indicates the management IP address that is advertised from the interface.

The **LLDP Port Table** page displays the LLDP Port Configuration. To open the **LLDP Port Table**, click **System → LLDP → Port Settings → Show All** in the tree view.

Figure 1-3.   LLDP Port Table

LLDP Port Table

Table 1-3.   LLDP Port settings CLI Commands

CLI Command	Description
`clear lldp rx` *interface*	Restarts the LLDP RX state machine and clearing the neighbors table
`lldp optional-tlv` *tlv1 [tlv2 … tlv5]*	Specifies which optional TLVs from the basic set should be transmitted
`lldp enable` [rx | tx | both]	To enable Link Layer Discovery Protocol (LLDP) on an interface.

The following is an example of the CLI commands:

```
Console(config)# interface ethernet 1/e5
Console(config-if)# lldp enable
```

Viewing Advertised Information

The **Advertised Information** page displays the information advertised by specific ports when advertising LLDP information.

To open the **Advertised Information** page, click **System** → **LLDP** → **Advertised Information** in the tree view.

Figure 1-4.   Advertised Information
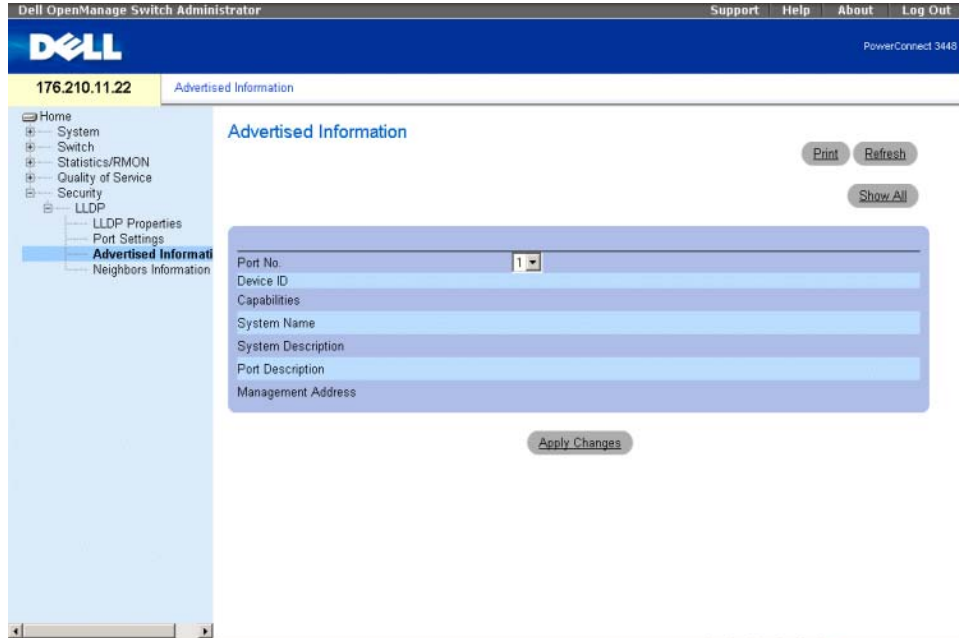
Port — Displays the port number from which the advertised information is sent.

Device ID — Displays the advertised device ID.

Capabilities — Displays the advertised device capabilities.

System Name — Displays the advertised system name.

System Description — Displays the advertised system description.

Port Description — Displays the advertised port description.

Management Address — Displays the advertised management address.

Displaying the Advertised Information Table

To open the **Advertised Information table**, click **System** → **LLDP** → **Advertised Information** → **Show All** in the tree view.

Figure 1-5.   Advertised Information Table

Advertised Information table

Table 1-4.   LLDP Advertised Information CLI Commands

| CLI Command	Description
`show lldp local` *ethernet interface*	Displays LLDP information advertised from a specific port.

The following is an example of the CLI commands:

```
Switch# show lldp local ethernet 1/e1
Device ID: 0060.704C.73FF
Port ID: 1
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex,
1000BASE-T full duplex
Operational MAU type: 1000BaseTFD
LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts
LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
```

Viewing the LLDP Neighbor Information

The **Neighbors Information** page contains information received from neighboring device LLDP advertisements.

To open the **Neighbors Information** page, click **System** → **LLDP** → **Neighbors Information** in the tree view.

Figure 1-6. Neighbors Information
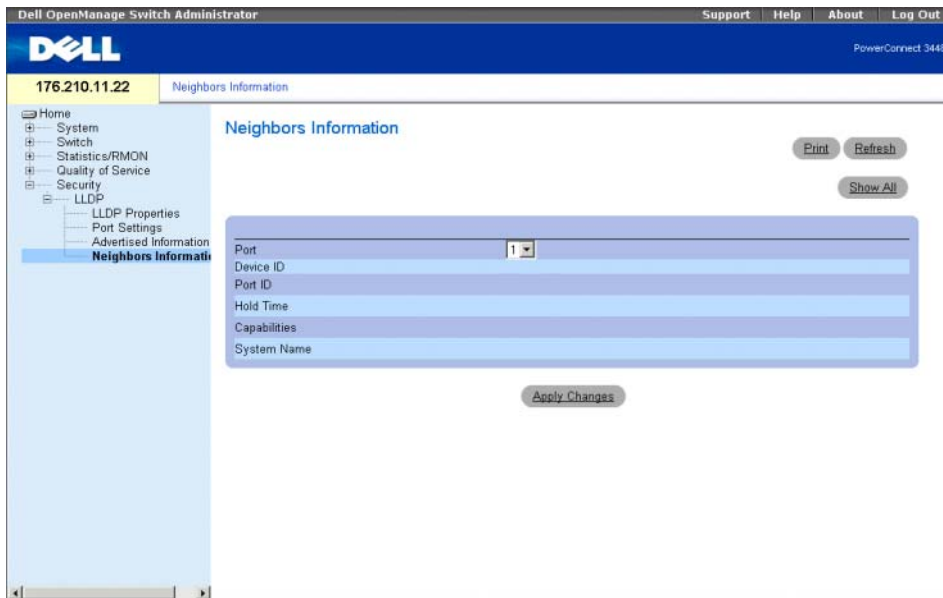
Port — Displays the neighboring port number.

Device ID — Displays the neighboring device ID.

Port ID — Displays the neighboring port ID.

Capabilities — Displays the neighboring device capabilities.

System Name — Displays the neighboring system time.

  1 Select a port.

  2 Click **Apply Changes**. The port advertisement information is displayed.

Displaying the Neighbor Information Table

  1 Click **System** → **LLDP** → **Neighbors Information** in the tree view.

  2 Click **Show All**. The **Neighbor** Table opens.

Figure 1-7.   Neighbors Table

Table 1-5.   LLDP Neighbor Information CLI Commands

CLI Command	Description
show lldp neighbors *interface*	Displays information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP)

The following is an example of the CLI commands:

Switch# **show lldp neighbors**

| Port	Device ID	Port ID	Hold Time	Capabilities	System Name
1/e1	0060.704C.73FE	1	117	B	ts-7800-2
1/e2	0060.704C.73FD	1	93	B	ts-7800-2
2/e3	0060.704C.73F C	9	1	B, R	ts-7900-1
1/e1	0060.704C.73FB	1	92	W	ts-7900-2

HTTP/HTTPS Upload/Download

Downloading Files

The **File Download from Server** page contains fields for downloading system image and Configuration files from the TFTP server to the device.

To open the **File Download from Server** page:

  1 Click **System** → **File Management**→ **File Download** in the tree view.

Figure 2.   File Download from Server
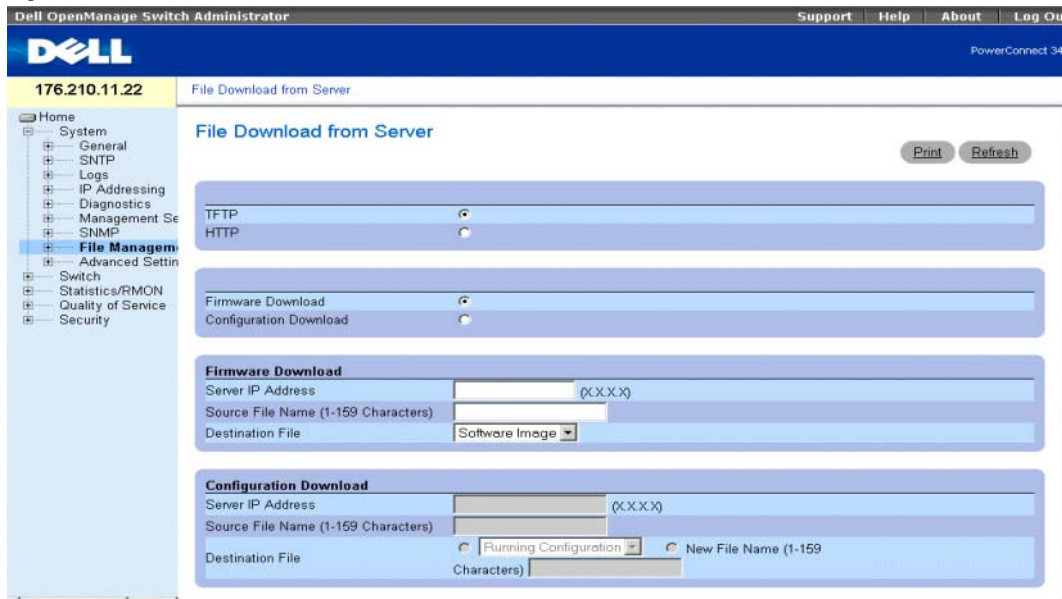
TFTP — Enables initiating an upload via the TFTP server.

HTTP — Enables initiating an upload via the HTTP/HTTPS server.

Firmware Download — The Firmware file is downloaded. If **Firmware Download** is selected, the **Configuration Download** fields are grayed out.

Configuration Download — The Configuration file is downloaded. If **Configuration Download** is selected, the **Firmware Download** fields are grayed out.

Firmware Download

  Server IP Address — The Server IP Address from which the firmware files are downloaded.

  Source File Name — Indicates the file to be downloaded.

  Destination File Name — The destination file type to which the file is downloaded. The

possible field values are:

Software Image — Downloads the Image file.

Boot Code — Downloads the Boot file.

Configuration Download

Server IP Address — The Server IP Address from which the configuration files are downloaded.

Source File Name — Indicates the configuration files to be downloaded.

Destination File Name — The destination file to which the configuration file is downloaded.

The possible field values are:

Running Configuration — Downloads commands into the Running Configuration file.

Startup Configuration — Downloads the Startup Configuration file, and overwrites it.

User Defined Backup Configuration — Downloads the user-defined Backup

Configuration file, and overwrites it.

New File Name — Downloads a new backup configuration file can be specified as the

destination file.

🖉 **NOTE:** The image file overwrites the non-active image. It is recommended to designate that the nonactive image will become the active image after reset, and then to reset the device following the download. During the Image file download a dialog box opens which displays the download progress. The window closes automatically when the download is complete.
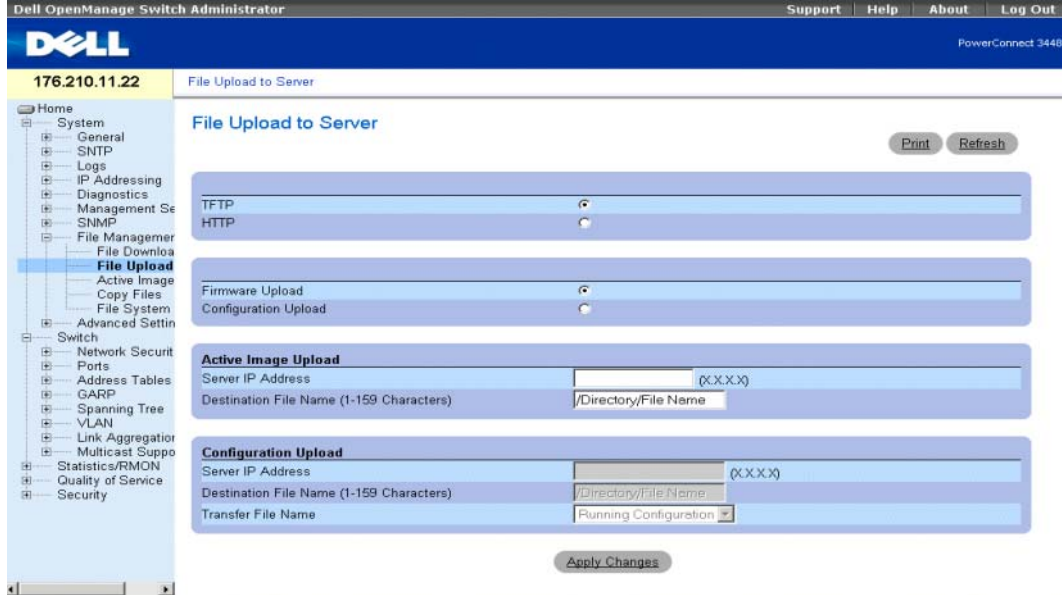
Uploading Files

The **File Upload to Server** page contains fields for uploading the software or the configuration file to the TFTP server from the device. The Image file can also be uploaded from the **File Upload to Server** page.

To open the **File Upload to Server** page:

1 Click **System** → **File Management** → **File Upload** in the tree view.

Figure 3. File Upload to Server

TFTP — Enables initiating an image upload via the TFTP server.

HTTP — Enables initiating an image upload via the HTTP or HTTPS server.

Firmware Upload — The Firmware file is uploaded to the HTTPS server. If **Firmware Upload** is selected, the **Configuration Upload** fields are grayed out.

Configuration Upload — The Configuration file is uploaded. If **Configuration Upload** is selected, the **Active Image Upload** fields are grayed out.

Active Image Upload

Server IP Address — The TFTP Server IP Address to which the Software Image is uploaded.

Destination File Name (1-159 Characters) — Indicates the Software Image file path to which the file is uploaded.

Configuration Upload

Server IP Address — The TFTP Server IP Address to which the Configuration file is uploaded.

Destination File Name (1-159 Characters) — Indicates the Configuration file path to which the file is uploaded.

Transfer File Name — The software file to which the configuration is uploaded. The possible field values are:

    Running Configuration — Uploads the Running Configuration file.

Startup Configuration — Uploads the Startup Configuration file.

List of User Defined Configuration Files — Uploads a user-defined configuration file.

NOTE: This list of user-defined configuration files only appears if the user created backup configuration files. For example, if the user copied the running configuration file to a user-defined configuration file called BACKUP-SITE-1, this list appears on the File Upload to Server page and the BACKUP-SITE-1 configuration file appears in the list.