CHAPTER 14

Discrepancies and Best Practices Deviations

The Discrepancies Reporting module of LMS allows you to view the discrepancies and best practices deviations in your network. This chapter contains the following:

Understanding Discrepancies and Best Practices Deviations

LMS provides reports on discrepancies, such as network inconsistencies and anomalies or misconfiguration in the discovered network. This makes it easy to identify configuration errors such as link-speed mismatches on either end of a connection. Discrepancies are computed at the end of each data collection schedule.

LMS also reports Best Practices Deviations. These are variations from the normal or recommended practices in a network. These do not have any serious impact on the functioning of the network.

LMS allows you to:

- View Reports on Discrepancies. Select **Reports > Fault and Event > Best Practices > Discrepancies**.
- View Reports on Best Practices Deviations. Select **Reports > Fault and Event > Best Practices > Deviation**.
- Acknowledge Discrepancies.
- Acknowledge Best Practices Deviations.
- Resolve Discrepancies and Best Practices Deviations.
- Customize Discrepancies Reporting. For details, see Customizing Discrepancies Reporting and Syslog Generation.

Fixing Discrepancies and Best Practices Deviations through LMS

The following Discrepancies can be fixed through LMS:

- Link Duplex Mismatch
- Link Speed Mismatch
- Link Trunk/NonTrunk Mismatch
- Port Fast Enabled on Trunk Port

The following Best Practices Deviations can be fixed through LMS:

- BPDU Filter Disabled on Access Ports
- BPDU-Guard Disabled on Access Ports
- Loop Guard and Port Fast Enabled on Ports
- UDLD Disabled on Link Ports
- CDP Enabled on Access Ports
- High Availability not Operational

Interpreting Discrepancies

This section contains information on each of the discrepancy reported in LMS. It describes the discrepancy, the impact it has on the network, and ways to resolve it.

The user interface in LMS displays commands you can use to make configuration changes on devices to resolve discrepancies.

This section contains:

- Trunking Related Discrepancies
- VLAN-VTP Related Discrepancies
- Link Related Discrepancies
- Port Related Discrepancy
- Device Related Discrepancy
- Spanning Tree Related Discrepancy

Trunking Related Discrepancies

The trunking related discrepancies that LMS reports are:

- Trunk Negotiation Across VTP Boundary
- Native VLANs Mismatch
- Trunk VLANs Mismatch
- Trunk VLAN Protocol Mismatch

Trunk Negotiation Across VTP Boundary

LMS reports a discrepancy when the trunk mode on any end of the trunk link is set to Auto or Desirable.

Dynamic Trunking Protocol (DTP) cannot be used for trunk negotiation across VTP domain boundary. This occurs when trunk mode on both sides has any of the following combinations:

- On/Auto
- On/Desirable
- Desirable/Auto
- Desirable/Desirable
- Off/Desirable

Impact

Trunk negotiation across VTP boundary (that is, trunk link connecting two devices that are part of different VTP domains) fails.

Fix

You cannot fix this discrepancy using LMS.

To fix the discrepancy on switches using Cisco IOS:

Step 1 Make sure that the Trunk mode is ON, on both sides of the link.

Step 2 Enter the following command:

switchport trunk encapsulation *dot1q* | *isl*

switchport mode trunk

end

Step 3 Enter the following command to check the status:

show interfaces trunk

Or

show interface *mod interface_id* **trunk**

To fix the discrepancy on switches using Catalyst operating system:

Step 1 Make sure that the Trunk mode is ON, on both sides of the link.

Step 2 .Enter the following command:

set trunk *mod/port* **on Dot1Q** | **ISL**

Step 3 Enter the following command to check the status:

show trunk *mod/port*

Native VLANs Mismatch

LMS reports a discrepancy when the native VLANs of all ports in a trunk do not match.

This mismatch occurs when you have created a trunk port to connect another switch, and both ends are in different native VLANs.

Note This discrepancy is applicable only for trunks that use 802.1q encapsulation.

Impact

The native VLAN must match on both sides of the trunk link, otherwise the traffic flow across the link is affected. The trunk continues to remain operational.

Fix

If you have altered the default native VLAN configuration, ensure that all trunks have the same native VLAN. Use the **`set vlan`** command for Cisco Catalyst operating system switches or the **`switchport trunk native vlan`** command for Cisco IOS switches to specify the native VLAN.

You cannot fix this discrepancy through LMS.

Trunk VLANs Mismatch

LMS reports a discrepancy when the list of active or allowed VLANs between the two ends of a trunk do not match.

Impact

The trunk remains operational but the network traffic across the link is affected.

Fix

You can resolve this by modifying the list of allowed VLANs between the two ends of a trunk and ensuring that there is no mismatch. You cannot fix this discrepancy through LMS.

Trunk VLAN Protocol Mismatch

LMS reports a discrepancy when different trunk encapsulations are set on the two ends of a trunk.

For example, when one end of a trunk is configured as ISL and the other as 802.1q, LMS reports a discrepancy.

ISL and 802.1q are the different encapsulation types that you can configure in a trunk VLAN.

Impact

The trunk remains operational when the trunk mode is set to **On** or **No-negotiate** with mismatching encapsulation types. However, the network traffic across the link is affected because of the mismatch.

Fix

Configure the same encapsulation type on both ends of the trunk. You cannot fix this discrepancy through LMS.

VLAN-VTP Related Discrepancies

The VLAN-VTP related discrepancies that LMS reports are:

- VTP Disconnected Domain
- No VTP Server in Domain with at least One VTP Client

VTP Disconnected Domain

LMS reports a discrepancy if the devices that are part of the same VTP domain have different VTP configuration revision numbers. When a switch in the same VTP domain has a higher configuration revision number compared to the other switches, it could overwrite your server-configured switch with incorrect information.

Impact

The VLAN information is not dynamically shared across the VTP domain.

Fix

Ensure that you configure VTP Configuration Revision number consistently across devices of the same VTP domain. You cannot fix this discrepancy through LMS.

No VTP Server in Domain with at least One VTP Client

LMS reports a discrepancy when there is no VTP Server configured in a VTP domain.

You can configure a switch to operate in any one of these VTP modes—Server, Client, Transparent, and Off. Primary and secondary servers are two types of servers that may exist on an instance in the VTPv3 domain.

A VTP client cannot store VLAN information. When a VTP client boots, it needs to reacquire the entire configuration that is propagated by VTP.

The primary server can initiate or change the VTP configuration. The main purpose of a VTP secondary server is to back up the configuration that is propagated over the network.

Impact

LMS reports a discrepancy when an existing VTP server or primary server goes down and there is no alternative or backup server.

This can occur in a VTPv2 or VTPv3 domain that has only client mode devices. This could happen when the existing primary server or server mode device has gone down temporarily and if the server mode device does not come up.

If you do not configure at least one server, the devices become unreachable. LMS discovers only the client-mode devices in the domain and ignores the rest.

Fix

Configure at least one device as server in a VTP domain. If the device you have configured as server is temporarily down, configure another device as server. You cannot fix this discrepancy through LMS.

For more information on VTP domain, see the document *Configuring VTP* at the following location:

http://www.cisco.com/en/US/products/hw/switches/ps708/prod_eol_notices_list.html

Link Related Discrepancies

The link related discrepancies that LMS reports are:

- Link Duplex Mismatch
- Link Speed Mismatch
- Link Trunk/NonTrunk Mismatch

Link Duplex Mismatch

LMS reports a discrepancy when there is a duplex mismatch between links.

Duplex mismatch on 10/100Mb Ethernet links occurs when one port on the link is operating at half-duplex while the other port is operating at full-duplex.

This happens when one or both ports on a link are reset and the auto-negotiation process does not cause both partners to have the same configuration. It also happens when you reconfigure one side of a link and do not reconfigure the other side.

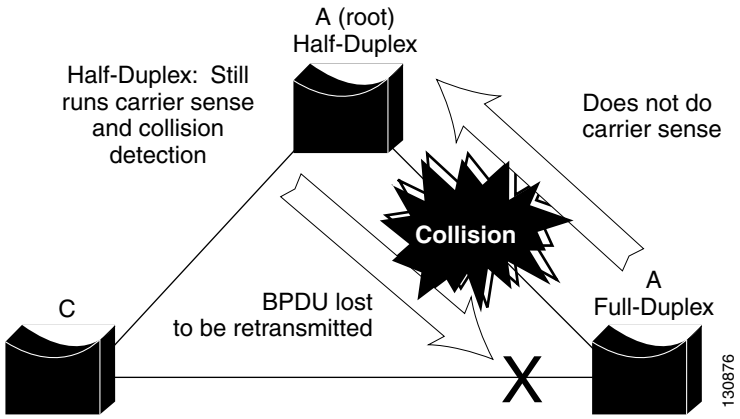
Impact

Half-duplex device waits until no other devices are transmitting on the same LAN segment. However a full-duplex device transmits whenever it has something to send, regardless of other devices.

If this transmission occurs while the half-duplex device is transmitting, the half-duplex device will consider this either a collision (during the slot time), or a late collision (after the slot time). Since the full-duplex side does not expect collisions, it does not realize that it must retransmit that dropped packet.

A low percentage rate of collisions are normal with half-duplex, but not with full-duplex. If the switch port receives many late collisions, it usually indicates a duplex mismatch problem. See Figure 14-1.

Figure 14-1 Duplex Mismatch



Fix

LMS provides commands to resolve link duplex mismatch. LMS displays commands to set the port speed to Auto. Setting the port speed to Auto will automatically make the link duplex to be negotiated between devices.

To fix the discrepancy on switches using Cisco IOS:

Step 1 Go to the Discrepancy report and click the hyperlink in the Summary field.

The Discrepancy Detail dialog box appears. The Recommended Fix field displays the following command:

```
duplex auto
end
```

where *auto* enables the autonegotiation capability.

Step 2 Click **Fix**.

A message appears indicating whether the discrepancy was successfully fixed or not.

To fix the discrepancy on switches using Catalyst operating system:

Step 1 Go to the Discrepancy report and click the hyperlink in the Summary field.

The Discrepancy Detail dialog box appears. The Recommended Fix field displays the following command:

`set port speed` *mod/port* `auto`

where:

- *mod/port* refers to the number of the module and the port on the module
- `auto` specifies autonegotiation for transmission speed and duplex mode on 10/100 Fast Ethernet ports

Step 2 Click **Fix**.

A message appears indicating whether the discrepancy was successfully fixed or not.

Link Speed Mismatch

LMS reports a discrepancy when there is a mismatch in the link speeds, that is, different link speeds on either side of a link (for 10/100 ports or for any group of links).

The IEEE 802.3u autonegotiation protocol manages the switch settings for speed (10 Mbps or 100 Mbps) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

- A manually-set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is in Autonegotiate mode and the connected port is set to full duplex with no autonegotiation.

Impact

Link speed mismatch results in reduced performance of the link.

Fix

LMS displays commands to resolve link speed mismatch.

To fix the discrepancy on switches using Cisco IOS:

Step 1 Go to the Discrepancy report and click the hyperlink in the Summary field.

The Discrepancy Detail dialog box appears. The Recommended Fix field displays the following command:

```
speed auto
end
```

where `auto` enables the autonegotiation capability.

Step 2 Click **Fix**.

A message appears indicating whether the discrepancy was successfully fixed or not.

To fix the discrepancy on switches using the Catalyst operating system:

Step 1 Go to the Discrepancy report and click the hyperlink in the Summary field.

The Discrepancy Detail dialog box appears. The Recommended Fix field displays the following command:

`set port speed` *mod/port* `auto`

where:

- *mod/port* refers to the number of the module and the port on the module
- `auto` specifies autonegotiation for transmission speed and duplex mode on 10/100 Fast Ethernet ports

Step 2 Click **Fix**.

A message appears indicating whether the discrepancy was successfully fixed or not.

Link Trunk/NonTrunk Mismatch

LMS reports a discrepancy when there are trunking ports and non-trunking ports on either side of a link. This happens when one end of the trunk is set to On, and the other end is set to Off.

Impact

This results in the trunk not coming up, and there would be no traffic flow across the link.

Fix

LMS resolves the discrepancy by setting the trunk modes on the switches to Desirable mode.

To fix the discrepancy on switches using the Catalyst operating system:

Step 1 Go to the Discrepancy report and click the hyperlink in the Summary field.

The Discrepancy Detail dialog box appears. The Recommended Fix field displays the following command:

`set trunk` *mod/port* `desirable`

where:

- `desirable` causes the port to negotiate actively with the neighboring port to become a trunk link
- *mod/port* specifies the number of the module and the port or ports on the module

Step 2 Click **Fix**.

A message appears indicating whether the discrepancy was successfully fixed or not.

To fix the discrepancy on switches using Cisco IOS:

Step 1 Go to the Discrepancy report and click the hyperlink in the Summary field.

The Discrepancy Detail dialog box appears. The Recommended Fix field displays the following command:

```
switchport mode dynamic desirable
end
```

where `dynamic desirable` specifies an interface that actively attempts to convert the link to a trunk link.

Step 2 Click **Fix**.

A message appears indicating whether the discrepancy was successfully fixed or not.

Port Related Discrepancy

The port related discrepancy that LMS reports is Port is in Error Disabled State. See Port is in Error Disabled State

Port is in Error Disabled State

LMS reports a discrepancy when one or more of the switch ports in the discovered network have a status of errDisable.

Causes of errDisable

A port enters errdisable state for any of the following reasons:

- Channel misconfiguration
- Duplex mismatch
- BPDU port-guard
- UDLD

Impact

When a port is error-disabled, it is effectively shut down and no traffic is sent or received on that port. The port LED is set to the color orange and when you enter the **`show port`** command, the port status shows errdisable.

Fix

To recover from errDisable:

Step 1 Identify and fix whatever caused the ports to become error-disabled (cable, NICs, EtherChannel, and so on).

Step 2 Re-enable the port.

You cannot fix this discrepancy through LMS.

For more information on the *errDisable* state, see the document *Recovering From errDisable Port State on the CatOS Platforms* at the following location:

http://www.cisco.com/en/US/tech/tk389/tk214/technologies_tech_note09186a0080093dcb.html

Device Related Discrepancy

The device related discrepancy that LMS reports is Devices With Duplicate Sysname. See Devices With Duplicate SysName, page 14-11

Devices With Duplicate SysName

LMS reports a discrepancy when it discovers two devices with the same SysName. LMS stores the device details of only one of the two devices.

Impact

LMS manages only one of these devices.

Fix

Assign unique SysName for all devices in the network. You cannot fix this discrepancy through LMS.

Spanning Tree Related Discrepancy

The spanning tree related discrepancy that LMS reports is PortFast Enabled on Trunk Port. See Port Fast Enabled on Trunk Port

Port Fast Enabled on Trunk Port

LMS reports a discrepancy when PortFast is enabled on trunk ports.

PortFast causes a spanning tree port to immediately enter the forwarding state, bypassing the listening and learning states.

You must disable STP PortFast for switch-switch links. This is because, if you enable PortFast on a port that is connected to another Layer 2 device, such as a switch, you might create network loops.

Impact

If you enable PortFast on ports that connect two switches, spanning tree loops can occur if Bridge Protocol Data Units (BPDUs) are being transmitted and received on those ports.

Fix

LMS provides commands for disabling PortFast on ports.

To fix the discrepancy on switches using the Catalyst operating system:

Step 1 Go to the Discrepancy report and click the hyperlink in the Summary field.

The Discrepancy Detail dialog box appears. The Recommended Fix field displays the following command:

```
set spantree portfast mod/port disable
```

where `disable` disables the spanning tree PortFast-start feature on the port.

Step 2 Click **Fix**.

A message appears indicating whether the discrepancy was successfully fixed or not.

To fix the discrepancy on switches using Cisco IOS:

Step 1 Go to the Discrepancy report and click the hyperlink in the Summary field.

The Discrepancy Detail dialog box appears. The Recommended Fix field displays the following command:

```
no spanning-tree portfast
end
```

This command disables PortFast on the given port.

Step 2 Click **Fix**.

A message appears indicating whether the discrepancy was successfully fixed or not.

Interpreting Best Practices Deviations

This section contains information on each of the Best Practice Deviation reported in LMS. It gives a description of the Best Practice Deviation, the impact (if any) it has on the network, and ways to resolve it.

The user interface in LMS displays commands to make configuration changes on devices, to resolve some Best Practices deviations.

This section contains:

Channel Ports Related Best Practices Deviations

The channel ports related best practices deviations that LMS reports are:

- Non-channel Port in Desirable Mode
- Channel Port in Auto Mode

Non-channel Port in Desirable Mode

LMS reports a Best Practice Deviation when a non-channel port is in the Desirable mode.

There are four user-configurable channel modes:

- On
- Off
- Auto
- Desirable

Port Aggregation Protocol (PAgP) packets are exchanged only between ports in Auto and Desirable modes. Ports configured in on or off mode do not exchange PAgP packets.

To form EtherChannel between, it is best to have both switches set to the Desirable mode. This gives the most robust behavior if one side or the other encounters error situations or is reset. The default mode of the channel is Auto.

Both Auto and Desirable modes allow ports to negotiate with connected ports to determine whether they can form a channel. The determination is based on criteria such as port speed, trunking state, and native VLAN.

Ports can form an EtherChannel when they are in different channel modes if the modes are compatible.

Examples of ports that can form an EtherChannel are:

- A port in desirable mode can successfully form an EtherChannel with another port that is in Desirable or Auto mode.
- A port in the Auto mode can form an EtherChannel with another port in the Desirable mode.
- A port in the Auto mode cannot form an EtherChannel with another port that is also in the Auto mode, since neither port initiates negotiation.
- A port in the On mode can form a channel only with a port in the On mode because ports in On mode do not exchange PAgP packets.
- A port in Off mode cannot form a channel with any port.

Impact

When a non-channel port is in the Desirable mode, the links will not be efficiently used.

Fix

To fix the Best Practice Deviation on switches using Catalyst operating system:

Step 1 Go to the Best Practice Deviation report and click the hyperlink in the Summary field.

The Best Practice Deviation Detail dialog box appears. The Recommended Fix field displays the following command:

set port channel *mod/port* mode auto

Step 2 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

To fix the Best Practice Deviation on switches using Cisco IOS:

Step 1 Go to the Best Practice Deviation report and click the hyperlink in the Summary field.

The Best Practice Deviation Detail dialog box appears. The Recommended Fix field displays the following command:

channel-group *Channel group number* mode auto

Step 2 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

Channel Port in Auto Mode

LMS reports a Best Practice Deviation when a channel port is in *Auto* mode.

There are four user-configurable channel modes:

- On
- Off
- Auto
- Desirable

Port Aggregation Protocol (PAgP) packets are exchanged only between ports in Auto and Desirable mode. Ports configured in On or Off mode do not exchange PAgP packets.

For switches to which you want to form an EtherChannel, it is best to have both switches set to Desirable mode. This gives the most robust behavior if one of the sides encounters error situations or is reset. The default mode of the channel is Auto.

Both Auto and Desirable modes allow ports to negotiate with connected ports to determine if they can form a channel. The determination is based on criteria such as port speed, trunking state, and native VLAN.

Ports can form an EtherChannel when they are in different channel modes if the modes are compatible.

Examples of ports that can form an EtherChannel are:

- A port in Desirable mode can successfully form an EtherChannel with another port that is in Desirable or Auto mode.
- A port in Auto mode can form an EtherChannel with another port in Desirable mode.

- A port in Auto mode cannot form an EtherChannel with another port that is also in Auto mode, since neither port initiates negotiation.
- A port in On mode can form a channel only with another port also in On mode, because ports in this mode do not exchange PAgP packets.
- A port in Off mode cannot form a channel with any port.

Impact

Channel port set to Auto mode is considered a Best Practice Deviation because it is not the recommended configuration. Cisco recommends that you set the channel port to Desirable mode. There is no serious impact on the network.

Fix

To fix the Best Practise Deviation on switches using the Catalyst operating system:

Step 1 Go to the Best Practise Deviation report and click the hyperlink in the Summary field.

The Best Practise Deviation Detail dialog box appears. The Recommended Fix field displays the following command:

`set port channel` *mod/port* `mode desirable`

which sets the port to desirable mode.

Step 2 Click **Fix**.

A message appears indicating whether the Best Practise Deviation was successfully fixed or not.

To fix the Best Practise Deviation on switches using Cisco IOS:

Step 1 Go to the Best Practise Deviation report and click the hyperlink in the Summary field.

The Best Practise Deviation Detail dialog box appears. The Recommended Fix field displays the following command:

`channel-group` *`Channel group number`* `mode desirable`

which sets the port to desirable mode.

Step 2 Click **Fix**.

A message appears indicating whether the Best Practise Deviation was successfully fixed or not.

Spanning Tree Related Best Practices Deviations

The spanning tree related best practices deviations that LMS reports are:

- BPDU Filter Disabled on Access Ports
- BPDU-Guard Disabled on Access Ports
- BackboneFast Disabled in Switch
- UplinkFast not Enabled
- Loop Guard and Port Fast Enabled on Ports

BPDU Filter Disabled on Access Ports

LMS reports a Best Practice Deviation when BPDU Filter is not enabled on access ports.

Impact

BPDU filtering allows you to avoid transmitting BPDUs on PortFast-enabled ports that are connected to an end system. When you enable PortFast on the switch, spanning tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states.

By default, spanning tree sends BPDUs from all ports regardless of whether PortFast is enabled. BDPUFilter can be enabled for each port or globally. When you enable BPDUFilter globally, it applies to all PortFast-enabled ports on the switch.

When you disable PortFast on a port, the BPDU Filter that was globally enabled on the PortFast enabled port is also disabled.

Fix

LMS provides commands for enabling BPDU Filter on access ports.

To fix the Best Practice Deviation on switches using Catalyst operating system:

Step 1 Go to the Best Practices Deviations report and click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

`set spantree bpdu-filter` *mod/port* **`enable`**

where:

- *mod/port* specifies the number of the module and the port on the module
- **`enable`** enables BPDU packet filtering

Step 2 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

To fix the Best Practice Deviation on switches using Cisco IOS:

Step 1 Go to the Best Practices Deviations report and click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
spanning-tree bpdufilter enable
end
```

where `enable` enables BPDU Filtering on the particular interface.

Step 2 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

BPDU-Guard Disabled on Access Ports

LMS reports a Best Practice Deviation if PortFast is enabled and BPDU-Guard is not enabled on a port.

BPDU-Guard prevents spanning-tree loops by moving a port into the errdisable state when a BPDU is received on that port. When you enable BPDU-Guard on the switch, spanning tree shuts down the interfaces that receive BPDUs instead of putting the interfaces into the spanning-tree blocking state.

Impact

Cisco recommends that you enable BPDUGuard to block incoming BPDUs on edge devices (end-hosts). The Cisco BPDUGuard feature, when enabled, informs the switch to disable PortFast ports if a BPDU is received on those ports.

BDPUGuard can be enabled on each port or globally. When you enable BPDUGuard globally, it applies to all PortFast-enabled ports on the switch.

Fix

LMS displays commands for enabling BPDU Filter on access ports.

To fix the Best Practice Deviation on switches using Catalyst operating system:

Step 1 Go to the Best Practices Deviations report and click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

`set spantree bpdu-guard` *mod/port* **`enable`**

where:

- *mod/port* specifies the number of the module and the port on the module
- **`enable`** enables BPDUGuard

Step 2 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

To fix the Best Practice Deviation on switches using Cisco IOS:

Step 1 Go to the Best Practices Deviations report and click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
spanning-tree bpduguard enable
end
```

where `enable` enables BPDUGuard on the particular interface.

Step 2 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

BackboneFast Disabled in Switch

LMS reports a Best Practice Deviation when BackboneFast is enabled on one of the switches and not enabled on all other switches in a switch cloud.

Cisco recommends that BackboneFast be enabled on all switches running STP. It can be added without disruption to a production network.

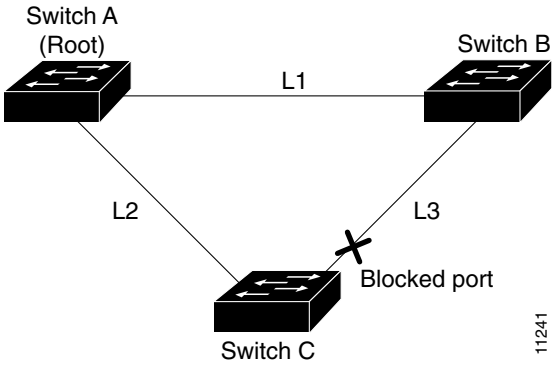
Impact

If you do not enable BackboneFast on all devices, it might lead to undesirable effects on the spanning tree operation.

BackboneFast provides rapid convergence from indirect link failures. By adding functionality to STP, you can reduce convergence times from the default of 50 seconds to 30 seconds.

Figure 14-2 shows an example topology with no link failures. Switch A, the root switch, connects directly to Switch B over link L1 and to Switch C over link L2. The port on Switch C that connects directly to Switch B is in the blocking state.

Figure 14-2 BackboneFast Example Before Indirect Link Failure



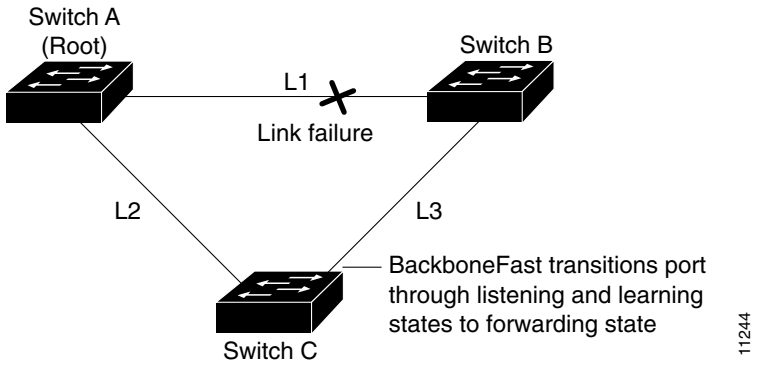
If link L1 fails, Switch C detects this failure as an indirect failure, because it is not connected directly to link L1.

Switch B no longer has a path to the root switch. BackboneFast allows the blocked port on Switch C to move immediately to the listening state without waiting for the maximum aging time for the port to expire.

BackboneFast then transitions the port on Switch C to the forwarding state, providing a path from Switch B to Switch A.

This switchover takes approximately 30 seconds. Figure 14-3 shows how BackboneFast reconfigures the topology to account for the failure of link L1.

Figure 14-3 BackboneFast Example After Indirect Link Failure



Fix

Enable BackboneFast on all switches in a switch cloud.

To enable BackboneFast Globally on a Catalyst operating system:

Step 1 Enter the command:

```
set spantree backbonefast enable
```

Step 2 Enter this command to check the status:

```
show spantree backbonefast
```

To enable BackboneFast Globally on Cisco IOS:

Step 1 Enter the command:

```
spanning-tree backbonefast
```

Step 2 Enter this command to check the status:

```
show spanning-tree backbonefast
```

You cannot fix this Best Practice Deviation through LMS.

For more information on Spanning Tree related configuration, see the document *Configuring Spanning Tree PortFast, UplinkFast, and BackboneFast* at the following location:

http://www.cisco.com/en/US/products/hw/switches/ps708/prod_eol_notices_list.html

UplinkFast not Enabled

LMS reports a Best Practice Deviation when UplinkFast is not enabled on switches.

Note This Best Practice Deviation is not applicable if the device is not an access layer switch.

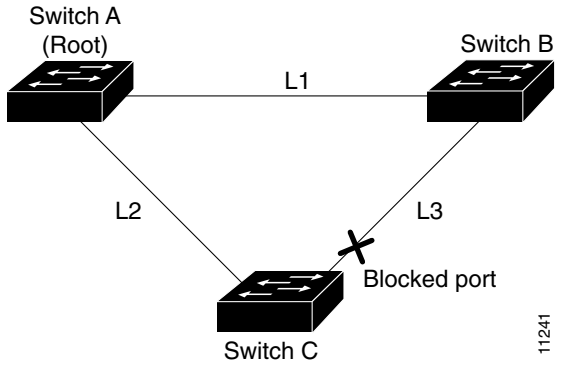
Cisco recommends that you enable UplinkFast for switches with blocked ports, typically at the access layer. Do not use on switches without the implied topology knowledge of a backup root link—typically, distribution and core switches in Cisco's multilayer design. It can be added without disruption to a production network.

Impact

UplinkFast provides fast STP convergence after a direct link failure in the network access layer. It operates without modifying STP, and its purpose is to speed up convergence time in a specific circumstance to less than three seconds, rather than the typical 30-second delay.

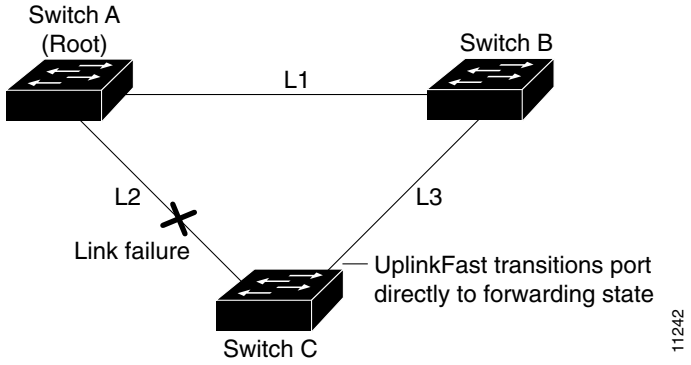
Figure 14-4 shows an example topology with no link failures. Switch A, the root switch, is connected directly to Switch B over link L1 and to Switch C over link L2. The port on Switch C that is connected directly to Switch B is in the blocking state.

Figure 14-4 UplinkFast Example Before Direct Link Failure



If Switch C detects a link failure on the currently active link L2 (a direct link failure), UplinkFast unblocks the blocked port on Switch C and transitions it to the forwarding state without going through the listening and learning states, as shown in Figure 14-5. This switchover takes approximately 1 to 5 seconds.

Figure 14-5 UplinkFast Example After Direct Link Failure



Fix

Enable UplinkFast on all access layer switches.

To enable Uplink Fast on Catalyst operating system:

Step 1 Enter the command:

```
set spantree uplinkfast enable
```

Step 2 Enter this command to check the status:

```
show spantree uplinkfast
```

To enable Uplink Fast on Cisco IOS:

Step 1 Enter the command:

```
spanning-tree uplinkfast
```

Step 2 Enter this command to check the status:

```
show spanning-tree uplinkfast
```

You cannot fix this Best Practice Deviation through LMS.

For more information on Spanning Tree related configuration, see the document *Configuring Spanning Tree PortFast, UplinkFast, and BackboneFast* at the following location:

http://www.cisco.com/en/US/products/hw/switches/ps708/prod_eol_notices_list.html

Loop Guard and Port Fast Enabled on Ports

Loop Guard

Assume that a switch port is receiving BPDUs, and is in the blocking state. The port makes up a redundant path. It is blocking because it is neither a Root Port nor a Designated Port. If, the flow of BPDUs stops, the last known BPDU is retained until the Max Age timer expires.

When the Max Age timer expires, that BPDU is flushed, and the switch thinks there is no longer a need to block the port. The port moves through the STP states until it begins to forward traffic. The switch then forms a bridging loop. In its final state, the port becomes a Designated Port.

To prevent this situation, you can use the loop guard STP feature. When you enable this feature, loop guard keeps track of the BPDU activity on nondesignated ports. While BPDUs are received, the port is allowed to behave normally.

When BPDUs are missing, loop guard moves the port into the loop-inconsistent state. The port is effectively blocking at this point to prevent a loop from forming and to keep it in the nondesignated role.

After BPDUs are received on the port again, loop guard allows the port to move through the normal STP states and become active. In this way, Loop Guard automatically governs ports without the need for manual intervention.

STP PortFast

STP configures meshed topology into a loop-free, tree-like topology. When the link on a bridge port goes up, STP calculation occurs on that port. The result of the calculation is the transition of the port into forwarding or blocking state. The result depends on the position of the port in the network and the STP parameters.

This calculation and transition period usually takes about 30 to 50 seconds. At that time, no user data passes through the port. Owing to this, some user applications can time out during the period.

To allow immediate transition of the port into forwarding state, enable the STP PortFast feature. PortFast immediately transitions the port into STP forwarding mode upon linkup. This way the port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into the STP blocking mode.

Impact

Enabling both the above features in a port, gives unpredictable results. Hence LMS flags it as a Best Practice Deviation.

Fix

If you fix the above Best Practice Deviation through LMS, it disables the Port Fast feature in the port.

To fix the Best Practice Deviation on switches using the Catalyst operating system:

Step 1 Go to the Best Practices Deviations report and click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
set spantree portfast disable
```

Step 2 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

To fix the Best Practice Deviation on switches using Cisco IOS:

Step 1 Select **Reports > Fault and Event**.

Step 2 Select Best Practices Deviation Report from the TOC.

Step 3 Click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
spanning-tree portfast disable
```

Step 4 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

Trunk Ports Related Best Practices Deviations

The trunk ports related best practices deviations that LMS reports are as follows:

- Non-trunk Ports in Desirable Mode
- Trunk Ports in Auto Mode

Non-trunk Ports in Desirable Mode

LMS reports a Best Practice Deviation when non-trunk ports are set to Desirable mode.

Impact

Cisco recommends that you set trunk to **Off** on all non-trunk ports. This helps eliminate wasted negotiation time when bringing host ports up. If a non-trunk port is set to **Desirable**, it attempts to become a trunk port if the neighboring port is in **Desirable** or **Auto** mode, although that is not the intended behavior.

Fix

To fix the Best Practice Deviation, set the trunk mode to **Off** on all non-trunk ports.

To fix it through LMS, on switches using the Catalyst operating system:

Step 1 Select **Reports > Fault and Event**.

Step 2 Select Best Practices Deviation Report from the TOC.

Step 3 Click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
set port host mod/port
```

Step 4 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

To fix it through LMS, on switches using Cisco IOS:

Step 1 Select **Reports > Fault and Event**.

Step 2 Select Best Practices Deviation Report from the TOC.

Step 3 Click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
switchport mode access
```

Step 4 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

Table 14-1 lists all possible combinations of trunk mode configurations and when LMS reports a Best Practice Deviation.

Table 14-1 Trunking Configuration [1]

Modes	On	Auto	Desirable	Nonegotiate	Off
On	None. (Trunking)	Reports Best Practice Deviation. (Trunking)	None. (Trunking)	None. (Trunking)	Reports Best Practice Deviation. (Not Trunking)
Auto	Reports Best Practice Deviation. (Trunking)	None. (Not Trunking)	Reports Best Practice Deviation. (Trunking)	Reports Best Practice Deviation. (Not Trunking)	None. (Not Trunking)
Desirable	None. (Trunking)	Reports Best Practice Deviation. (Trunking)	None. (Trunking)	Reports Best Practice Deviation. (Not Trunking)	Reports Best Practice Deviation. (Not Trunking)
Nonegotiate	None. (Trunking)	Reports Best Practice Deviation. (Not Trunking)	Reports Best Practice Deviation. (Not Trunking)	None. (Trunking)	Reports Best Practice Deviation. (Not Trunking)
Off	Reports Best Practice Deviation. (Not Trunking)	None. (Not Trunking)	Reports Best Practice Deviation. (Not Trunking)	Reports Best Practice Deviation. (Not Trunking)	None. (Not Trunking)

1. Information in brackets indicate the trunking state of the interface.

Trunk Ports in Auto Mode

LMS reports a Best Practice Deviation when trunk ports are set to Auto mode.

Impact

Cisco recommends an explicit trunk configuration of Desirable at both ends. Auto mode indicates a static property and the port will not initiate the trunking link, if the neighbor does not initiate it. See Table 14-1 for different trunk mode combinations.

Fix

To fix the Best Practice Deviation on switches using the Catalyst operating system:

Step 1 Select **Reports > Fault and Event**.

Step 2 Select Best Practices Deviation Report from the TOC.

Step 3 Click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
set trunk mod/port desirable
```

Step 4 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

To fix the Best Practice Deviation on switches using Cisco IOS:

Step 1 Select **Reports > Fault and Event**.

Step 2 Select Best Practices Deviation Report from the TOC.

Step 3 Click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
switchport mode dynamic desirable
```

Step 4 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

VLAN Related Best Practices Deviations

The VLAN related best practices deviations that LMS reports are as follows:

- VLAN Index Conflict
- VLAN Name Conflict

VLAN Index Conflict

LMS reports a Best Practice Deviation when there is a conflict in the VLAN Index. A VLAN Index conflict occurs in case of a VTP domain which has Server mode and Transparent or Off mode devices, where a same VLAN index has different VLAN name in transparent and server mode devices in the domain.

Impact

There is no serious impact on the network connectivity. It is considered as a Best Practice Deviation because LMS cannot manage a VTP domain where the same VLAN index has different VLAN names in transparent and server mode devices.

Fix

Assign the same name for a VLAN Index in both the transparent and server modes of the VTP domain. You cannot fix this Best Practice Deviation through LMS.

VLAN Name Conflict

LMS reports a Best Practice Deviation when there is a conflict in the VLAN Name. A VLAN Name conflict occurs in case of a VTP domain which has Server mode and Transparent or Off mode devices, where a VLAN part of the transparent mode device in the domain has the same name as VLAN part of the server mode device in the domain.

Impact

There is no serious impact on the network connectivity. It is considered as a Best Practice Deviation because LMS cannot manage a VTP domain with devices where a VLAN part of the transparent mode device in the domain has the same name as VLAN part of the server mode device in the domain.

Fix

Resolve the conflict by assigning different names for the VLAN part of the transparent mode and the server mode devices. You cannot fix this Best Practice Deviation through LMS.

Link Ports Related Best Practice Deviation

The link port related Best Practice Deviation that LMS reports is UDLD Disabled on Link Ports. See UDLD Disabled on Link Ports

UDLD Disabled on Link Ports

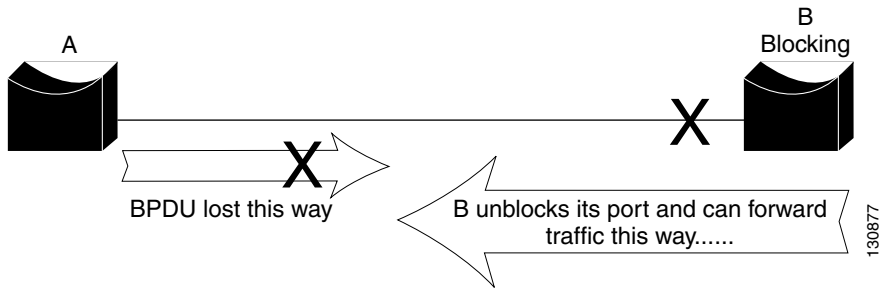
LMS reports a Best Practice Deviation if UniDirectional Link Detection (UDLD) is disabled on link ports.

Impact

If you disable UDLD, it could result in Spanning Tree loops.

Unidirectional links are often caused by a failure not detected on a fiber link, or by a problem with a transceiver.

Figure 14-6 Unidirectional Links



In Figure 14-6, suppose the link between A and B is unidirectional and drops traffic from A to B while transmitting traffic from B to A. Suppose that B should be blocking. It has previously been stated that a port can only block if it receives BPDUs from a bridge that has a higher priority. In this case, all these BPDUs coming from A are lost and bridge B eventually forwards traffic, creating a loop.

To detect the unidirectional links before the forwarding loop is created, Cisco designed and implemented the UniDirectional Link Detection (UDLD) protocol. This feature is able to detect improper cabling or unidirectional links on Layer 2 and automatically break resulting loops by disabling some ports.

For maximum protection against symptoms resulting from uni-directional links, we recommend that you enable aggressive mode UDLD on point-to-point links between Cisco switches, where you have set the message interval to the default 15 seconds.

Fix

LMS provides commands to enable UDLD on link ports.

To fix the Best Practice Deviation on switches using Catalyst operating system:

Step 1 Go to the Best Practices Deviations report and click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
set udld enable mod/port
```

where *enable* enables the UDLD information display.

Step 2 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

To fix the Best Practice Deviation on switches using Cisco IOS:

Step 1 Select **Reports > Fault and Event**.

Step 2 Select Best Practices Deviation Report from the TOC.

Step 3 Click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix displays the following command:

```
udld port
end
```

This command enables UDLD in normal mode by default on all interfaces.

Step 4 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

Access Ports Related Best Practice Deviation

The access ports related Best Practice Deviation that LMS reports is CDP Enabled on Access Ports. See CDP Enabled on Access Ports

CDP Enabled on Access Ports

LMS reports a Best Practice Deviation when Cisco Discovery Protocol (CDP) is enabled on the access port of a switch.

CDP is enabled by default and is essential to gain visibility of adjacent devices and for troubleshooting. It is also used by network management applications to build Layer 2 topology maps.

Impact

In parts of the network where a high level of security is required (such as Internet-facing de-militarized zones), you should turn off CDP.

Fix

LMS provides commands to disable CDP on switches.

To fix the Best Practice Deviation on switches running Catalyst operating system:

Step 1 Select **Reports > Fault and Event**.

Step 2 Select Best Practices Deviation Report from the TOC.

Step 3 Click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
set cdp disable mod/port
```

Step 4 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

To fix the Best Practice Deviation on switches running Cisco IOS:

Step 1 Select **Reports > Fault and Event**.

Step 2 Select Best Practices Deviation Report from the TOC.

Step 3 Click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
no cdp enable
```

Step 4 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

Cisco Catalyst 6000 Devices Related Best Practice Deviation

The Cisco Catalyst 6000 devices related Best Practice Deviation that LMS reports is High Availability not Operational. See High Availability not Operational

High Availability not Operational

Enabling High Availability on switches is applicable only for Cisco Catalyst 6000 devices. LMS reports a Best Practice Deviation when there are two supervisor engines in Cisco Catalyst 6000 devices and High Availability is not enabled.

Impact

High Availability:

- Is a critical requirement for most networks. Switch downtime must be minimal to ensure maximum productivity in a network.
- Allows you to minimize the switch-over time from active supervisor engine to the standby supervisor engine, if the active supervisor engine fails.

- Allows the active supervisor engine to communicate with the standby supervisor engine, keeping feature protocol states synchronized.
- Provides a versioning option that allows you to run different software images on the active and standby supervisor engines.

You can enable High Availability using Command Line Interface (CLI).

Fix

As a general practice with redundant supervisors, we recommend that you enable High Availability feature for normal operation.

LMS provides commands for enabling High Availability.

To fix the Best Practice Deviation on switches using Catalyst operating system:

Step 1 Go to the Best Practices Deviations report and click the hyperlink in the Summary field.

The Best Practice Deviation Details dialog box appears. The Recommended Fix field displays the following command:

```
set system highavailability enable
```

Step 2 Click **Fix**.

A message appears indicating whether the Best Practice Deviation was successfully fixed or not.

For more information on Supervisor engines and High Availability, see the document *Configuring Redundancy* at the following location:

http://www.cisco.com/en/US/products/hw/switches/ps708/prod_eol_notices_list.html

Customizing Discrepancies Reporting and Syslog Generation

You can customize the Discrepancies Report and Best Practices Deviations Report to display only those discrepancies and Best Practice Deviations about which you want to be notified.

To customize the reports:

Step 1 Select **Admin > Network > Best Practices Deviation Settings**.

The discrepancies page appears. You can view the list of Network discrepancies, and Discrepancies configured to send Syslog messages by clicking the corresponding **View Details** link.

Step 2 Click **Configure**.

The **Configuring Discrepancies** dialog box appears.

- To include a Discrepancy or Best Practice Deviation in the Reports, check the check box next to it.

  Checking all the check boxes results in a report displaying all discrepancies and Best Practice Deviations in the network.
- To exclude a Discrepancy or Best Practice Deviation from the Reports, uncheck the corresponding check box.

Step 3 Generate Syslog messages for the selected Discrepancies and Best Practice Deviations. To do this, check **Configure Syslog** and click **Next**.

A list of the selected Discrepancies and Best Practice Deviations appears.

Step 4 Check **Send Syslogs** and enter the name of the server in the Syslog Server field.

Step 5 Select the Discrepancies and Best Practice Deviations for which you want to generate Syslog messages and click **Next**.

A summary of the selected Discrepancies and Best Practice Deviations appears.

Step 6 Click **Finish**.

You can use the filters to display discrepancy reports for specific devices, link or network types. This makes it easy to find a particular discrepancy for a particular type.

You can use more than one filter at the same time, but results will vary.

- If you select more than one filter in the same top-level category, Boolean OR is used.

  For example, if you select Duplex, Speed under Link, any link or port that fulfils at least one filter criteria will be displayed in the report.

- If you select more than one filter from different top-level categories, Boolean AND is used.

  For example, if you select both a Link type and a Port type filter from the discrepancy filter, any link that fulfils both filter criteria will appear in the report.