FORCEPOINT

POWERED BY **Raytheon**

X Series™ Switch Configuration

Forcepoint™ X Series Appliance

v8.5.x

Forcepoint X Series Appliance

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

Trademarks

Forcepoint X Series™ Switch Configuration

In this guide:

Switch basics

X Series appliances come with two Dell PowerConnect M6220 switches. When used with the X10G™, each switch supports two 10Gb SFP+ ports.

Support is provided for VLAN, with optional switch high availability (A1/A2). See *Configuring VLAN and switch high availability*, page 15.

The switch ports used and their specific configuration are determined by the network type.

A Microsoft Windows hosted switch configuration tool is provided to simplify the switch configuration process.

VLAN and switch high availability

The X10G integrated 10Gb switches (A1 and A2) can be configured for both VLAN and switch high availability (HA).

Support for VLANs requires:

- A connection to an external upstream switch with one or two 10Gb trunk ports.
- A 10Gb cable to a 10Gb port on the A1 switch.
- Configuration of both switch A1 and A2 using the X Series switch configuration tool. Optionally, the switches can be configured manually by a knowledgeable administrator.
- Configuration of VLAN support on the blades.

- Configuration of the STP priority on the upstream switch, X10G switches, and blades.

Support for switch HA requires:

- Configuration of VLAN support on the blades.
- Connection of a 10Gb trunk port on both the A1 and A2 switches on the X10G chassis to one or more upstream switches.
- Configuration of the A1 and A2 switches, performed with the X Series switch configuration tool. Optionally, the switches can be configured manually by a knowledgeable administrator.

In the switch HA configuration, any one switch can be removed from service at any time for maintenance.

It is a best practice to verify that network traffic is flowing to your blade servers as expected, and if switch HA is configured, that failover works as expected.

Default switch configuration

Switches A1 and A2 arrive with the following default configuration:

Switch A1	
P1 Te1/2/1	**Enabled** 10 gigabit 1518 maximum frame size (configurable) Full duplex Auto negotiation disabled Flow control disabled
P1 Te1/2/2	**Disabled** 10 gigabit 1518 maximum frame size (configurable) Full duplex Auto negotiation disabled Flow control disabled
Other ports are not supported.	

Switch A2	
P2 Te1/2/1	**Enabled** 10 gigabit 1518 maximum frame size (configurable) Full duplex Auto negotiation disabled Flow control disabled
P2 Te1/2/2	**Disabled** 10 gigabit 1518 maximum frame size (configurable) Full duplex Auto negotiation disabled Flow control disabled
Other ports are not supported.	

Accessing a switch

To access switch A1 or A2:

1. Log on to the CMC, go to **I/O Module Overview**, and click the **Launch IOM GUI** button for switch A1 or switch A2.

   If the button isn't available, it's because an IP address has not been configured. See *Assigning switch I/O modules an IP address*, page 5.

2. A logon window displays. Log on. The Dell default credentials are: Username 'root', password 'calvin'. Change these to comply with your organization's security policies.

   The switch home screen shows the status of all ports on the switch. A green port is up (enabled), a blue port is down (disabled).

3. Click on a port to go to its configuration page.
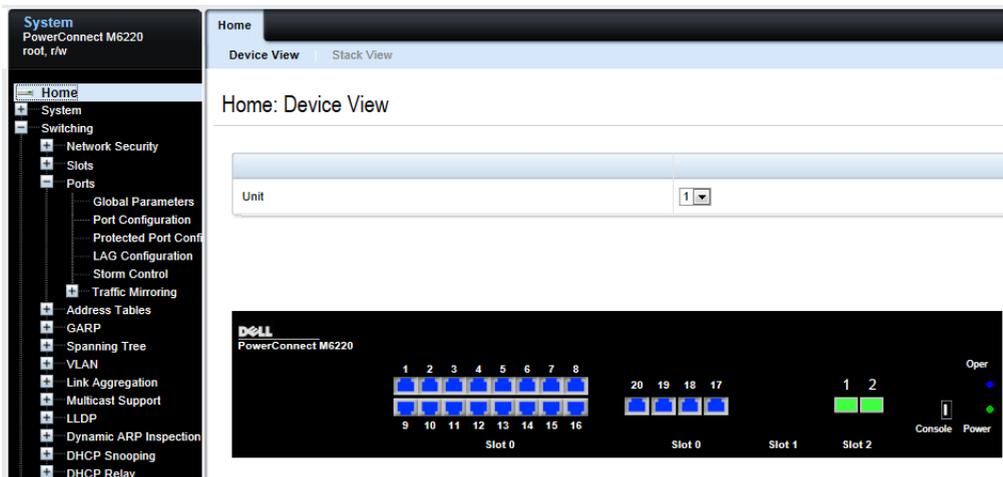
Proceed with your desired configuration changes.

For additional guides for the X10G Chassis and Security Blades, please visit the X10G support page.

Assigning switch I/O modules an IP address

Switches A1 and A2 are accessed through the Chassis Management Controller (CMC). Before they can be accessed, each must be assigned an IP address. To assign an IP address:

1. Log on to the CMC and go to **Chassis Overview > I/O Module Overview > A1 Gigabit Ethernet** (or A2).
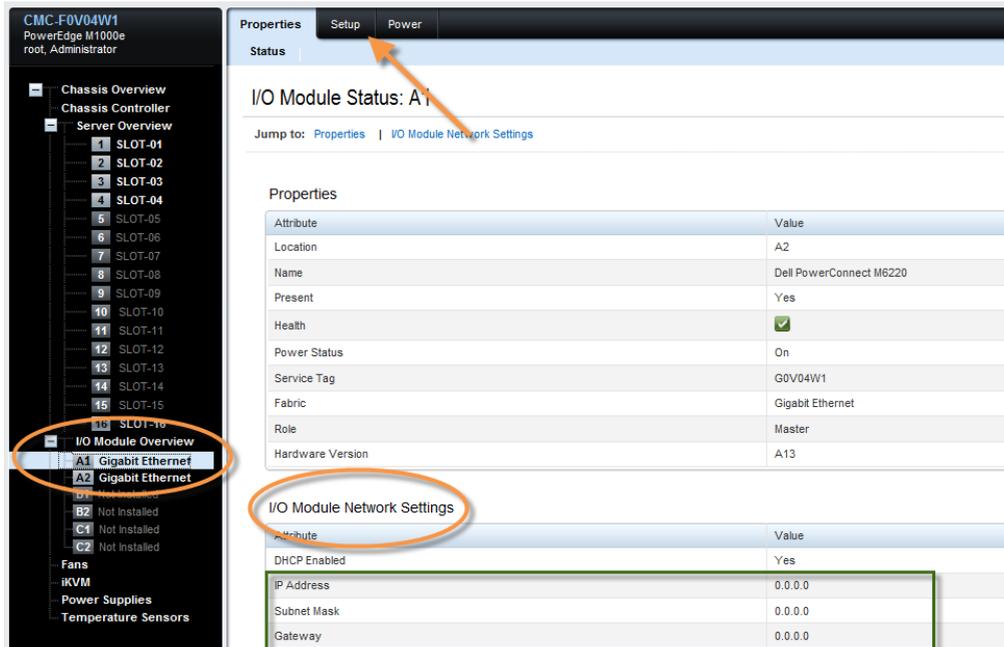
2. Click the **Setup** tab.
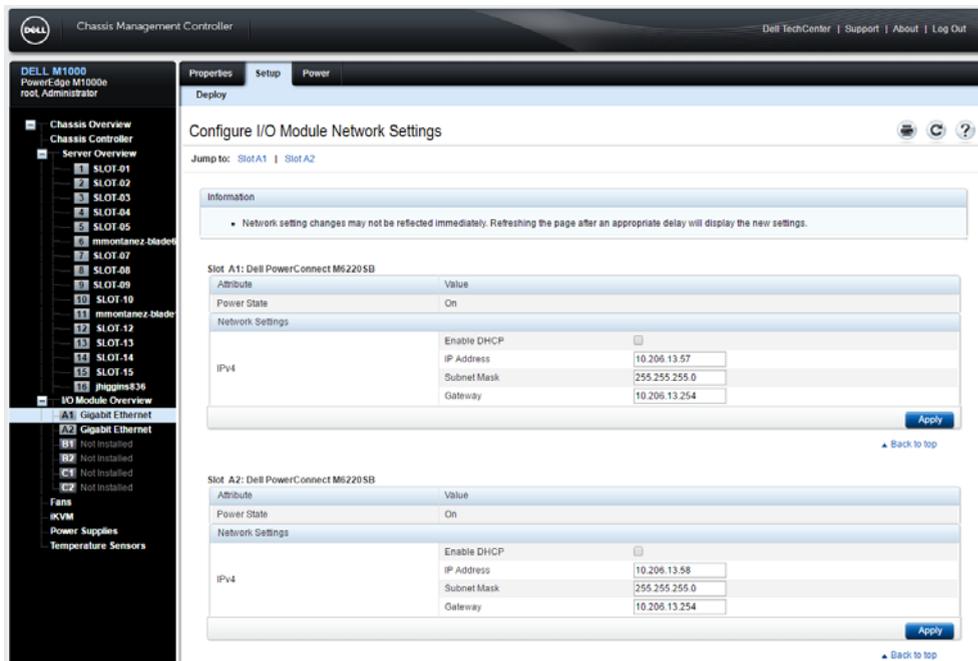
3. For each of A1 and A2, uncheck **DHCP Enabled**, and enter an IP address, subnet mask, and gateway. The IP addresses must be unique.

4. Click **Apply**. It takes a minute or 2 for the settings to be applied.

IMPORTANT: The GUI may initially indicate that the settings reverted to the previous values. Wait 2 or 3 minutes for the configuration action to complete and then refresh the page.

To access a switch, go to **Chassis Overview > I/O Module Overview** and click the **Launch IOM GUI** button corresponding to the switch you want to access.

Enabling and disabling ports

Enabling and disabling ports should not be necessary if you plan to use the provided switch configuration tool to configure the switches.

To enable or disable a port:

1. Log on to the CMC, go to **I/O Module Overview**, and click the **Launch IOM GUI** button for switch A1 or A2.

   If the button isn't available, it's because an IP address has not been configured. See the preceding section.

2. A logon window displays. Log on.
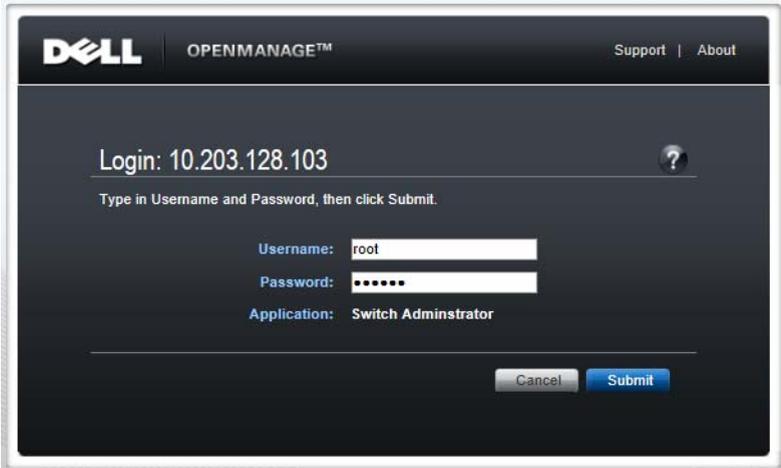
The home screen shows the status of all ports on the switch. A green port is up (enabled), a blue port is down (disabled).
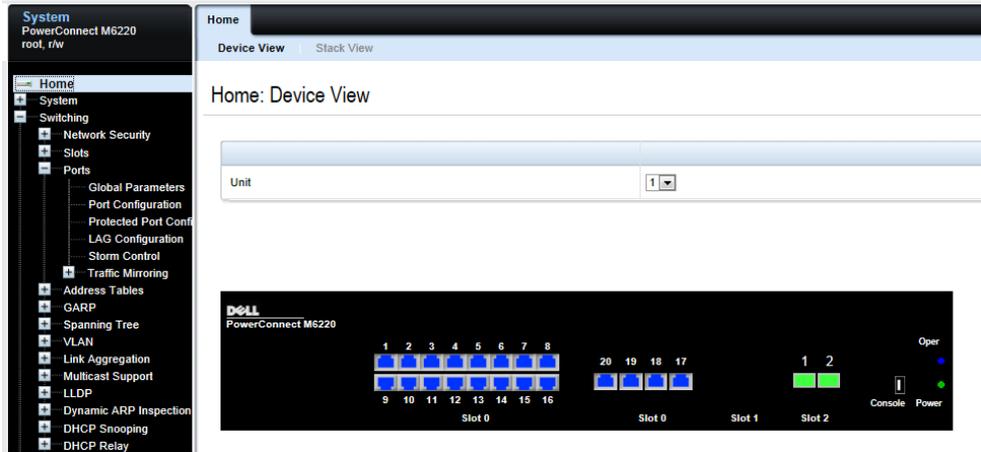
3. To enable or disable a port, click on the green or blue area of the port. This opens the **Port Configuration: Detail** page.
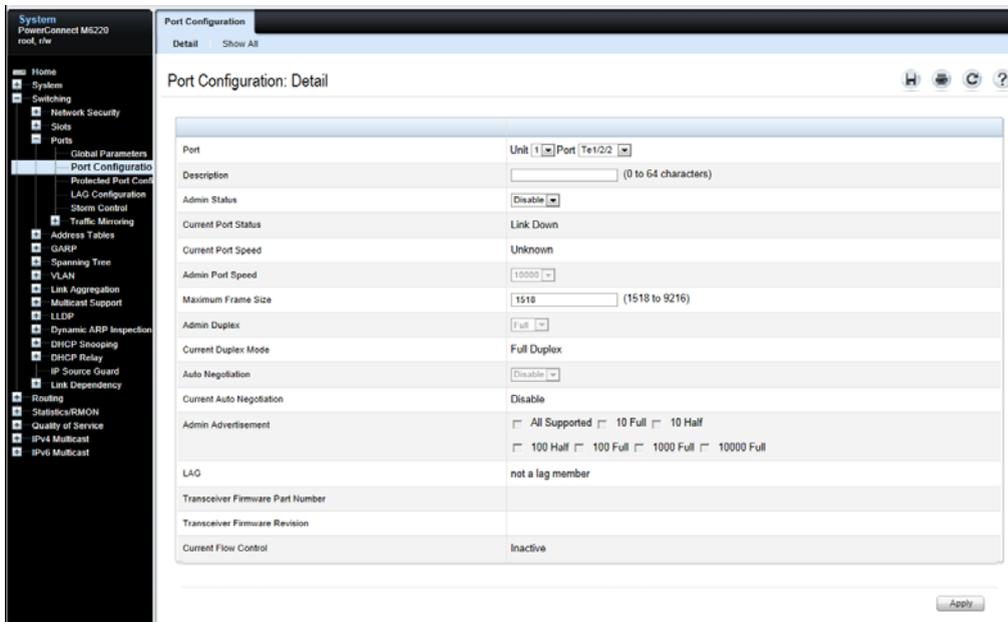
a. Confirm that the **Port** selection is correct. Change to another port if desired.

b. Add a description if desired.

c. Select **Enable** or **Disable** from the **Admin Status** drop down. This determines if the port is enabled or disabled.

d. Examine and adjust other settings as needed and click **Apply**.

   IMPORTANT: The UI may initially indicate that the settings reverted to the previous values. Wait 2 or 3 minutes for the configuration action to complete and then refresh the page.

Stacking Modules

Notes

- To avoid a potential network loop, remove all cables from both switches.
- Be sure to save all running-config to startup-config.
- Be sure to set root and enable password after configuration.
- LACP guidelines:
    - LACP should be reconfigured on both sides of the link.
    - The interfaces on either side of the link should be set to the same speed.

Configuring switches from factory default configuration

1. Insert stacking module into Module Bay 1.

2. Insert switches into A1 and A2.
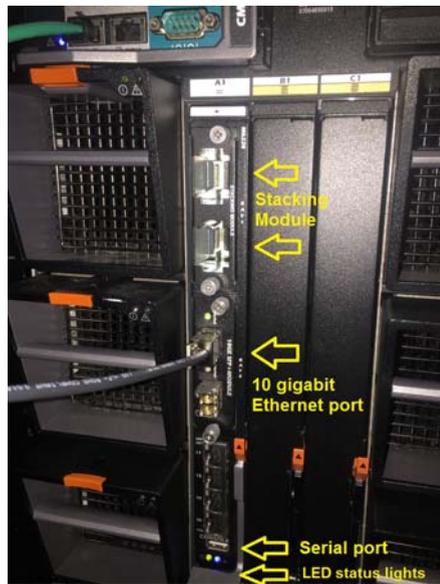
3. Connect switch cables:

   a. Connect A1-xg1 with A2-xg2.

   b. Connect A1-xg2 with A2-xg1.

4. Wait a few minutes and then use one of the following methods to determine which switch is the M6220 stack master switch:

   a. Identify the master switch by the blue illuminated LED just below the serial console connector.

b. SSH to CMC and run the following command.

```
$ getioinfo
<IO>      <Name>                    <Type>              <Presence>   <POST>    <Power>   <Role>
Switch-1  Dell PowerConnect M6220SB  Gigabit Ethernet   Present      OK        ON        Member
Switch-2  Dell PowerConnect M6220SB  Gigabit Ethernet   Present      OK        ON        Master
Switch-3  N/A                        None                Not Present  N/A       N/A       N/A
Switch-4  N/A                        None                Not Present  N/A       N/A       N/A
Switch-5  N/A                        None                Not Present  N/A       N/A       N/A
Switch-6  N/A                        None                Not Present  N/A       N/A       N/A
```

c. Check the **Role** column in the **I/O Module Status** table in CMC Web UI management.

			Properties	Setup	Power	Troubleshooting	Update

Status

I/O Modules Status

Slot	Health	Fabric	Name	Launch IOM GUI	Role	Power Status	Service Tag
A1	☑	Gigabit Ethernet	Dell PowerConnect M6220SB		Master	On	400N6S1
A2	☑	Gigabit Ethernet	Dell PowerConnect M6220SB		Member	On	DG2N6S1
B1							
B2							
C1							
C2							

5. Connect to the master switch. From a CMC SSH session, use the "connect switch-1" or "connect switch-a1" command.

> **Note**
>
> To connect to the member switch, use the "connect switch-2" or "connect switch-a2" command from a CMC SSH session. If you are connected to the member switch, the console will print the following message.
>
> ```
> Unit 2 - CLI unavailable - please connect to
> master on Unit 1
> ```

a. Configure spanning-tree (default value is 32768; priority is 57344).

b. Add VLAN information (depending on customer environment).

```
console#config
console(config)#vlan 4000
console(config-vlan4000)#name example
console(config-vlan4000)#exit
console(config)#
```

c. Run the following command for interfaces 1-16 on both switches.

```
console#config
console(config)#spanning-tree priority 57344
console(config)#interface range gigabitethernet 1/0/1-16
console(config-if)#spanning-tree guard root
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan all
```

```
console(config-if)#exit
console(config)#interface range gigabitethernet 2/0/1-16
console(config-if)#spanning-tree guard root
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan all
console(config-if)#exit
console(config)#exit
console#write
This operation may take a few minutes.
Management interfaces will not be available during this
time.
Are you sure you want to save? (y/n) y
Configuration Saved!
```

    d. Shut down reserved external interfaces (17-20)

```
console#config
console(config)#interface range gigabitethernet 1/0/17-20
console(config-if)#shutdown
console(config-if)#exit
console(config)#interface range gigabitethernet 2/0/17-20
console(config-if)#shutdown
console(config-if)#exit
console(config)#exit
console#write
This operation may take a few minutes.
Management interfaces will not be available during this
time.
Are you sure you want to save? (y/n) y
Configuration Saved!
```

    e. Create a port channel.
       In the example below, the uplink ports are 10 gigabit Ethernet ports 1/2/1
       and 2/2/1. They use dynamic LAG (static command is "channel-group 1
       mode on), which is consistent with the other side ports of the uplink
       switch.

```
console#config
console(config)#interface tengigabitethernet 1/2/1
console(config-if-Te1/2/1)#channel-group 1 mode active
console(config-if-Te1/2/1)#exit
console(config)#interface tengigabitethernet 2/2/1
console(config-if-Te2/2/1)#channel-group 1 mode active
console(config-if-Te2/2/1)#exit
console(config)#interface port-channel 1
console(config-if-Po1)#spanning-tree  disable
```

```
console(config-if-Po1)#switchport mode trunk
console(config-if-Po1)#switchport trunk allowed vlan all
console(config-if-Po1)#exit
console(config)#exit
console#write
This operation may take a few minutes.
Management interfaces will not be available during this
time.
Are you sure you want to save? (y/n) y
Configuration Saved!
```

Adding stacking module to current environment

If you have already deployed the X10G appliance and want to add stacking modules into the current environment, follow these steps.

1. Set up LACP on uplink switch-related ports.
2. Insert stacking module and connect stack cable.
3. Wait a few minutes and connect to master switch.
4. Configure port channel. See *Configuring switches from factory default configuration*, Step 5d.

Configuring switches to remove the stacking module

1. Remove stacking modules from A1 and A2.
2. Connect to physical serial port of each switch.
3. Remove all links from both switches.
4. Restart switches and reset to factory default setting, or delete startup-config and then reload switch without saving running-config.
5. If the switch number is not set to 1, reset it to 1 manually.

```
$ connect switch-a2
connect: acquiring remote port.
Connected to remote port.
Escape character is '^\'.

console>
console>en

console#show switch

    Management Standby   Preconfig     Plugged-in    Switch        Code
SW  Status    Status     Model ID      Model ID      Status        Version
--- --------- ---------  ------------- ------------- ------------- -----------
2   Mgmt Sw              PCM6220       PCM6220       OK            4.2.2.3

console#config

console(config)#switch 2 renumber 1
```

6. Use current switch configuration tool to set up both switches.
7. Update uplink switch configuration to remove LACP.

Configuring VLAN and switch high availability

Configuring for VLAN and switch HA requires:

- One or two external upstream switches with 10Gb trunk ports configured
- *VLAN Enabled: Cabling the switches*, page 15 (next section)
- Configuration of A1 and A2 with the *X10G switch configuration tool*, page 20
- *Configure VLAN support on the blades*, page 16
- *Deployment and test steps to avoid a network loop*, page 16

VLAN Enabled: Cabling the switches

Chassis switch cabling
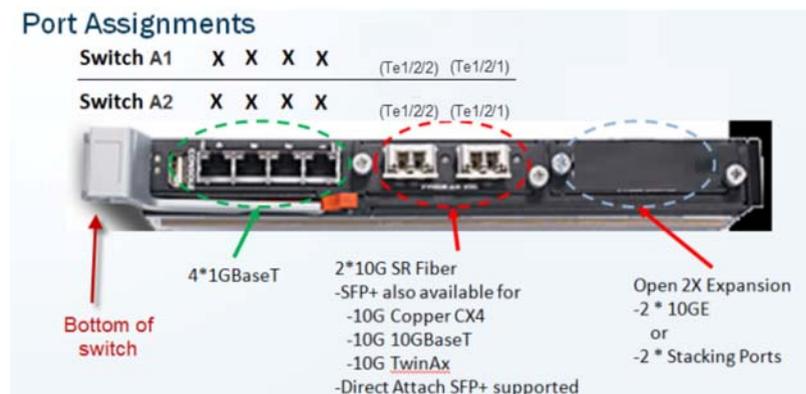
The primary port is A1 Te1/2/2 (the lower 10Gb port; P1).

The secondary port, for optional switch high availability, is A2 Te1/2/2 (P2).

With 10Gb ports use SFP+ cables.

When VLAN is enabled, after running the X10G switch configuration tool, P1 and P2 are configured as trunk ports.

> **Important**
> In the X10G switch configuration tool, when prompted for the external port, select the option for **Te1/2/2**.

When cabling is complete, configure the switch with the *X10G switch configuration tool*, page 20.

Upstream switch configuration

Cable appropriately to the upstream switch.

Upstream 10Gb ports should be in **trunk** mode.

Enable spanning tree on the ports. The mode can be STP, RSTP, MSTP, or PVST.

Designate one upstream switch as the root bridge by assigning it a priority number lower than the X10G switches.

- ■ Pre-8.0: the default setting is 32768 on both M6220 switches and the blades
- ■ 8.0 and higher: the default setting is 57344 on the switches and 61440 on the blades.

Configure VLAN support on the blades

After configuring the switch to recognize VLAN traffic and direct it appropriately, configure VLAN support on each blade.

> **Important**
> Once you have assigned a VLAN to any appliance interface, returning the appliance to a VLAN-unaware (no VLAN) state requires reimaging the blade.
>
> You can, however, reassign the VLAN ID with the 'set interface vlan' command, described below.

With new installations, you are offered the option to assign a default VLAN to interface P1 as part of the **firstboot** script.

For upgrades from VLAN-unaware configurations, or to add VLAN support after installation, use the appliance CLI as follows:

1. Connect to the blade that you want to configure, and log on as **admin**.
2. Enter **config** mode and enter the admin password when prompted.
3. Use the **set interface vlan** command to assign a VLAN ID to the first interface. For example:

   ```
   set interface vlan --interface p1 --vid 400
   ```
4. Use the **set interface vlan** command to assign a VLAN ID to the second interface. For example:

   ```
   set interface vlan --interface p2 --vid 1025
   ```
5. When you are finished, use the **show interface info** command to review the updated configuration.

Deployment and test steps to avoid a network loop

When deploying the X10G in a VLAN with high availability, to avoid introducing a network loop, configure the devices and test the configuration in careful steps. Include a network engineer in the configuration and testing of the switches.

Before making any changes, ensure that you have accurate documentation of the current network configuration, as well as the planned, finished configuration.

You should know:

1. The active and planned STP protocols.

2. The active and planned STP priority of each switch.

Supported STP protocols include:

- RSTP - The default protocol on the X10G Dell M6220 switches.
- MSTP - Document the STP priority on each VLAN, including the STP management VLAN. Know the STP priority of each VLAN allowed through the trunk interface.
- PVST* - Document the STP priority on each VLAN, including the STP management VLAN, typically VLAN 1. *If you plan to deploy PVST, it is recommended that you contact Technical Support to review planning and configuration steps.

Recommended configuration and deployment steps.

1. Ensure that the external switch has a lower priority number than the X10G switches (lower than the Dell M6220 default setting).

   - Pre-8.0: the default setting is 32768 on both M6220 switches and the blades
   - 8.0 and higher: the default setting is 57344 on the switches and 61440 on the blades.

2. Ensure that all X10G blade switch interfaces are configured with STP enabled and have root guard enabled. Switch interfaces Gi1/0/1-16 should have a configuration similar to:

```
interface Gi1/0/1
spanning-tree guard root
switchport mode trunk
switchport trunk allowed vlan 869
exit
```

3. Until STP and networking are confirmed working, shut down all but one of the blade interfaces. This limits the amount of network loop traffic generated if something goes wrong.

4. Connect only one 10Gb interface at a time to the external switch. Make sure that the other M6220 10Gb interface is either physically disconnected or in an admin shutdown state. This prevents the possibility of a network loop while STP testing is performed.

5. Configure the 10Gb trunk interface on both the external switch and the M6220 switch, and bring them up.

   If all VLANs are not being allowed in the configuration, it is recommended to manually add VLAN 1 to the allowed VLANs on the trunk on the external port. VLAN 1 is typically the management non-tagged VLAN that carries STP BPDU traffic between the switches. The M6220 automatically detects that VLAN 1 has been added.

6. When the trunk is up, test that STP is working correctly.

   a. Log on to the M6220 and run:

   ```
   show spanning-tree detail
   ```

   If spanning tree is working correctly:

   ○ The external switch root's MAC address is listed in the ROOT ID Address

   ○ One of the 10Gb interfaces is listed as the Root Port.

   b. Check to see if BPDU packets are being sent and received on the uplink port to the external switch. To do this, after running the "show spanning-tree detail" command, scroll down to the Ten Gig Ethernet interfaces such as Te1/2/1 or Te1/2/2. In the screen capture you can see that BPDU packets are being sent and received. The interface is also designated as the "root" and is in a "forwarding" state.

   c. Use "ping" and "ssh" (if enabled on the blade) to test connectivity to the enabled blade.

   If after running "show spanning-tree detail" you see the message "This Switch is the Root", there is a configuration problem. Do not proceed to the next step until you can get the trunk and STP up and confirmed talking with BPDU packets.

7. After the first switch is configured and confirmed to be using STP correctly, shut down that 10Gb interface and bring up the other switch's 10Gb interface. Follow the same steps as above until networking and STP function are confirmed working.

8. Confirm that STP functionality is working all the way through to the blade's Open Vswitch (OVS). To do this safely, with one of the switches up, connect with "ping" to the blade. Then shut down the switch port that is up and bring up the other switch port.

   If this test is successful, you know that STP is working all the way through to the blade.

9. It is now safe to enable both Dell 6220 switch uplink ports to the switches. Start with only one blade interface enabled.

10. Monitor CPU traffic on the switches. If there are any heavy spikes, immediately shut down one of the uplink interfaces.

Setting the STP priority on an X10G blade

Blades running v8.1.0 and higher

1. Log on to the blade's CLI and enter **config** mode.
2. Use **show vswitch priority** to see the current STP priority setting.
3. Use **set vswitch <priority_value>** to set the STP priority value. Specify an integer in the range 4096-61440.

Blades running v8.0.x and lower

With the assistance of Technical Support, acquire access to the blade's base operating system.

Edit the network bridge interface network script:
/etc/sysconfig/network-scripts/ifcfg-ovsbr0

The STP priority value is specified in hexadecimal.

In version 7.8.4 the default STP priority value is 32768 (0x8000).

In version 8.0.0, the default value is 61400 (0xF000). Make sure the upstream switch has a lower priority number than this value.

Some examples of valid STP priorities that are lower than 32768 include:

```
0xA000 = 40960
0xE000 = 57344
0xF000 = 61440
```

The value to change is in bold face in the configuration file example below.

```
# cat /etc/sysconfig/network-scripts/ifcfg-ovsbr0
HOTPLUG=no
BOOTPROTO=none
DEVICETYPE=ovs
DEVICE=ovsbr0
OVS_EXTRA="set Bridge $DEVICE stp_enable=true -- set Bridge
$DEVICE other_config:stp-priority=0xA000"
TYPE=OVSBridge
ONBOOT=yes
```

How OVS works within the blade
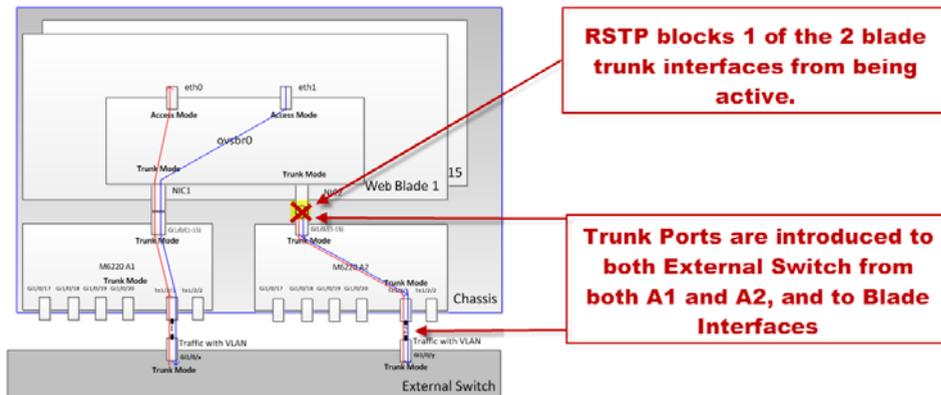
X10G switch configuration tool

The switch configuration tool allows you to rapidly and accurately configure the X10G switches to support either:

- VLAN with switch high availability
- No VLAN (VLAN-unaware); no support for high availability

Before you begin, download the switch configuration tool to a Windows machine in your network. The Windows machine must be able to connect to the appliance CMC via a web browser. To download the switch tool:

1. Open a browser and go to My Account.
2. Log in when prompted, then select the **Downloads** tab.
3. Select X10G Base Configuration from the Product drop-down list, then select **8.2.x** from the Version list.
4. Click the **download** link for the **Switch Configuration Tool**.
5. When the download is complete, extract the archive to a temporary directory.

Using the tool requires:

- The CMC IP address
- The CMC root password
- If set on either of the switches, the Enable password (not set, by default)

To configure the switch:

1. Use the CMC manager to verify that SSH connections are enabled on the **Chassis Overview > Network > Services** page under **SSH Configuration**.
2. Navigate to the Windows folder containing the switch configuration tool, and double-click **switch-tool.exe** to launch the tool.

3. When prompted, enter the **CMC IP address**.

4. Enter **root** as the **CMC user name**, followed by the root password.

5. If an Enable password has been set (not set, by default), enter the **Enable password for switch A1**, followed by the **Enable password for switch A2**.

```
Welcome to the X Series switch tool, used to configure the Dell M6220 switches
on the X10G Appliance.

Version: 8.4.0


Enter the CMC IP address: 10.206.13.60
Enter the CMC root password: ************
```

The switch tool displays the current running configuration for switch A1, followed by the configuration for switch A2. For example:

```
Show running configuration for switch a1:

Port            Status          Mode        Vlan
--------        ----------      ------      --------------------
Gi1/0/1                         access      1
Gi1/0/2                         access      1
Gi1/0/3                         access      1
Gi1/0/4                         access      1
Gi1/0/5                         access      1
Gi1/0/6                         access      1
Gi1/0/7                         access      1
Gi1/0/8                         access      1
Gi1/0/9                         access      1
Gi1/0/10                        access      1
Gi1/0/11                        access      1
Gi1/0/12                        access      1
Gi1/0/13                        access      1
Gi1/0/14                        access      1
Gi1/0/15                        access      1
Gi1/0/16                        access      1


Gi1/0/17        shutdown        access      1
Gi1/0/18        shutdown        access      1
Gi1/0/19        shutdown        access      1
Gi1/0/20        shutdown        access      1
Te1/2/1                         access      1
Te1/2/2         shutdown        access      1

----------------------------------------------------------------
STP status: off
STP protocol:
Bridge ID: 32768:D067.E57D.97B2
================================================================
```

6. Select the X10G external port that is connected to your third-party upstream switch. Use option 5 or 6 for VLAN enabled.

```
Select the external port that is connected to the upstream switch:

 1. Gi1/0/17
 2. Gi1/0/18
 3. Gi1/0/19
 4. Gi1/0/20
 5. Te1/2/1
 6. Te1/2/2

You have entered:   6_
```

7. When prompted to select a deployment option, enter option **1** to enable VLAN support and switch high availability, or option **2** to leave the switch in No VLAN (not VLAN-aware) mode.

```
Select the option that best describes your deployment. Both options are
supported with both Web and Email modes.

1. The chassis or blades are VLAN-aware. The port of the upstream switch
   that is connected to the A1/A2 external port is set to trunk mode to
   support VLAN use and high availability.

2. The chassis and blades are not VLAN-aware. The port of the upstream switch
   that is connected to the A1/A2 external port is set to access mode, and
   does not support VLAN.

You have entered option:
```

8. If you selected option **1**:

    a. Enter the STP priority value for the switches. The recommended value is 57344 (and 61440 on the blades). The STP priority value you set on the upstream switch must be lower (with the effect of making it the root).

    b. You are prompted to configure VLAN settings for one or more blades.

    To start, enter the blade number or numbers in a comma-separated list (1,2,3), range format (1-3), or a combination (1,2, 5-8).

    ○ All of the selected blades will receive traffic for the same VLAN or VLANs.

    ○ After configuring the first blade or set of blades, you will be given the option to configure additional sets of VLAN settings for your remaining blades.

    c. Enter the **VLAN ID** or IDs to configure the traffic that will be directed to the selected blades. VLAN IDs can be entered in a comma-separated list (100,101,102), range format (100-102), or a combination.

    Each blade supports a maximum of 3 VLANs.

    d. If you have additional blades to configure, enter **yes**, and repeat steps a and b.

    When you are finished, enter **no** to continue with the next step.

    e. Specify whether to perform a full factory reset before reconfiguring each switch, then review the configuration settings displayed. There is no need to perform a factory reset unless you know there is a problem with the switch configuration.

9. If the new settings look correct, enter **1** to start the switch reconfiguration process.

    Progress information is displayed as first switch A1, then switch A2, is configured.

    The switch reconfiguration process should take only a few minutes.

10. When the switch reconfiguration is complete, press any key to exit the switch configuration tool.

If you have configured for VLAN support, ensure that your upstream switch is configured to send VLAN traffic to the X10G, and then configure individual blades to

recognize VLAN traffic. See *Configure VLAN support on the blades*, page 16, for instructions.

Setting up a mirror port on an X10G appliance

In X Series appliances with the switch configuration port installed, you can use the CLI or the API to enable the Decryption Port Mirror feature with the N interface as an SSL mirror port.

1. Power off the X10G blade.
2. Remove and open the blade.
3. Insert the network module into the blade at the B position.
4. Place the blade back into the chassis.
5. Insert the pass-through module into the B1 position of the chassis.

Connect the network cable to the number *n* port of the pass-through module in the B1 position.

Installing a new switch

If you must replace a switch:

1. Contact Forcepoint Technical Support for assistance.
2. When replacing the switch make certain that it is fully seated in the chassis, and that the switch lever is latched.
3. During the replacement procedure, ask the Technical Support specialist to demonstrate that the new switch is functioning properly, per your switch configuration requirements.