



## Discrepancy Reporting

---

The Discrepancy Reporting module allows you to view the physical and logical discrepancies in your network. This chapter contains the following:

- [Understanding Discrepancy Reporting, page 7-1](#)
- [Interpreting Discrepancies, page 7-6](#)

### Understanding Discrepancy Reporting

This feature offers reports on network inconsistencies, anomalies or misconfiguration in the physical and logical layout in the discovered network. This makes it easy to identify configuration errors such as link-speed mismatches on either end of a connection. This chapter contains the following:

- [Physical Discrepancies, page 7-1](#)
- [Logical Discrepancies, page 7-3](#)

### Physical Discrepancies

Physical discrepancies are potential misconfigurations in the physical layout of your network. Physical discrepancies include mismatches in link speed, trunk configuration, or duplex mode on two ends of a link.

For example, full duplex configured on one side of a link and half duplex configured on the other side. [Table 7-1](#) lists the physical discrepancies reported by Campus Manager.

**Table 7-1**      **Physical Discrepancies**

Field	Discrepancy	Description
Physical > Link > Duplex	Link Duplex Mismatch	Full-duplex versus half-duplex on either side of a link
Physical > Link > Speed	Link Speed Mismatch	Different link speed on either side of a link (for 10/100 ports or for any group of links)
General > DuplicateSysName	Duplicate SysName	More than one device with the same sysname (SystemName) on the Network.
Physical > Link > Trunk	Trunk/nonTrunk Mismatch	Trunking ports versus nontrunking ports on either side of a link
Physical > Port > ErrDisabled	Port in ErrorDisabled State	Port is in Error Disabled state caused by erroneous traffic
Physical > Port > PortFastEnabled	PortFastEnabled on Trunk Port	A port configured for trunk is in Spanning Tree PortFastEnabled state
Physical > High AvailabilityDisabled	High Availability Disabled	High Availability Feature is disabled in a device when it has more than one Supervisor Card
Physical > CDPEnabledon AccessPort	CDP Enabled on Access Port	An access port of a device is enabled for CDP
Physical > Device > BackboneFastDisabled	BackboneFast Disabled	BackboneFast feature is disabled on a device
Physical > Device > UplinkFastDisabled	UplinkFast Disabled	UplinkFast feature is disabled on a device
Physical > Port > UDLDDisabled	UDLD Disabled	Unidirectional Link Detection feature is disabled on a device
Physical > Port > STPEnabledonAccess Ports	STP Enabled on Access Ports	An access port of a device in which STP is enabled
Physical > Port > BPDUGuardDisabled	BPDU Guard Disabled	BPDU Guard Feature is disabled on a port

**Table 7-1** *Physical Discrepancies (continued)*

Field	Discrepancy	Description
Physical > Port > AutoChannel	Auto Channel	A port is configured for auto mode, and it is part of channel
Physical > Port > NoChannel	No Channel	A port is configured for desirable mode, and it is not part of channel
Physical > Port > AutoTrunk	Auto Trunk	Trunk Mode is set to Auto, but port is trunking
Physical > Port > NoTrunk	No Trunk	Trunk mode set to desirable, but port is not trunking

## Logical Discrepancies

Logical discrepancies include inconsistent or incorrect settings in VTP domains, VLANS, and ATM LANE components.

For example, an ATM VLAN that has no entry in the LECS or if there is a VTP client and no VTP server. [Table 7-2](#) lists the logical discrepancies reported by Campus Manager.

**Table 7-2** *Logical Discrepancies*

Field	Discrepancy	Description
LANE > ATM-VLAN > NoEntryInLECS	ATM-VLAN with no entry in LE Config Server	ATM-VLAN having no entry in LE Config Server
LANE > ATM-VLAN > NoLESBUSEntryInLECS	ATM-VLAN with LE Server having no entry in LE Config Server	ATM-VLAN with LE Server having no entry in LE Config Server
LANE > ATM-VLAN > Partitioned	Partitioned ATM-VLAN	Partitioned ATM-VLAN
LANE > LECS > MultiMaster	More than one LE Config Server in a single ATM Domain	More than one LE Config Server present in a single ATM Domain
VLAN > Domain > Disconnect	VTP Disconnected Domain	VTP Disconnected Domain

**Table 7-2** Logical Discrepancies (continued)

Field	Discrepancy	Description
VLAN > Domain > NoServerWithClients	No VTP Server in Domain	No VTP Server configured in Domain
VLAN > DripEnabled	DRiP enabled VLAN	DRiP enabled VLAN
VLAN > EtherChannelPort > SpanningTree	EtherChannel Port Spanning Tree not disabled	EtherChannel Port Spanning Tree not disabled
VLAN > Link > Multi	Trunk VLANs Mismatch	Trunk VLANs Mismatch
VLAN > Link > Protocol	Trunk VLAN Protocol Mismatch	Trunk VLAN Protocol Mismatch
VLAN > Link > Single	Native VLANs Mismatch	Native VLANs Mismatch
VLAN > Link > TrunkNegotiationEnabled	Trunk Negotiation Enabled	DTP enabled on trunk port across VTP boundary
VLAN > Pair > Index	VLAN Index Conflict	VLAN Index Conflict
VLAN > Pair > Name	VLAN Name Conflict	VLAN Name Conflict

## Configuring Discrepancy Reporting and Syslog Message Generation

You can customize the Discrepancy Report to display only those discrepancies about which you want to be notified.

To customize the reports:

- 
- Step 1** Select **Campus Manager > Administration > Network Discrepancies**.  
The **Network Discrepancies** window appears.
- Step 2** Click **Configure** to include or exclude discrepancies to be reported, and also to configure syslog.  
The **Configure Network Discrepancies** dialog box appears.

- Step 3** Select the discrepancies to be included in the Discrepancy Report.
- To include a discrepancy in the Discrepancy Reports, check the box next to it. If you check all the boxes, a report appears with all discrepancies in the network.
  - To exclude a discrepancy from the Discrepancy Reports, uncheck the box.
- Step 4** Select the Configure Syslog check box and click **Next**.  
The list of selected discrepancies appears.
- Step 5** Select the Send Syslogs check box and enter the name of the server in the Syslog Server field.
- Step 6** Select the discrepancies for which you want to generate syslog messages and click **Next**.  
A summary of the selected discrepancies appears.
- Step 7** Click **Finish**.
- 

## Viewing Physical Discrepancy Reports

Discrepancy reports can be viewed using either of the following methods:

- From the CiscoWorks Homepage:

Select **Campus Manager > Discrepancy Reports > Physical Discrepancy Report**.

Or

- From a network topology view:

To view physical discrepancies for the entire network, from the LAN Edge or Layer 2 Network View window, select **Reports > Discrepancies**. It displays any link-setting mismatches that might need to be corrected on devices.

You can also display physical discrepancies for a specific ATM or VTFI domain by selecting the discrepancy filters within the Network View window for that domain.

## Viewing Logical Discrepancy Reports

You can display logical discrepancies to identify inconsistencies in the logical setup of the VTP Domains, VLANs, and LANE components in your network.

To display these discrepancies, you can do either of the following:

- From the CiscoWorks Homepage:  
Select **Campus Manager > Discrepancy Reports > Logical Discrepancy Report**.

Or

- Follow this procedure in Topology Services:

- 
- Step 1** From Topology Services , select **Reports > Discrepancies**. The Logical Discrepancy report appears.
- To print this report, select **File > Print** from the Discrepancy Report menu.
  - To save the summary of discrepancies as a file, select **File > Export > Summary** from the Discrepancy Report menu bar.
  - To save the summary and details of discrepancies as a file, select **File > Export > Details** from the Discrepancy Report menu.
- Step 2** Select a discrepancy and click **Details** for more information.
- 

## Interpreting Discrepancies

When interpreting the discrepancy report, consider that some configurations may appear as discrepancies. If you had planned to configure your network in this way, you can ignore the discrepancies.

## Interpreting Physical Discrepancies

Physical discrepancies are potential misconfigurations in the physical layout of your network. This section contains information on the physical discrepancies reported in Campus Manager 4.0.3. It gives the description of the discrepancy, the impact it has on the network, and ways to resolve it.

### Link Duplex Mismatch

Campus Manager 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 result in both link partners having the same configuration. It also happens when you reconfigure one side of a link and do not reconfigure the other side.

#### Impact

Unlike half-duplex, which must wait until no other devices are transmitting on the same LAN segment, a full-duplex device will transmit 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 a lot of late collisions, this usually indicates a duplex mismatch problem.

#### Fix

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

```
speed auto  
end
```

where **auto** enables the autonegotiation capability.

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

```
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

## Link Speed Mismatch

Campus Manager reports a discrepancy when there is a mismatch in the link speeds, that is, different link speed 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

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

```
speed auto
```

```
end
```

where **auto** enables the autonegotiation capability.

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

```
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

## Duplicate SysName

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

### Impact

Campus Manager manages only one of these devices.

### Fix

Assign unique SysName for all devices in the network.

## Trunk/Non-Trunk Mismatch

Campus Manager 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**

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

```
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

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

```
switchport mode dynamic desirable  
end
```

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

## Port in Error Disabled State

Campus Manager 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**

In order to recover from `errDisable` you should:

- 
- 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.
- 

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/partner/tech/tk389/tk214/technologies\\_tech\\_note09186a0080093dcb.shtml](http://www.cisco.com/en/US/partner/tech/tk389/tk214/technologies_tech_note09186a0080093dcb.shtml)

## PortFastEnabled on Trunk Port

Campus Manager 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**

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

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

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

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

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

This command disables PortFast on the given port.

## High Availability Disabled

Enabling High Availability on switches is applicable only for Cisco Catalyst 6000 devices. Campus Manager reports a discrepancy 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.

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

```
set system highavailability enable
```

## CDP Enabled on Access Ports

Campus Manager reports a discrepancy 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

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

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

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

```
no cdp enable
```

## BackboneFast Disabled

Campus Manager reports a discrepancy 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.

**Fix**

Enable BackboneFast on all switches in a switch cloud.

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

```
set spantree backbonefast enable
```

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

```
spanning-tree backbonefast
```

## UplinkFast Disabled

Campus Manager reports a discrepancy when UplinkFast is not enabled on switches.

**Note**

---

This discrepancy is not applicable if the device is not an access layer switch.

---

We recommend 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. You can add this 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.

**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
```
- 

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/univercd/cc/td/doc/product/lan/cat6000/sw\\_8\\_4/config\\_gd/stp\\_enha.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_4/config_gd/stp_enha.htm)

## UDLD Disabled

Campus Manager reports a discrepancy 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.

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

```
set udd enable mod/port
```

where **enable** enables the UDLD information display.

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

```
udld port  
end
```

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

## BPDU Guard Disabled

Campus Manager reports a discrepancy if PortFast is enabled and BPDUGuard 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.

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

### Fix

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

```
set spantree bpduguard mod/port enable
```

where:

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

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

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

where **enable** enables BPDUGuard on the particular interface.

## STP Enabled on Access Ports

Campus Manager reports a discrepancy when STP is 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. BDPUPFilter can be enabled for each port or globally. When you enable BDPUPFilter 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

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

```
set spantree bpd-filter mod/port enable
```

where:

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

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

```
spanning-tree bpdudfilter enable
end
```

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

## Auto Channel

Campus Manager reports a discrepancy 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 side or the other encounters error situations or is reset. The default mode of the channel is Auto.

Both the 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 as long as the modes are compatible.

This list provides examples:

- 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 a port in 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**

Channel port set to Auto mode is considered a discrepancy 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**

Set the channel port to Desirable mode.

## No Channel

Campus Manager reports a discrepancy when a non-channel port is in 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 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 side or the other encounters error situations or is reset. The default mode of the channel is Auto.

Both the 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 as long as the modes are compatible.

This list provides examples:

- 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 a port in 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 Desirable mode, the links will not be efficiently used.

**Fix**

Set the non-channel port to Auto mode.

## Auto Trunk

Campus Manager reports a discrepancy 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 7-3](#) for different trunk mode combinations.

**Table 7-3** *Trunking Configuration*<sup>1</sup>

Modes	On	Auto	Desirable	Nonegotiate	Off
On	None. (Trunking)	Reports discrepancy. (Trunking)	None. (Trunking)	None. (Trunking)	Reports discrepancy. (Not Trunking)
Auto	Reports discrepancy. (Trunking)	None. (Not Trunking)	Reports discrepancy. (Trunking)	Reports discrepancy. (Not Trunking)	None. (Not Trunking)
Desirable	None. (Trunking)	Reports discrepancy. (Trunking)	None. (Trunking)	Reports discrepancy. (Not Trunking)	Reports discrepancy. (Not Trunking)

**Table 7-3** *Trunking Configuration (continued)<sup>1</sup>*

Modes	On	Auto	Desirable	Nonegotiate	Off
Nonegotiate	None. (Trunking)	Reports discrepancy. (Not Trunking)	Reports discrepancy. (Not Trunking)	None. (Trunking)	Reports discrepancy. (Not Trunking)
Off	Reports discrepancy. (Not Trunking)	None. (Not Trunking)	Reports discrepancy. (Not Trunking)	Reports discrepancy. (Not Trunking)	None. (Not Trunking)

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

**Fix**

Set both ends of trunk ports to Desirable mode. You cannot fix this discrepancy through Campus Manager.

Enter the following command to set Desirable mode:

```
set trunk mod/port desirable ISL | dot1q
```

**No Trunk**

Campus Manager reports a discrepancy 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**

Set the trunk mode to Off on all non-trunk ports.

[Table 7-3 on page 7-20](#) lists all possible combinations of trunk mode configurations and when Campus Manager reports a discrepancy.

## Interpreting Logical Discrepancies

Logical discrepancies identify inconsistencies in the logical setup of the VTP Domains, VLANs, and LANE components in your network. This section contains information on the physical discrepancies reported in Campus Manager 4.0.3. It gives the description of the discrepancy, the impact it has on the network, and ways to resolve it.

### Trunk VLANs Mismatch

Campus Manager 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.

### Native VLANs Mismatch

Campus Manager reports a discrepancy when 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.

---

#### 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.

For more information on configuring VLANs, see the document *Creating and Maintaining VLANs* at the following location:

[http://www.cisco.com/en/US/partner/products/hw/switches/ps637/products\\_configuration\\_guide\\_chapter09186a008007f261.html](http://www.cisco.com/en/US/partner/products/hw/switches/ps637/products_configuration_guide_chapter09186a008007f261.html)

## VLAN Name Conflict

Campus Manager reports a discrepancy 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/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 discrepancy because Campus Manager 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.

## VLAN Index Conflict

Campus Manager reports a discrepancy 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/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 discrepancy because Campus Manager 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.

## Trunk VLAN Protocol Mismatch

Campus Manager 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, Campus Manager 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.

## VTP Disconnected Domain

Campus Manager 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.

## No VTP Server in Domain

Campus Manager 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 the 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**

Campus Manager 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. Campus Manager 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.

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

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw\\_8\\_1/config\\_gd/vtp.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_1/config_gd/vtp.htm)

## EtherChannel Port Spanning Tree Not Disabled

Campus Manager reports a discrepancy when Spanning Tree is enabled on EtherChannel links.

Spanning Tree Protocol is not supported with Catalyst software release 2.3 and lower. Therefore, disable Spanning Tree on switches with active VLANs that span Fast EtherChannel connections.

For Catalyst software release 3.1 and higher, configure Spanning Tree on Fast EtherChannel links.

## ATM-VLAN With no Entry in LE Config Server

Campus Manager reports a discrepancy when the LECS database does not have corresponding entry for a LANE Broadcast and Unknown Server (BUS).

### Impact

When the LECS database does not have an entry for a LANE BUS, the LAN Emulation Clients (LECs) cannot contact the LAN Emulation Server (LES) BUS. This will affect the network connectivity.

### Fix

Create an entry for the LANE BUS in the LECS database.

For more information on ATM networks, see the document *Designing ATM Internetworks* at the following location:

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2008.htm>

## ATM-VLAN With LE Server Having no Entry in LE Config Server

Campus Manager reports a discrepancy when there is no entry for an Emulated LAN (ELAN) in the LAN Emulation Configuration Server (LECS).

The LECS maintains a database of ELANs and the ATM addresses of the LAN Emulation Servers (LES) that control the ELANs.

**Impact**

If there is no entry for an ELAN in the LECS database, the LANE clients in the corresponding ELAN will not be able to join the ELAN. This affects the network connectivity and flow of traffic.

**Fix**

Create an entry for the ELAN in the LECS database.

For more information on ATM networks, see the document *Designing ATM Internetworks* at the following location:

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2008.htm>

## More Than One LE Config Server Present in a Single ATM Domain

Campus Manager reports a discrepancy when more than one LECS is found in an ATM cloud in a LANE 1.0 specification.

**Impact**

When there is more than one LECS in an ATM cloud, it results in faulty and inconsistent behavior of the LANE. The network connectivity is affected.

**Fix**

Ensure that there is only one LECS in an ATM cloud.

For more information on ATM networks, see the document *Designing ATM Internetworks* at the following location:

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2008.htm>

## Partitioned ATM-VLAN

Campus Manager reports a discrepancy when there is a partitioned ATM-VLAN, that is, when clients of one ELAN have joined a different LES.

**Impact**

The clients of the ELAN which have become part of another LES cannot communicate with other clients. The network connectivity in the ATM-VLAN is disrupted.

For more information on ATM networks, see the document *Designing ATM Internetworks* at the following location:

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2008.htm>

## DRiP Enabled VLAN

Campus Manager reports a discrepancy when there are two identical Token Ring Concentrator Relay Function (TrCRF) in a Token Ring Bridge Relay Function (TrBRF).

The Duplicate Ring Protocol (DRiP) is a Cisco proprietary protocol that runs on Cisco routers and switches that support switched VLAN networking and is used to identify active Token Ring VLANs.

DRiP maintains the status of TrCRFs and uses this information to determine whether there are multiple TrCRFs active in a TrBRF.

### Impact

If you enable TrCRF on more than one switch or router, the ports associated with the TrCRF are disabled on all switches. A router will not disable the internal ring used for source-route bridging, and for routing source-routed traffic.

Instead, the router displays the following error message to indicate that two identical TrCRFs exist:

```
DRIP conflict with CRF <vlan-id>
```

### Fix

Assign a unique ring number for each TrCRF.

## Trunk Negotiation Enabled

Campus Manager reports a discrepancy when trunk mode on any one 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 combination:

- On/Auto
- On/Desirable

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

**Impact**

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

**Fix**

To fix the discrepancy on switches using Cisco IOS, enter the following at the CLI:

```
switchport trunk encapsulation dot1q | isl  
switchport mode trunk  
end
```

To fix the discrepancy on switches using Catalyst operating system, enter the following at the CLI:

```
set trunk mod/port on Dot1Q
```

Or

```
set trunk mod/port on ISL
```

■ Interpreting Discrepancies