Before using this information and the product it supports, read the information in "Notices" on page 75.
Contents

About this guide ........................................ v
Who should read this guide ............................ v
Publications ............................................ v
  Tivoli Switch Analyzer library ........................ v
  Prerequisite publications .............................. v
  Accessing publications online ........................ v
  Ordering publications ................................ vi
Accessibility ........................................... vi
Tivoli technical training ................................ vi
Support information ................................... vi
Participating in newsgroups ............................. vii
Conventions used in this guide ........................ vii
  Typeface conventions ................................. vii
  Operating system-dependent variables and paths .... viii

Chapter 1. Introduction ................................. 1
Managing layer 2 devices ................................. 1
Features of Tivoli Switch Analyzer ...................... 1

Chapter 2. Installing Tivoli Switch
Analyzer .................................................. 3
Checking prerequisites ................................... 3
Ensuring accurate layer 3 topology information ........ 4
  Discovering the layer 3 network ..................... 4
  Eliminating network islands ......................... 5
  Finding missing switches ............................ 5
Running the installation utility ......................... 6
  Running the installation program silently .......... 7
Verifying the installation ................................ 7
Configuring the Tivoli NetView Web server .......... 8
Uninstalling Tivoli Switch Analyzer ................. 9
  Running the uninstallation program silently ...... 9

Chapter 3. Layer 2 discovery ......................... 11
The layer 2 discovery process ......................... 11
Adding new device types ................................ 12
Selectively disabling discovery ....................... 12
Rediscovering the layer 2 topology .................. 13
  Rediscovering the entire network ................... 13
  Rediscovering specific devices ..................... 13
Generating discovery reports ......................... 14

Chapter 4. Fault detection and root
cause analysis ........................................ 15
Fault detection mechanisms ........................... 15
  Port status monitoring ................................ 15
Impact-based fault detection .......................... 16
Root cause analysis ................................... 17
  Tivoli NetView integration ........................... 18
  Layer 3 correlation .................................... 19
  Redundant path correlation ........................... 19
  Correlator processing ................................. 20
Tivoli NetView topology maps .......................... 21
Viewing correlated layer 2 status ..................... 22
  Viewing layer 2 status using the Object Properties window ................ 22
  Viewing layer 2 status using the System Configuration view ................ 22
  Viewing layer 2 status from a command line ....... 22

Chapter 5. Viewing layer 2 topology ............... 25
Physical view ............................................ 25
  Opening the Physical view ............................ 25
  Understanding the Physical view window ........... 25
  Hop count ............................................. 27
VLAN view .............................................. 27
  Opening the VLAN view ............................... 28
  Understanding the VLAN view window ............... 29
Selecting a new VLAN to view ......................... 29
Point to Point view ..................................... 29
  Opening the Point to Point view .................... 30
  Understanding the Point to Point view window .... 30
Understanding status in the layer 2 views ........... 31
Taking action on an object ............................ 32
Getting help ............................................. 33
  Getting Tivoli Switch Analyzer help ............... 33
  Getting Tivoli NetView help ......................... 33
Tivoli Switch Analyzer tool bar ...................... 33
Understanding deleted views ......................... 34
Scenarios using the layer 2 views ................... 34

Chapter 6. Generating reports ....................... 37
Generating the summary report ....................... 37
  Summary report contents ............................ 37
Generating the discovery report ...................... 40
Generating an impact analysis report ............... 41
Generating the layer 2 status report ................. 41
  Layer 2 status report contents ..................... 42

Chapter 7. Administration ............................ 45
Starting and stopping Tivoli Switch Analyzer ........ 45
  Starting the daemon .................................. 45
  Stopping the daemon ................................. 45
Tivoli Switch Analyzer processes .................... 46
Changing the cache frequency ......................... 47
Cache files ............................................. 47
Configuring correlator options ....................... 48
Configuring the port status monitor .................. 50
  Configuring which switches to monitor ............. 50
  Port status monitor polling ......................... 51
Configuring port status monitoring options ........ 52
Tivoli Switch Analyzer logs .......................... 52
  Gathering debugging information ................... 53
  Log descriptions ............................... 53
Correlator client ..................................... 55
Configuring the Web servlet .......................... 56
  Configuring the ClientRequestTimeout value ...... 56
Web servlet and console debugging ................... 57
About this guide

This document provides information about IBM® Tivoli® Switch Analyzer, Version 1.3. Tivoli Switch Analyzer extends the ability of the Tivoli NetView® product to perform root cause analysis of layer 2 problems. Tivoli Switch Analyzer is tightly integrated with the Tivoli NetView product. Working with Tivoli Switch Analyzer, the Tivoli NetView product can isolate problems to non-IP ports on managed layer 2 devices. Using Tivoli Switch Analyzer, Tivoli NetView users can view the status of switch ports and view the impact of taking down a switch.

Who should read this guide

This guide is for system administrators who perform the following tasks:
• Installation
• Configuration
• Administration
• Problem diagnosis

Publications

This section lists publications in the Tivoli Switch Analyzer library and related documents. It also describes how to access Tivoli publications online and how to order Tivoli publications.

Tivoli Switch Analyzer library

The following publications are in the Tivoli Switch Analyzer library:
• Tivoli Switch Analyzer Administrator’s Guide, GC32-9415-00
  Provides information about installing, configuring, and using Tivoli Switch Analyzer.
• Tivoli Switch Analyzer Release Notes, GI11-4076-00
  Provides the latest information about installation, system requirements, known problems, and limitations.

Prerequisite publications

To use the information in this guide effectively, you must have some prerequisite knowledge, which you can obtain from the following guide:
• See the Tivoli NetView for UNIX® library or the Tivoli NetView for Windows® library for information about the Tivoli NetView product.

Accessing publications online

The product CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both.

To open the Tivoli Switch Analyzer Release Notes using a Web browser, open the tsarmstftrm.htm file. The file is in the appropriate publications directory on the product CD.

To open the Tivoli Switch Analyzer Administrator’s Guide using a Web browser, open the tsaaamstftrm.htm file. The file is in the appropriate publications directory on the product CD.
IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli software information center Web site. Access the Tivoli software information center by first going to the Tivoli software library at the following Web address:


Scroll down and click the Product manuals link. In the Tivoli Technical Product Documents Alphabetical Listing window, click the Tivoli Switch Analyzer link to access the product library at the Tivoli software information center.

**Note:** If you print PDF documents on other than letter-sized paper, set the option in the File → Print window that allows Adobe Reader to print letter-sized pages on your local paper.

**Ordering publications**

You can order many Tivoli publications online at the following Web site:


You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

**Accessibility**

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. When installing this product, you can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. You can generate all Tivoli Switch Analyzer reports using a command line interface instead of the mouse. You can also magnify what is displayed on your screen.

**Tivoli technical training**

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site:

http://www.ibm.com/software/tivoli/education

**Support information**

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

- Searching knowledge bases: You can search across a large collection of known problems and workarounds, Technotes, and other information.
- Obtaining fixes: You can locate the latest fixes that are already available for your product.
- Contacting IBM Software Support: If you still cannot solve your problem, and you need to work with someone from IBM, you can use a variety of ways to contact IBM Software Support.
For more information about these three ways of resolving problems, see “Support information” on page 71.

**Participating in newsgroups**

User groups provide software professionals with a forum for communicating ideas, technical expertise, and experiences related to the product. They are located on the Internet and are available using standard news reader programs. These groups are primarily intended for user-to-user communication and are not a replacement for formal support.

To access a newsgroup, use the instructions appropriate for your browser.

IBM Tivoli Switch Analyzer

`news://news.software.ibm.com/ibm.software.tivoli.switch-analyzer`

IBM Tivoli NetView for UNIX and IBM Tivoli NetView for Windows

`news://news.software.ibm.com/ibm.software.netview`

**Conventions used in this guide**

This guide uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

**Typeface conventions**

This guide uses the following typeface conventions:

**Bold**
- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as Tip: and Operating system considerations)
- Keywords and parameters in text

**Italic**
- Words defined in text
- Emphasis of words (words as words)
- New terms in text (except in a definition list)
- Variables and values you must provide

**Monospace**
- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options
Operating system-dependent variables and paths

This guide uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace $variable with %variable% for environment variables and replace each forward slash (/) with a backslash (\) in directory paths. The names of environment variables are not always the same in Windows and UNIX. For example, %TEMP% in Windows is equivalent to $tmp in UNIX.

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.
Chapter 1. Introduction

IBM Tivoli Switch Analyzer extends the ability of the IBM Tivoli NetView product to perform root cause analysis of layer 2 problems. By using Tivoli Switch Analyzer with the Tivoli NetView product, you can isolate network problems to non-IP ports on managed layer 2 devices. You can also view the port-level discovery of switches and view *what-if* scenarios showing the impact of taking down a switch.

Managing layer 2 devices

The Tivoli NetView product provides network management and root-cause analysis at layer 3 (the network layer) of the standard Open Systems Interconnection (OSI) model. This means that the Tivoli NetView product uses the IP addresses of managed devices to gather routing and topology data, to identify problems, and to perform root cause analysis.

However, layer 3 network management might not be able to correctly identify a problem that occurs at layer 2 (the data link layer) of the OSI model. Without layer 2 network management, a failure in a layer 2 device such as a switch is detected only as an inability to reach connected layer 3 devices. This can result in incorrect root cause analysis, showing the unreachable layer 3 device as the cause of a problem that is actually affecting a layer 2 device.

For example, consider a layer 3 router that is connected (on the downstream side) to a layer 2 switch. If the switch port to which the router is connected fails, the router becomes inaccessible. In this case, the root cause of the problem is the switch port failure. Because the switch port outage is not detected by the Tivoli NetView product, the router appears to be the device with the problem.

Using Tivoli Switch Analyzer, Tivoli NetView can detect the layer 2 failure by directly polling the switch at the data link layer. In addition, Switch Analyzer can perform root cause analysis using both layer 2 and layer 3 data.

Features of Tivoli Switch Analyzer

Tivoli Switch Analyzer provides the following functions:

**Port status monitoring**
Port status monitoring uses continual polling to detect outages affecting layer 2 devices, even if no layer 3 outage has occurred.

**Layer 2 topology visualization**
The following views display the layer 2 topology with status, providing enhanced visual troubleshooting capability:
- Physical view
- Point to Point view
- VLAN view.

For details on the views, see Chapter 5, “Viewing layer 2 topology,” on page 25.
Root cause analysis
Layer 2 root cause analysis augments the Tivoli NetView layer 3 root cause function. This includes enterprise traps used to identify the layer 2 root cause.

Topology map status
Topology map status for switches displays layer 2 problems that are otherwise hidden from Tivoli NetView layer 3 monitoring. This status is integrated with the IP status to alert users to layer 2 or layer 3 connectivity problems. An object database field for switches contains the layer 2 status. Three Tivoli NetView status traps for layer 2 device status display changes to layer 2 status. For more information, see “Tivoli NetView topology maps” on page 21.

Impact analysis tools
The impact analysis tool provides a what if function that provides a way to determine which devices are affected if a specific switch fails.

Reports
Reports provide details about the layer 2 discovery, port connectivity, and port status.

Point-to-point link processing
The point-to-point link processing function provides concise information about correlated events for point-to-point protocols, including frame relay, PPP, and ATM.

Tivoli NetView integration
The Tivoli Switch Analyzer itsl2 daemon runs as a well-behaved daemon that is fully synchronized with other Tivoli NetView daemons and databases. Layer 2 reports are available from integrated menus that are available using the Tivoli NetView Web console and native console. For more information, see “Tivoli NetView integration” on page 18.

Tivoli Enterprise Console® integration
Tivoli Switch Analyzer uses Tivoli Enterprise Console events and rules that are shipped with the Tivoli Enterprise Console product to help operators locate the source of a problem and follow the progress of its resolution. These rules are specifically designed to correlate layer 2 and layer 3 traps, perform housekeeping on the traps, and update the status of the problem as it progresses to resolution.
Chapter 2. Installing Tivoli Switch Analyzer

This topic explains how to install Tivoli Switch Analyzer on your system and configure it for optimal layer 2 network management.

This chapter contains the following installation tasks:

1. Refer to the installation checklist in the Tivoli Switch Analyzer Release Notes.
2. Check the prerequisites to make sure Tivoli Switch Analyzer can manage the layer 2 devices in your environment (see "Checking prerequisites").
3. Resolve any problems with layer 3 network topology data (see "Ensuring accurate layer 3 topology information" on page 4).
4. Run the installation utility to install the Tivoli Switch Analyzer product on your system (see "Running the installation utility" on page 6).
5. Verify that the product is correctly installed (see "Verifying the installation" on page 7).
6. Configure the NetView Web server (see "Configuring the Tivoli NetView Web server" on page 8).

Checking prerequisites

Before installing Tivoli Switch Analyzer, make sure your environment satisfies the applicable prerequisites.

Verify that the system where you are installing Tivoli Switch Analyzer satisfies the hardware and software prerequisites, including the correct version of the Tivoli NetView product and required Tivoli NetView interim fixes. Refer to the chapter on installing and upgrading in the IBM Tivoli Switch Analyzer Release Notes for prerequisite system and software requirements as well as an installation checklist.

Also verify that Tivoli Switch Analyzer supports port discovery for the switches you want to manage. For switch ports to be discovered by Tivoli Switch Analyzer, a switch must meet the following criteria:

- It must support the bridge MIB defined by RFC 1493, including the bridge forwarding database.
- For the discovery report to show connections to the switch, it must be reachable through a fully discovered layer 3 connection path from the Tivoli NetView server.
- It must not have multiple IP addresses.
- If the switch is connected to multiple VLANs and is not manufactured by Cisco Systems, it must not use community string indexing (CSI). Tivoli Switch Analyzer supports CSI only on Cisco Systems switches. Switches from other vendors that use CSI are currently limited to discovery of VLAN1.

If you are unsure about which switch ports Tivoli Switch Analyzer can discover and manage in your network, you can use the IBM Global Services ITSATool application to find out. For more information, contact your IBM Global Services representative.
Ensuring accurate layer 3 topology information

Before installing Tivoli Switch Analyzer, make sure you resolve any problems affecting the accuracy of layer 3 topology information.

The ability of Tivoli Switch Analyzer to accurately discover the connected layer 2 topology and perform root cause analysis depends upon the availability of accurate information from the MIBs of managed devices and from the Tivoli NetView database. If your network has not previously been managed at the layer 2 level, there might be undetected problems in the layer 3 topology that affect the accuracy of this information. Before installing Tivoli Switch Analyzer, do the following steps to identify and resolve these problems:

1. “Discovering the layer 3 network”
2. “Eliminating network islands”
3. “Finding missing switches” on page 5

Discovering the layer 3 network

The first step in ensuring accurate topology information is to discover the layer 3 network.

1. Using the Tivoli NetView product, discover the layer 3 network that you want to manage. For information about how to do this, see the Tivoli NetView documentation.

2. Make sure the Tivoli NetView server itself (the system on which the Tivoli NetView product is installed) has been discovered. You can determine this using any of the following methods:
   - Look at the Tivoli NetView topology map view and confirm that the icon representing the Tivoli NetView server has an inner graphic.
   - Check the Tivoli NetView object definition for the Tivoli NetView server and confirm that the isSNMPSupported field is set to true.
   - Make sure there are no DNS discrepancies, and that the Tivoli NetView server hostname and IP address correctly resolve to each other.

Note: If the itsl2 daemon attempts to start before the Tivoli NetView server is in the Tivoli NetView topology, you get the following error in the correlator log:

```
Cannot find node for management system host: NetView server [ip address]
```

Check to make sure this node has been discovered by Tivoli NetView and then restart the itsl2 daemon.

If you have a large network, let Tivoli NetView discover the network before starting the itsl2 daemon. This allows time for the Tivoli NetView management machine to be discovered and makes for a more efficient discovery.

Eliminating network islands

After you have discovered the layer 3 network, identify and eliminate any network islands to ensure a more complete and accurate discovery report.

An island is a portion of the network that seems to be unconnected to the rest of the network in the topology view. A network island indicates that one or more routers have not been discovered. Because the Tivoli Switch Analyzer correlator works only with switches within the contiguous connected topology, minimizing
the number of network islands increases your ability to take advantage of layer 2 root cause analysis. (The port status monitor can manage switches located in a remote campus.)

Tivoli Switch Analyzer manages only devices that can be reached through a discovered layer 3 connection path, so any islands must be eliminated by identifying and discovering the missing routers. In most cases, failure to discover a router results when the community name of the router is not listed in the communityNames.conf file. To correct this problem, follow these steps:

1. Identify the router that was not discovered by the Tivoli NetView product and determine its SNMP community name.
2. Stop the netmon daemon.
3. Add the new community name to the communityNames.conf file. You can do this either by editing the file with a text editor, or by using the Tivoli NetView SNMP Configuration window.
4. Restart the netmon daemon.
5. Demand poll the router.

Note: By default, the Tivoli NetView product is limited to a maximum of 7 community names in the communityNames.conf file. You can change this default by adding the MaximumCommunityNames option in the /usr/OV/conf/netmon.conf file. For more information, refer to the Tivoli NetView documentation.

If it is not possible to gain SNMP access to one or more routers, you can create a custom link in Tivoli NetView between two routers. On the Tivoli NetView maps this shows as a dot-dashed line which indicates a logical link or tunnel across an unmanaged region. Refer to the Tivoli NetView documentation for more information.

Finding missing switches
After discovering the network at layer 3, make sure all switches in the network are correctly identified as switches.

Tivoli Switch Analyzer can manage only switches that have been discovered at layer 3 by the Tivoli NetView product and defined as layer 2 devices in the Tivoli NetView database. To make sure all of the switches you want to manage have been correctly discovered at layer 3, follow these steps:

1. To create a list of identified layer 2 devices, run this command:

   /usr/OV/bin/ovtopodump -X

2. Check the generated list to make sure it includes all of the layer 2 devices you want to manage. Any switches not in the list were not discovered by the Tivoli NetView product, or were not identified as switches.
3. For each missing switch, follow these steps:
   a. Ping the switch to ensure it is reachable.
   b. Demand poll the nearest router, or put an entry in the seed file for the switch.
   c. Make sure the SNMP agent is running on the switch.
   d. Make sure the SNMP community name for the switch is defined in the communityNames.conf file.
   e. Check the /usr/OV/conf/oid_to_type file and make sure the switch is listed with the correct sysObjectID flag. For the switch to be recognized as a
layer 2 device, the sysObjectID flag must be set to either B (bridge or switch) or H (multiport repeater or hub). A switch must not be set to G (gateway or router). See “Adding new device types” on page 12 for more information on updating the oid_to_type file.

Determining why a device is not classified as a switch

If the Tivoli NetView product has not classified a layer 2 device as a switch, you can use the `ovtopodump` command to find out why. Run the following command, specifying the TCP/IP host name of the device that you want information about:

```
/usr/OV/bin/ovtopodump -X hostname
```

When applicable, the command output indicates one of the following reasons in the Layer 2 OID? column:

- There is no SNMP access to that switch.
- The SNMP sysObjectID is not defined in the oid_to_type file.

Running the installation utility

To install the Tivoli Switch Analyzer product, run the installation utility. You can also install Tivoli Switch Analyzer in silent mode.

1. Log in to a user ID with the necessary privileges:
   - On a Linux® or UNIX system, log in as a root user.

   **Note:** Make sure the following line is included in your startup environment file:

   ```
   . /usr/OV/bin/NVenvironment
   ```

   This line should be added during the Tivoli NetView post-installation procedure; it provides the environment variables required for correct operation of the Tivoli NetView and Tivoli Switch Analyzer command-line utilities. (Note the space after the leading period.)

   - On a Windows system, log in to an account with administrator privileges.

2. Insert the Tivoli Switch Analyzer product CD in the CD-ROM drive.

3. On a Windows system, the installation utility starts automatically. If it does not start, or if you are installing on a Linux or UNIX system, go to a command prompt and start the installation program:

   - On a Linux or UNIX system, run the `switchanalyzer_UNIX_install` command.
   - On a Windows system, run the `\Windows\switchanalyzer_install.exe` command.

4. Follow the instructions on your screen to complete the installation.

   **Note:** The installation process stops the Tivoli NetView netmon daemon. During the installation, a prompt is displayed asking whether you want to restart all stopped Tivoli NetView daemons, including the Tivoli Switch Analyzer daemon (itsl2). You can click Yes to start the daemons, or No if you want to start them manually. (For information about starting the itsl2 daemon manually, see “Starting the daemon” on page 45.)

5. Restart all Tivoli NetView native consoles.
After the installation is complete, a window is displayed detailing the results of the installation.

**Running the installation program silently**

You can automate Tivoli Switch Analyzer installation by using command-line options in a response file.

To silently install Tivoli Switch Analyzer, do the following steps:

1. Review the information in the response file. You can find the response file on the Tivoli Switch Analyzer CD in the following location:
   - On a Windows system: `\Windows\installresponsefile.txt`
   - On a UNIX system: `/UNIX/installresponsefile.txt`
2. If needed, modify the file. Be sure to save the file after you modify it.
3. From the command prompt, type the following command:
   - On a Windows system: `switchanalyzer_install.exe –options <location of response file>\installresponsefile.txt`
   - On a UNIX system: `switchanalyzer_install –options <location of response file>/installresponsefile.txt`

Make sure to type the fully-qualified path for the location of the response file.

   Make sure the installation starts.

**Note:** When running the command on a Windows system, the prompt returns just after submission but continues to run in the background. To have the prompt wait until completion, run the command with `start /w` as in the following example:

   `start /w windows\switchanalyzer_install.exe`

4. The installation is complete when the command returns and the command prompt is displayed.

**Verifying the installation**

Follow these steps to verify that Tivoli Switch Analyzer has been installed correctly.

1. If it is not already running, start the Switch Analyzer itsl2 daemon. (For more information, see "Starting the daemon" on page 45.)
2. Run the `ovstatus` command to verify that the itsl2 daemon is running:

   `/usr/OV/bin/ovstatus itsl2`

   You should see the following information:

   object manager name: itsl2
   behavior: OVs WELL_BEHAVED
   state: RUNNING
   PID: 19838
   last message: Initialization complete.
   exit status: -

   If you cannot start the itsl2 daemon, check that the Tivoli NetView server has been discovered. If the Tivoli NetView server has not been discovered, the itsl2 daemon does not start. Look for the following error message in the `/usr/OV/ITSL2/log/coordinator.log` file:

   Cannot find node for management system host: `servername [x.x.x.x]`

   where `servername` is the host name and `x.x.x.x` is the IP address of the Tivoli NetView server. For information on how to check if the Tivoli NetView server
has been discovered, see [“Discovering the layer 3 network” on page 4]. Restart the itsl2 daemon after the Tivoli NetView server has been discovered.

3. Using the Tivoli NetView console, verify that the Tivoli Switch Analyzer traps have been configured.

To see the configured traps on a Windows system, follow these steps:

a. In the Tivoli NetView console, click Options → Trap Settings. The Trap Settings window opens.

b. In the Select an enterprise field, select ITSL2. The Tivoli Switch Analyzer traps are displayed (see [“Traps and events” on page 60] for more information).

To see the configured traps on a UNIX system, follow these steps:


b. In the Enterprise Identification field, select ITSL2. The Tivoli Switch Analyzer traps are displayed (see [“Traps and events” on page 60] for more information).

---

### Configuring the Tivoli NetView Web server

Before you can access Tivoli Switch Analyzer actions, you must configure the Tivoli NetView Web server to make the actions available to the required user roles.

To make the actions available to a role, follow these steps:

1. From the main menu of the Tivoli NetView native console, open the Web Console Security window:
   - On a Linux or UNIX system, click Administer → Security Administration → Web Console Security.
   - On a Windows, system, click Options → Web Console Security.

2. Make sure the Tivoli Switch Analyzer actions are checked for the user roles that require access. Select all of the following actions:
   - Impact Analysis
   - Impact Analysis (connectors)
   - Discovery
   - Rediscovery
   - Layer 2 Status

   **Note:** The Switch Analyzer actions are checked by default for the SuperUser and Admin roles.

3. From the main menu, click File → Save.

4. From the main menu, click File → Restart Web Server to integrate the menu items.

The Tivoli NetView Web console users with the appropriate roles now have access to the Tivoli Switch Analyzer actions through the Tivoli NetView Web console menus.

**Note:** By default, operators do not have the authority to perform rediscovery.
Uninstalling Tivoli Switch Analyzer

The Tivoli Switch Analyzer installation process also creates a utility you can use to remove the product from your system.

1. To uninstall Tivoli Switch Analyzer, run one of the following commands:
   - On a Windows system, run
     \usr\OV\ITSL2\_uninst\uninstaller.exe
   - On a Linux or UNIX system, run
     # cd /usr/OV/ITSL2
     #_uninst/uninstaller.bin

   This command launches a utility for uninstalling Tivoli Switch Analyzer. Follow the instructions on your screen to remove Tivoli Switch Analyzer from your system.

   **Note:** The Tivoli NetView netmon daemon is stopped and restarted during uninstallation.

2. From the main menu of the Tivoli NetView native console, open the Web Console Security window:
   - On a Linux or UNIX system, click **Administer → Security Administration → Web Console Security**.
   - On a Windows, system, click **Options → Web Console Security**.

3. From the main menu, click **File → Save**.
4. From the main menu, click **File → Restart Web Server** to integrate the menu items.
5. Restart all Tivoli NetView native and Web consoles.
6. From the main menu of the Tivoli NetView native console, open the Web Console Security window:
   - On a Linux or UNIX system, click **Administer → Security Administration → Web Console Security**.
   - On a Windows, system, click **Options → Web Console Security**.
7. From the main menu, click **File → Save**.
8. From the main menu, click **File → Restart Web Server** to integrate the menu items.

**Running the uninstallation program silently**

You can automate Tivoli Switch Analyzer uninstallation by using command-line options in a response file.

To silently uninstall Tivoli Switch Analyzer, do the following steps:
1. Review the information in the response file. You can find the response file in the following location:
   - On Windows systems: %NV_DRIVE%\usr\OV\ITSL2\uninstallresponsefile.txt
   - On UNIX systems: /usr/OV/ITSL2/uninstallresponsefile.txt
2. If needed, modify the file. Be sure to save the file after you modify it.
3. From the command prompt, run the following command:
   - On Windows systems: switchanalyzer_uninstall.exe –options <location of response file>\uninstallresponsefile.txt
   - On UNIX systems: switchanalyzer_uninstall –options <location of response file>/uninstallresponsefile.txt
Make sure to type the fully-qualified path for the location of the response file. The uninstallation program starts.

**Note:** When running the command on a Windows system, the prompt returns just after submission but continues to run in the background. To have the prompt wait until completion, run the command with `start /w` as in the following examples:
```
start /w _uninst\uninstaller.exe
start /w _uninst\uninstaller.exe -options uninstallresponsefile.txt
```

4. The uninstallation is complete when the command returns and the command prompt is displayed.
Chapter 3. Layer 2 discovery

Tivoli Switch Analyzer extends the network topology discovered by Tivoli NetView to include layer 2 information. The layer 2 discovery process depends upon the availability of valid layer 3 topology data; after both discovery processes are complete, Tivoli Switch Analyzer can manage layer 2 devices and perform root-cause analysis using both layer 2 and layer 3 data.

The layer 2 discovery process

Discovery of the layer 2 network occurs automatically when the itsl2 daemon starts. The layer 2 discovery process includes the following steps:

1. During installation, Tivoli Switch Analyzer reads the contents of the Tivoli NetView /usr/OV/conf/oid_to_type file. This file lists the object identifiers (OIDs) of the devices discovered by Tivoli NetView at layer 3 and identifies the type of each device.
   Tivoli NetView examines the flags in the topology attributes field to determine whether each listed device is a layer 2 device or a layer 3 device. A layer 2 device is indicated by the presence of either or both of the following flags:
   - B (bridges and switches)
   - H (multi-port repeaters or hubs)
   
   **Note:** A layer 2 device must not be listed with the G flag (which indicates a gateway or router).

2. Using this information, the installation process creates the /usr/OV/ITSL2/conf/files/l2_oids.cfg file, which lists the OIDs of the identified layer 2 devices. (This file can be updated later if new OIDs have been added to the oid_to_type file; for more information, see “Adding new device types” on page 12.)

3. When the itsl2 daemon starts, it downloads the topology from Tivoli NetView. It reads the list of devices in the l2_oids.cfg file and attempts to discover the layer 2 information from those devices using SNMP queries. First, the daemon uses the community name defined in the Tivoli NetView SNMP configuration to query the dot1dBridge.dot1dBase.dot1dBaseBridgeAddress object from the bridge MIB followed by other SNMP queries. If the SNMP agent on a device does not respond to the query, layer 2 discovery for that device fails.

4. The daemon then discovers the layer 2 topology by doing additional SNMP queries using both standard and proprietary MIBs. For Cisco Systems switches with multiple VLANs defined, the itsl2 daemon uses community string indexing to query the dot1dBridge MIB for topology information.

5. The resulting layer 2 topology is stored in the internal Tivoli Switch Analyzer layer 2 topology cache. The topology information is also written to the /usr/OV/ITSL2/cache/topo_cache file, which is used for generating reports.

   **Note:** By default, the cache file is updated every 15 minutes. (For information about changing this interval, see “Changing the cache frequency” on page 47.) Newly discovered layer 2 topology information does not appear in generated reports until the cache file is updated; however, you can force an immediate update when generating a report. For more information, see Chapter 6, “Generating reports,” on page 37.
6. For each switch listed in the port status monitor switch table, the daemon queries the port table from the bridge MIB. By default, these ports are the ones that are polled by the port status monitor.

If the itsl2 daemon encounters an error during layer 2 discovery, it writes an error message to the /usr/OV/ITSL2/log/l2_topo_adapter.log file. You can check this file to see which devices have problems that prevent discovery, and to identify the causes of these problems. Prior to Tivoli Switch Analyzer Version 1.3, this log file was named topo_server.log.

Note: Unmanaging layer 2 switches from Tivoli NetView is not recommended because missing layer 2 information can negatively affect complete discovery of the layer 2 topology around that device. This causes unpredictable results.

Adding new device types

If you add a new layer 2 device type to the Tivoli NetView oid_to_type file after installing Tivoli Switch Analyzer, you must update the Tivoli Switch Analyzer configuration to allow layer 2 discovery of the new device.

Tivoli Switch Analyzer attempts to discover only devices whose OIDs are listed in the l2_oids.cfg file, which is created during installation based on the contents of the /usr/OV/conf/oid_to_type file. To rebuild this file using an updated oid_to_type file, follow these steps:

1. Check the Tivoli NetView oid_to_type file and make sure the device type is listed with the correct sysObjectID flag. For the switch to be recognized as a layer 2 device, the sysObjectID flag must be set to either B (bridge or switch) or H (multislot repeater or hub). Tivoli Switch Analyzer does not recognize as layer 2 any device defined with the G flag (gateway or router).

2. Run the importNvOids command:
   • On a Linux or UNIX system, run /usr/OV/ITSL2/netview/importNvOids.
   • On a Windows system, run \usr\OV\ITSL2\bin\importNvOids.

3. Delete the node from Tivoli NetView and rediscover it. Check that Tivoli NetView has rediscovered it correctly as a switch by running the ovtopodump -X command and checking it is present in the output.

4. Restart the itsl2 daemon.

Selectively disabling discovery

In some situations, you might want to disable layer 2 discovery of a specific type of device. Tivoli Switch Analyzer uses the l2_oids.cfg configuration file to determine which devices are discovered. To disable discovery for a device, follow these steps:


2. Add a new entry or modify the existing entry describing the device or devices for which you want to disable discovery. Each entry in the l2_oids.cfg file includes five fields separated by vertical bar characters (|):
   
   type|description|OID|IP_address|discover|

The fields are as follows:

- **type**: The type of entry. In the l2_oids.cfg file, this should always be l2_oid.
Rediscovering
Rediscovering
Rediscovering

To

Note:

has

If

"Starting

network

If

should

discovery_interval

hours.

network

Rediscovery

periodically

The

discover

Whether devices matching this entry should be discovered at layer 2. The value of this field should be Y (discover the device) or N (do not discover the device).

To disable discovery of all devices of a certain type, find the entry with the corresponding object identifier and change the value of the discover field to N. To disable discovery of a single, specific device, add an entry describing that device (including the IP address), specifying N in the discover field.

Rediscovering the layer 2 topology

The itsl2 daemon automatically redisCOVERs the network when it starts, and it periodically repeats this rediscovery by polling all of the layer 2 devices. Rediscovery detects any changes in the layer 2 topology since the last time the network was discovered. By default, automatic rediscovery takes place every 24 hours. The timer begins at startup. To change this interval, modify the discovery_interval parameter in the /usr/OV/ITSL2/conf/l2_topo_adapter.ini file and specifying, in minutes, how long you want the daemon to wait before each automatic rediscovery.

If you corrected problems that were preventing complete layer 2 discovery, you should rediscover the layer 2 topology.

Note: Operators do not have the authority to perform rediscovery.

Rediscovering the entire network

If you corrected a large number of problems, you should rediscover the entire network by stopping and restarting the itsl2 daemon. For more information, see “Starting and stopping Tivoli Switch Analyzer” on page 45.

Rediscovering specific devices

If you resolved only a small number of problems, you do not need to rediscover the entire network. Instead, you can rediscover only the devices whose information has changed.

Note: If the devices you want to discover were not previously identified as layer 2 devices, you must restart the itsl2 daemon. This is the case if the /usr/OV/ITSL2/conf/files/l2_oids.cfg file has changed (for example, if you ran the importNvOids command). Changes to l2_oids.cfg take effect only when the itsl2 daemon starts.

To rediscover one or more devices, follow these steps:
1. In the Tivoli NetView map, select the layer 2 device you want to rediscover.
2. From the main menu, select Monitor → Layer 2 → Rediscover.
To determine the result of the rediscovery, check the /usr/OV/ITSL2/log/l2_topo_adapter.log file. For more information, see “The layer 2 discovery process” on page 11.

Generating discovery reports

After layer 2 discovery has completed, you can generate reports from the discovered topology information. You can use these reports to verify the layer 2 topology and to resolve any discovery problems.

1. To see the results of discovery for all layer 2 devices, generate the summary report. For more information, see “Generating the summary report” on page 37.

2. To see what devices and connections have been discovered, generate the discovery report. For more information, see “Generating the discovery report” on page 40.

3. To see summary information for managed switches, followed by detailed information about each managed switch and port, generate the layer 2 status report. For more information, see “Generating the layer 2 status report” on page 41.
Chapter 4. Fault detection and root cause analysis

Tivoli Switch Analyzer extends the Tivoli NetView layer 3 fault detection and root-cause analysis capabilities to include layer 2 problems and their impact.

Specifically, Tivoli Switch Analyzer performs the following functions:

- It detects outages affecting switch ports, using two separate mechanisms (the correlator and the port status monitor). Fault detection is available for all layer 2 devices, including multilayer switches and switches within a remote campus.
- For devices within the connected layer 2 topology, it correlates events to identify the root cause of an outage, whether at layer 2 or layer 3.
- It continually updates correlated layer 2 status information for all managed devices. Status information is available both from the Tivoli NetView topology map and from generated reports.

Fault detection mechanisms

Tivoli Switch Analyzer includes two separate mechanisms for layer 2 fault detection:

- Port status monitoring (see "Port status monitoring")
- Impact-based fault detection (see "Impact-based fault detection" on page 16)

Port status monitoring

Port status monitoring uses regularly-scheduled polling to detect layer 2 outages, even if no layer 3 outage has occurred.

The port status monitor is a process that complements the impact-based fault detection of the correlator. By itself, the correlator depends upon Tivoli NetView layer 3 outage events to trigger the detection of layer 2 problems. However, there are situations in which this approach might not be sufficient:

- Some layer 3 devices might not be managed by the Tivoli NetView product. If a layer 2 outage causes an unmanaged downstream node to become unreachable, no Tivoli NetView event is generated. The layer 2 outage is not detected unless it also affects a managed end node.
- Redundant paths to an end node might be available, meaning that it remains reachable even after a layer 2 outage occurs. Again, no Tivoli NetView event is generated, and the layer 2 outage is not detected unless additional outages affected all of the redundant paths.

Port status monitoring addresses these problems by separately polling the status of switch ports. If the status of a monitored port changes, the port status monitor generates an event. The frequency of polling is configurable. For more information, see "Configuring port status monitoring options" on page 52.

Note: Tivoli Switch Analyzer does not monitor individual ports in a Cisco Systems port channel, just the port channel itself.

Outages detected by port status monitoring trigger the Tivoli Switch Analyzer correlator, which issues root cause events. This means that correlation can be
triggered either by a layer 3 outage event (detected by the Tivoli NetView product) or by a layer 2 outage event (detected by Tivoli Switch Analyzer port status monitoring).

**Port status monitoring and discovery**

Port status monitoring is configured using a separate switch table in the `l2_polling.cfg` file. For more information, see “Configuring which switches to monitor” on page 50. The switch table can include any device that is part of the layer 3 network as discovered by the Tivoli NetView product, including devices that are not included in layer 2 discovery:

- You can monitor a switch within a remote campus. The port status monitor does not require a discovered layer 3 connection path to the monitored device.
- You can monitor a layer 3 switch. This includes multilayer switches defined in the Tivoli NetView `oid_to_type` file with the G flag.

The port status monitor queries the ports that were learned from the port table in the bridge MIB of each managed switch during the discovery phase. These ports are then polled for status changes, and any detected outages are processed by the correlator and reflected in the Layer2Status field of the affected objects. If the outage is within the connected topology, the correlator also performs root cause analysis as usual. Root cause analysis is not performed for outages in a remote campus, or outages affecting multilayer switches.

An outage affecting a switch outside the connected topology results in an Interface Down event for the affected port, and the Tivoli NetView Layer2Status field is updated to Marginal. Node Down events are not generated for nodes outside the connected topology. (If the node is unreachable, Tivoli NetView’s status monitoring handles it at the layer 3 level.)

**Note:** If the Tivoli NetView status of a layer 2 switch within the connected topology changes to Unmanaged, monitoring is discontinued for the ports on that switch. However, monitoring continues for an unmanaged multilayer switch or a switch in a remote campus. To discontinue polling of an unmanaged switch outside the layer 2 topology, you must modify the switch table to exclude the switch, and then restart the `itsl2` daemon.

By default, the port status monitor is configured to poll all of the ports listed in the MIB port tables of all switches discovered by the Tivoli NetView product. Within the connected layer 2 topology, you can optionally restrict polling to include only ports that are connected to devices that are discovered by the Tivoli NetView product.

The default settings also specify that the port status monitor polls all monitored switches during each polling cycle. You can change this behavior to optimize polling in large network environments.

For information about configuring these and other options affecting port status monitor polling, see “Configuring the port status monitor” on page 50.

**Impact-based fault detection**

Impact-based fault detection refers to layer 2 fault detection by the correlator that is triggered by impact on layer 3 devices.
When a managed node becomes unreachable because of a layer 2 outage, the Tivoli NetView product generates an Interface Down trap, identifying the connected interface on the unreachable node.

Tivoli Switch Analyzer is bound to the Tivoli NetView trapd daemon and receives these traps, triggering the correlator. A Tivoli NetView Interface Down event starts the Tivoli Switch Analyzer correlation process as follows:

1. An Interface Down event is detected by the Tivoli NetView product on an interface of a node.
2. Tivoli Switch Analyzer receives the event and begins its own polling.
3. The Tivoli Switch Analyzer polls devices that are upstream from the interface and peer devices. Polling continues until Tivoli Switch Analyzer finds the device that is the farthest upstream (closest to the management station) that is down.
4. Tivoli Switch Analyzer then determines the root cause of the original event. Correlation logic uses logical weighting to determine if there is a node down or a node marginal correlated event.

Root cause analysis

The Tivoli NetView router fault isolation (RFI) function identifies a network outage problem at the IP layer. If the problem is with a router, the Tivoli NetView program issues a Router Status trap and calculates the impact. Subnets and routers in the impacted partition are set to the Unreachable status. However, if the problem is with a layer 2 device, such as a switch, the Tivoli NetView program identifies the nearest impacted router as the root cause. It cannot detect port problems in the layer 2 switch. This problem is solved by the Tivoli Switch Analyzer product.

Tivoli Switch Analyzer discovers the ports of layer 2 devices and integrates this information into the known layer 3 topology, creating a complete layer 2 and layer 3 network topology. In addition, Tivoli Switch Analyzer creates a network segment for each port to represent the connection between the port and the devices connected directly to it. This means that correlation can be to a switch port, rather than a device downstream from that port.

The Tivoli Switch Analyzer correlator is a process that uses this integrated topology to determine the root cause of a network outage, either confirming the Tivoli NetView RFI result (at layer 3) or identifying a layer 2 root cause. Figure 1 on page 18 shows an example of a port failure that is the correlated root cause event.
Figure 1. Layer 2 logic and correlation

Figure 2 shows an example of several port failures correlated as a Node Marginal event.

Figure 2. Node marginal correlated event

Tivoli NetView integration

Tivoli Switch Analyzer is tightly integrated with the Tivoli NetView product, using and extending the Tivoli NetView topology and generating correlated events that are displayed in the Tivoli NetView event browser.

During the discovery process, Tivoli Switch Analyzer imports network information from the Tivoli NetView topology database; it also traps topology changes detected by the Tivoli NetView product. Because Tivoli Switch Analyzer is bound directly to the trapd daemon, topology changes are received as they occur. By continually checking and updating the topology, Tivoli Switch Analyzer keeps its root cause correlation synchronized with the Tivoli NetView topology database. This ensures that root cause correlation is always based on the current network and system infrastructure.

When the Tivoli Switch Analyzer receives interface down events from the trapd daemon, it begins to poll independently of the Tivoli NetView topology polling cycle. Because the Tivoli Switch Analyzer has its own poller, it can quickly process all the necessary interface information for correlation without waiting for the Tivoli NetView product to finish its polling sequence. The Tivoli Switch Analyzer understands the relationship between devices and interfaces, so it polls only the devices or interfaces that are required for the correlation process.
Layer 3 correlation

The Tivoli Switch Analyzer layer 3 correlation function identifies the root cause of a problem affecting IP-addressable devices, ports, or interfaces.

Figure 3 provides an example of a physical circuit outage that occurs on a frame relay circuit causing a permanent virtual circuit (PVC) to go down. Tivoli NetView polling finds an initial interface down condition (the IP address is unreachable). Tivoli Switch Analyzer then interrogates all topologically related interfaces to determine if other IP addresses are unreachable and what the root cause is. The root cause is reported in the event browser, thereby avoiding the confusion of multiple events and the need for manual intervention to determine the root cause.

Redundant path correlation

Tivoli Switch Analyzer can identify the root cause in an environment with redundant paths. Typical wide area networks (WANs) are comprised of a main site, a backup to the main site, and multiple remote sites. Permanent virtual circuits (PVCs) from the remote sites to both the main and main backup sites complete the redundancy needed for high availability.

As shown in Figure 4 on page 20, an outage on the border router produces multiple interface or port down events at remote sites across the entire WAN. Because the remote sites have only a single interface down, but the main border router has several but not all interfaces down, Tivoli Switch Analyzer correlates this to a node marginal event for the border router. This identifies the correct area to begin trouble resolution so time is not wasted diagnosing the problems on the remote devices.
Correlator processing
When an outage is detected, Tivoli Switch Analyzer determines the root cause of the problem and then does the following steps:

- It generates an event identifying the root cause device (whether it is a router, switch, or end node).
- It updates the object database Layer2Status field, if the root cause device is a switch or router.
- It continues to monitor and update the root cause device and associated devices until the problem is resolved, generating new events and updating the Layer2Status field as needed. It also identifies any new downstream problems as they become known.

Tivoli NetView traps
The Tivoli Switch Analyzer program generates ITSL2 Enterprise traps to notify the user of the correlated root cause and subsequent update events. These traps are handled as events by the Tivoli NetView program. If the Tivoli NetView product determines that a trap from Tivoli Switch Analyzer affects the status of a managed device, it generates a Tivoli NetView Enterprise layer 2 Status trap, which is used to update the status of the device on the Tivoli NetView layer 3 topology map. There are three traps: Up, Marginal, and Down.

You can use the Tivoli NetView program trap customization utility to define a notification method such as e-mail or pager.

Traps can be displayed using native event display and the Web console event browser. The traps identify the root cause device in the hostname field, and the type of event and the failing ports are identified in the description field. The Source field for these traps contains the letter V for vendor.

If the Tivoli NetView program has been configured to forward traps to the Tivoli Event Console, all of the Switch Analyzer traps are forwarded as TEC_ITS events by default. Tivoli Switch Analyzer traps are mapped to TEC_ITS_SA_STATUS
events. The status is defined in the sastatus slot. For more information about the Tivoli NetView rules, refer to the IBM Tivoli Enterprise Console documentation.

**Correlation timing**

The timing of correlation relates to the correlated events that populate the event browser. The correlation parameters provide a means of customizing correlation results for a specific environment and operations strategy. Correlation results can vary greatly depending on the values of the correlation parameters. For description and default values of the correlation parameters, refer to "Configuring correlator options" on page 48.

The following example provides an overview of correlation timing:

- An interface down trap is received from Tivoli NetView and the interface timeout period specified by the interface_timeout parameter begins.
- The Tivoli Switch Analyzer waits initially for the amount of time specified by the polling_wait_time parameter. This ensures that things like loss of the local management interface (LMI) are given sufficient time to occur (status within the Frame Relay can propagate) before the Tivoli Switch Analyzer begins polling.
- The Tivoli Switch Analyzer begins polling prior to determining the root cause problem during the rest of the time specified by the interface_timeout parameter.
- Correlation occurs within the time specified by the corr_timeout parameter. During the corr_timeout interval, the root cause devices are polled again to verify that they are still down.
- The root cause problem is determined and the Tivoli Switch Analyzer issues the correlated root cause trap.

If an interface goes down and comes back up (bounces) within the interface_timeout period, correlation is stopped and no correlated root cause trap is issued. The interface that bounced is monitored and compared to the bouncing threshold that is defined by the interface_bounce_count parameter and the interface_bounce_interval parameter. By default, if the interface goes down three times within one hour, a problem exists and a correlated root cause trap is issued. When the interface stays up for the same interface_bounce_interval, an up trap is issued.

**Tivoli NetView topology maps**

In addition to sending trap notification for layer 2 problems, Tivoli Switch Analyzer updates the Tivoli NetView layer 3 topology map symbol status for layer 2 devices. Layer 2 connector devices are displayed on the Network and Segment submaps. Without the Tivoli Switch Analyzer program installed, the status of a Tivoli NetView device is determined from the status of its interfaces. This means the status of a layer 2 device symbol depends on the availability status of a single layer 3 management IP interface.

**Note:** On a Windows system, the status of services also contributes to the status of the layer 2 device symbol.

With Tivoli Switch Analyzer installed, the status symbol for a layer 2 device is based either on its IP status or its layer 2 status, whichever is more severe. For example, if the status of the management interface is Up, but the layer 2 status indicates that one or more ports failed, then the status of the layer 2 device symbol is shown as Marginal. (Tivoli Switch Analyzer only changes the handling of status symbols for layer 2 switches.)
**Viewing correlated layer 2 status**

Tivoli Switch Analyzer indicates the current layer 2 status of an object by updating the Layer2Status field in the Tivoli NetView object database. The value of this field is initially Unset. When a problem occurs, Tivoli Switch Analyzer updates the Layer2Status field to either Marginal or Critical; as problems are resolved, it updates the field to either Marginal or Up. You can view the Layer2Status field using the Tivoli NetView Web console or at a command line.

In addition, Tivoli Switch Analyzer adds a symbol representing the compound status of the ports of each layer 2 switch object. This layer 2 status symbol appears with the interfaces on the IP topology node submap and is color-coded to indicate the current status:

<table>
<thead>
<tr>
<th>Color</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Unset</td>
</tr>
<tr>
<td>Green</td>
<td>All ports up</td>
</tr>
<tr>
<td>Yellow</td>
<td>One or more ports down</td>
</tr>
</tbody>
</table>

**Viewing layer 2 status using the Object Properties window**

To view the status of a layer 2 device using the Object Properties window, follow these steps:

1. In the Tivoli NetView Web console, select a layer 2 device from the Network or Segment submap.
2. Select **Object Properties** from the pop-up menu or the Object menu.
3. In the Object Properties window, select **Other**.

The displayed fields show the IP status, layer 2 status, and interface status for the selected device. (On Windows systems, the status of service objects is also displayed.)

**Viewing layer 2 status using the System Configuration view**

You can view the layer 2 status of one or more devices using the System Configuration view.

To open the System Configuration view, click **System Configuration View** in the Submap Explorer window. The displayed information includes the IP status and layer 2 status.

**Note:** Status updates are not automatically displayed in this window. To see updated status, select **Refresh Data** from the **Submap** menu.

**Viewing layer 2 status from a command line**

To view the status of a layer 2 device from a command line, use one of the following commands:

- `/usr/OV/bin/ovobjprint -s selectionname`
- `/usr/OV/bin/ovtopodump -l selectionname`

`selectionname` is either the fully qualified host name or the numeric IP address of the device.
The displayed fields show the IP status, layer 2 status, and interface status for the selected device. (On Windows systems, the status of service objects is also displayed.)
Chapter 5. Viewing layer 2 topology

Layer 2 views display the layer 2 topology with status, providing enhanced visual troubleshooting capability.

Tivoli Switch Analyzer contains the following layer 2 views:
- Physical view
- VLAN view
- Point to Point view

These views are available only using the NetView Web console.

Physical view

The Physical view is a layer 2 view that displays your selected object and all objects connected to it. The Physical view is dynamic. If the status of an object changes or a new node is discovered, the view updates automatically.

[Figure 5 on page 26](#) is a screen shot of a Physical view.
Opening the Physical view

To open the Physical view, do the following steps:

1. Using the Tivoli NetView Web console, select a switch, router, or node in the Submap Explorer or a layer 2 view.
2. From the Monitor menu, click Layer 2 → Physical View or select the object and right-click Physical View.

Understanding the Physical view window

At the top of the view is the title bar. The title bar displays Physical View, a number reflecting the number of times you have opened a layer 2 view in this
session, the name of the object that was selected when the view was opened, and with hop count 1. Click the arrow icons on the right to expand or compress the window. Click the close icon (X) to close the window.

Below the title bar is the Tivoli NetView help bar. Click the question mark icon ( ) to access Tivoli NetView help.

Below the Tivoli NetView help bar is the tool bar. See “Tivoli Switch Analyzer tool bar” on page 33 for information on the function of each icon. Click the Help button to display help on the layer 2 views.

Note: In all layer 2 views, port labels display the ifIndex value from the Interfaces MIB-II table in front of the label name.

Hop count
A hop is a connection within a string of connections that links two network devices. By default, the Physical view shows one hop count which means it shows your selected object and what is directly connected to it. Two hop counts shows your selected object, those objects connected to it, and also what is connected to those objects.

You can view from 0 to 4 hop counts. The number of hop counts is displayed to the right of the tool bar in the Physical view.

Adjusting the hop count number
To adjust the hop count, do the following steps in the Physical view:
1. Click the drop-down list to the right of Other Hop Counts.
2. Select the number of hop counts you want.
3. Click Switch to (hop count number).

After changing the hop count number, the new view is centered on the selected object, if one was selected. If no object was selected, the view is centered on the same object as in the previous view.

VLAN view
The VLAN view displays all switches, routers, and nodes in a VLAN. The VLAN view is a static view which means if the status of an object changes or a new node is discovered, the view does not update automatically. You must open the view again to see updated information.

Figure 6 on page 28 is a screen shot of a VLAN view.
Opening the VLAN view

To open the VLAN view, do the following steps:

1. Using the Tivoli NetView Web console, select a switch, router, or node in the Submap Explorer or a layer 2 view.
2. From the menu bar, click Monitor → Layer 2 → VLAN View or select the object and right-click VLAN View.
3. If there is more than one VLAN on that device, a dialog box displays, asking which VLAN you want to view. Select a VLAN and click OK.
Understanding the VLAN view window

At the top of the view is the title bar. The title bar displays VLAN View, then a number reflecting the number of times you have opened a layer 2 view in this session, and the name of the VLAN being viewed. Click the arrow icons on the right to expand or compress the window. Click the close icon (X) to close the window.

Below the title bar is the Tivoli NetView help bar. Click the question mark icon ( ) to access Tivoli NetView help.

Below the Tivoli NetView help bar is the tool bar. See “Tivoli Switch Analyzer tool bar” on page 33 for information on the function of each icon. Click the Help button to display help on the layer 2 views.

When you open the VLAN view, all objects are compressed.

Select an object in the view. If there are no other VLANs on the selected device, the following text displays to the right of the tool bar:

No other VLANs on hostname

If there are other VLANs connected to the selected object, a drop-down list displays next to the tool bar displaying the VLAN IDs of the remaining VLANs. You can select a new VLAN to view. See “Selecting a new VLAN to view” for details.

Tivoli Switch Analyzer includes only VLAN members that it is sure of in a view. When there is limited information, Tivoli Switch Analyzer discovery sometimes makes assumptions. These assumed connections are marked with an asterisk (*) in the Discovery Report and the connected devices are not displayed in the VLAN views.

Note: In all layer 2 views, port labels display the ifIndex value from the Interfaces MIB-II table in front of the label name.

Selecting a new VLAN to view

To select a new VLAN to view, do the following steps:

1. Select an object in the view.
2. At the top of the view in the drop-down list, choose the VLAN ID of the VLAN you want to display.
3. Click Switch to VLAN id.

Point to Point view

The Tivoli Switch Analyzer Point to Point view displays layer 2 and layer 3 devices between two selected points. The Point to Point view is a static view which means if the status of an object changes or a new node is discovered, the view does not update automatically. You must open the view again to see updated information.

Figure 7 on page 30 is a screen shot of a Point to Point view.
Opening the Point to Point view

You can open the Point to Point view by doing the following steps:

1. Using the Tivoli NetView Web console, select a switch, router, or node in the Submap Explorer or a layer 2 view.
2. From the Monitor menu, click Layer 2 → Point to Point View or select the object and right-click Point to Point View.
3. A window is displayed prompting you to type the node name or IP address for the second node. Type a node name or IP address in the text box. (The node name must match the name in the Tivoli NetView topology database.) Click OK.

You can also select two objects and open the Point to Point view by clicking Layer 2 → Point to Point View.

Understanding the Point to Point view window

At the top of the view is the title bar. The title bar displays Point to Point View, a number, which reflects the number of times you have opened a layer 2 view in a session, and From first node to second node. Click the arrow icons on the right to expand or compress the window. Click the close icon (X) to close the window.
Below the title bar is the Tivoli NetView help bar. Click the question mark icon to access Tivoli NetView help.

Below the Tivoli NetView help bar is the tool bar. See “Tivoli Switch Analyzer tool bar” on page 33 for information on the function of each icon. Click the Help button to display help on the layer 2 views.

When you open the Point to Point view, all objects are compressed.

The layer 2 segment of the path consists of the physical connections. Because the actual data path can easily change from when the last discovery poll took place, the layer 2 path is shown with other devices in the layer 2 segment to provide additional context. This helps when identifying related outages and problems that may be affecting traffic.

The Point to Point view displays a directional path calculated from the routing tables of the layer 3 devices with the layer 2 path inserted within each subnet, where possible. For a Point to Point path to be completed from source to destination, the layer 3 path must be discovered by Tivoli NetView. Tivoli NetView must also have SNMP access to each router along the path. The layer 2 path is inserted between the layer 3 devices if Tivoli Switch Analyzer has discovered a physical path between the layer 3 objects. This inserted layer 2 path looks like the Physical view. If a router along the path cannot be accessed, the path stops and the letter X is displayed. This indicates reachability or routing problems.

Some layer 2 switches, when specified as the starting point for a Point to Point view, do not provide the routing information required to create a Point to Point path view. You can avoid problems by choosing an SNMP-enabled router or end node as the first node for a Point to Point view. If the object you choose as the first node is a layer 2 switch or is not an SNMP-enabled device, a reverse lookup is done using the second node as the starting point. In this case, the word Reverse is displayed in the status bar at the bottom of the window to indicate that this is a reverse lookup. If both nodes specified for a Point to Point view are either layer 2 switches or not SNMP-enabled devices, an error message is displayed.

Note: In all layer 2 views, port labels display the ifIndex value from the Interfaces MIB-II table in front of the label name.

**Understanding status in the layer 2 views**

In the layer 2 views, status is calculated by Tivoli Switch Analyzer. Status may differ from the Tivoli NetView maps in timing or substance. Status in the layer 2 views is based on the correlated status maintained by Tivoli Switch Analyzer. The key difference is that the status is based on information that Tivoli Switch Analyzer has within its correlation process which may differ from the status maintained by Tivoli NetView. The status displayed in the layer 2 views is the same as the status shown in the layer 2 status reports.

For nodes, the Tivoli Switch Analyzer status is the following:
- **Up** – If there are no correlated events for node
- **Marginal** – If at least one interface is correlated down, but the node itself is up
- **Down** – If the node is correlated down

For interfaces, the Tivoli Switch Analyzer status is the following:
• **Up** – If there are no correlated events for interface
• **Down** – If the interface is correlated down, or a down event has been received for this interface and correlation is in process
• **Unmanaged** – If the interface is unmanaged within Tivoli Switch Analyzer. The interface is not necessarily unmanaged in Tivoli NetView.

Each Tivoli Switch Analyzer status change generates a Tivoli Switch Analyzer event with the source code V for Vendor.

---

### Taking action on an object

Context menus are pop-up menus that are provided for performing operations on individual objects. The context menus provide a subset of operations that are available from the menu bar.

From all layer 2 views, you can right-click an object to display a context menu that shows the actions you can take on an object. Depending on the type of object selected, the context menu displays a subset of the following selections:

- **Object Properties**
  - Displays the Tivoli NetView Object Properties window. See “Viewing layer 2 status using the Object Properties window” on page 22 for information about viewing layer 2 status using the Object Properties window.

- **Ping**
  - Pings the selected node

- **Physical View**
  - Displays the Tivoli Switch Analyzer Physical view. See “Physical view” on page 25 for information about the Physical view.

- **Point to Point View**
  - Displays the Tivoli Switch Analyzer Point to Point view. See “Point to Point view” on page 29 for information about the Point to Point view.

- **VLAN View**
  - Displays the Tivoli Switch Analyzer VLAN view. See “VLAN view” on page 27 for information about the VLAN view.

- **Layer 2 Status Report**
  - Runs the text-based layer 2 status report. See “Generating the layer 2 status report” on page 41 for information about the layer 2 status report.

- **Impact Analysis**
  - Generates a list of all of the nodes that would be affected if a selected device fails. See “Generating an impact analysis report” on page 41 for information about the Impact Analysis report.

- **Rediscovery**
  - Discovers changes in the layer 2 topology of the selected node since the last time the network was discovered and updates the view.

**Note:** By default, operators do not have the authority to perform rediscovery.

- **Impact Analysis (connectors)**
  - Generates a list of all connector devices that are affected if a selected device fails. See “Generating an impact analysis report” on page 41 for information about the Impact Analysis report.
Discovery
Generates a list of the discovered switches, sorted by TCP/IP host name. The report also lists the ports discovered on each switch and what device is connected to each port. See “Generating the discovery report” on page 40 for information about the Discovery report.

Getting help
From the layer 2 views, you can access both Tivoli Switch Analyzer help and Tivoli NetView help.

To get help on layer 2 views, see “Getting Tivoli Switch Analyzer help.”

To access Tivoli NetView help, see “Getting Tivoli NetView help.”

Getting Tivoli Switch Analyzer help
Tivoli Switch Analyzer provides help on the three layer 2 views.

To access Tivoli Switch Analyzer help, do the following steps:
1. Open one of the layer 2 views.
2. Click the Help button.

Tivoli Switch Analyzer help opens.

Getting Tivoli NetView help
You can access Tivoli NetView help while you are in layer 2 views.

To access Tivoli Switch Analyzer help from a layer 2 view, click the question mark icon. Tivoli NetView help opens.

Tivoli Switch Analyzer tool bar
All layer 2 views display the same tool bar. Use the icons in the tool bar to work with the layer 2 views.

Pause the mouse over the icons to display the name of the function that the icon provides.

Table 1 lists the icons in the tool bar:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pan</td>
<td></td>
</tr>
<tr>
<td>Select</td>
<td></td>
</tr>
<tr>
<td>Zoom into rectangle</td>
<td></td>
</tr>
<tr>
<td>Zoom in</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Tool bar icons and descriptions
**Table 1. Tool bar icons and descriptions (continued)**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Zoom out" /></td>
<td>Zoom out</td>
</tr>
<tr>
<td><img src="image" alt="Fit in window" /></td>
<td>Fit in window</td>
</tr>
<tr>
<td><img src="image" alt="View at natural size" /></td>
<td>View at natural size</td>
</tr>
</tbody>
</table>

**Understanding deleted views**

Occasionally you might see a *This view has been deleted* message in the status bar at the bottom of the view. This occurs when the centered object in a view is deleted.

If the object is unmanaged (or within a campus), the view can still get updated, although some updates, such as updates to the object status, might not be available.

To remove the message, open the view using a different object.

**Scenarios using the layer 2 views**

Scenario 1:
1. You receive a call from a client who says that he cannot reach his Lotus Notes® server.
2. The first thing you do is use Tivoli NetView to locate the Lotus® Server. You see that the server is still green, so you Quicktest (demandpoll) it to test its availability from your machine. It responds successfully.
3. You decides to use the Point to Point Service view as a starting point to examine the path from the caller to the server.
4. Using the Web console, you select the Lotus Notes server in the Tivoli NetView Submap Explorer and click on Point to Point view. You find the router in the caller’s IP subnet, since his desktop is not in the Tivoli NetView database.
5. You look to see if there are any outages you are not aware of on the path, and see none.
6. You select all the machines and initiate Quicktest (demandpoll) on them all. You know some of the machines are polled every 10 minutes and might not have been polled yet.
7. You ping the caller’s IP address and it times out. Using the Point to Point view, you select the router in the caller’s subnet and click on the physical view. You change the number of hops from 1 to 3.
8. A cascaded access switch off the router is showing marginal.
9. You ask for the caller’s MAC address and select the switch on the diagnostic switch view. You find his MAC address in the forwarding table before it has aged out, showing that his machine is downstream of one of the failed ports.
10. You right-click the switch and click **Object Properties** to find the contact information of the network administrator. You let the administrator know what you discovered.
Scenario 2:

1. You receive an event from Tivoli Switch Analyzer.
2. Looking at the other status events received in the last few minutes, you conclude that the problem is probably with the switch.
3. You select the affected switch and launch a layer 3 topology view from the Tivoli NetView Submap Explorer, and navigate to the Physical view. By default, it shows 1 hop. This shows you the impact of the failure of the ports listed in the Tivoli Switch Analyzer event.
4. The view shows one of the ports connected to another switch. You navigate to the connected view of that switch. It shows several servers that are impacted.
5. To help assess priority, you look at Object Properties from each server to see which services are running on the servers and note this in the trouble ticket.
Chapter 6. Generating reports

You can use Tivoli Switch Analyzer to generate reports containing information about the layer 2 topology and device status. Several reports are available:

**Summary report**

The summary report contains the results of the discovery process. Use this report to identify and resolve problems affecting layer 2 discovery.

**Discovery report**

The discovery report lists the discovered layer 2 devices and connections. Use this report to verify the connected topology.

**Impact analysis**

The impact analysis report shows which nodes would be affected if a specified device fails. You can generate an impact analysis report for all devices affected by the switch, or an impact analysis report that is limited to connector devices.

**Layer 2 status report**

The layer 2 status report lists all discovered layer 2 and multilayer switches currently managed by the port status monitor (as defined by the switch table in the port status monitor configuration), along with the current status of each port.

**Note:** Reports are generated based on the contents of the topology cache file, which is updated by default every 15 minutes. For information on changing the cache frequency, see [“Changing the cache frequency” on page 47](#).

---

Generating the summary report

The summary report lists the devices Tivoli Switch Analyzer has attempted to discover, along with the results of the discovery attempt. This report provides a quick way to see which devices were successfully discovered, which devices are still being discovered, and which devices have problems that prevent complete discovery.

To generate the summary report, use the **ITSL2_reports** script. On a Windows system, run this command:

```
\usr\ov\ITSL2\bin\ITSL2_reports.bat -r summary [-d]
```

On a Linux or UNIX system, run this command:

```
/usr/0W/ITSL2/bin/ITSL2_reports -r summary [-d]
```

The optional -d parameter forces an immediate update of the topology cache file before generating the report. Use this option if you want the report to reflect information discovered since the last cache update. (For more information, see [“The layer 2 discovery process” on page 11](#).

**Summary report contents**

The summary report includes all of the layer 2 devices for which discovery was attempted, sorted according to the return code resulting from the discovery attempt.
Any undiscovered or incompletely discovered switches might lead to inaccurate topology information for subnets attached to those switches. By using the summary report, you can identify and resolve discovery problems, which helps to ensure accurate information.

Devices in the summary report are sorted into the following categories:

**Discovery is in progress for the following nodes:**

The itsl2 daemon is still attempting to complete discovery for these devices. To make sure all discovery problems are identified, you should wait until this category is empty before you continue with the rest of the report.

If devices are listed in this category, follow these steps:
1. Wait at least 15 minutes to allow the itsl2 daemon to complete discovery.
2. Regenerate the summary report.

**Discovery has been completed for the following nodes, but one or more errors occurred (# = retry count has been exceeded):**

The itsl2 daemon has finished attempting to discover these devices, but was unsuccessful because of errors.

These errors are generally caused by SNMP problems such as missing MIB information or access problems. When the daemon encounters an SNMP error during discovery, it repeats the query until the retry count is exceeded. (The default retry count is 5; this value is defined by the retry_cnt parameter in the /usr/OV/ITSL2/conf/l2_topo_adapter.ini file.)

If devices are listed in this category, follow these steps:
1. Check the /usr/OV/ITSL2/log/l2_topo_adapter.log file to find any SNMP error messages related to these devices.
2. Resolve the problems that are causing the errors.
3. Rediscover the layer 2 topology by restarting the itsl2 daemon.
4. Regenerate the summary report.

**Discovery has been completed for the following nodes, but node was unreachable via layer 2 segments:**

The itsl2 daemon has finished attempting to discover these devices, but could not trace the layer 2 connection paths.

If a device appears in this category, this means that the itsl2 daemon did not find a layer 2 path from a router to the listed device. This can happen when information is missing from the bridge MIB forwarding tables on the listed device, or on a nearby switch, or a connected switch is not accessible for SNMP.

If devices are listed in this category, follow these steps:
1. On each device that is part of the undiscovered portion of the topology, try increasing the forwarding table cache age to 15 minutes or longer. This allows the itsl2 daemon more time to read the required information before it is deleted.
2. Check the discovery report to make sure it does not indicate incorrect connections between Cisco devices that are not actually connected to one another. This can be caused by use of the Cisco Discovery Protocol (CDP) within a heterogeneous network.
If this is happening, disable the CDP function on the ports of Cisco switches or routers that are connected to devices from other vendors. This is particularly important if multiple Cisco devices are connected to the ports of a switch from another vendor.

3. Rediscover the layer 2 topology by restarting the itsl2 daemon.
4. Regenerate the summary report.

**Discovery has been turned off for the following nodes:**

The itsl2 daemon did not discover these devices because a required MIB was not available.

For each device listed in this category, follow these steps:

1. Confirm that the device supports the required MIBs:
   - The bridge MIB defined by RFC 1493
   - The interface MIB defined by RFC 2020
2. Make sure the Tivoli NetView server has SNMP access to the device using the community string specified in the Tivoli NetView configuration.
   Access problems can result if the SNMP agent on the switch is configured with an access list that allows access only from certain nodes, or using certain community strings.
3. If the SNMP agent on the switch is causing access problems that you cannot resolve, you can prevent future discovery of the switch. See "Selectively disabling discovery" on page 12 for more information.
4. Rediscover the layer 2 topology by restarting the itsl2 daemon.
5. Regenerate the summary report.

**Discovery has been completed for the following nodes:**

The itsl2 daemon successfully discovered these devices without errors. As many switches as possible should be listed in this category to maximize the accuracy of the layer 2 topology.

**Note:** Even when a switch is listed in this category, topology inaccuracies can still occur if critical entries are missing from the bridge MIB forwarding table.

**Discovery will not be done for the following nodes because they are located within a remote campus:**

Switches in this section have not been discovered for topology connections nor have they been configured for port status monitoring.

If devices are listed in this category, follow these steps:

1. Make sure all routers connecting these devices to the network are managed by the Tivoli NetView product, and that the Tivoli NetView product has SNMP access to these routers or use the Tivoli NetView seed file to create custom links between routers across unmanaged WANs. Refer to Tivoli NetView documentation for more information.
2. Rediscover the layer 2 topology by restarting the itsl2 daemon.
3. Regenerate the summary report.

**Note:** If you are unable to resolve these problems, contact your customer support representative about the IBM Tivoli Remote Campus Installation Service for the Tivoli Switch Analyzer product. This
service enables a connection path that Tivoli Switch Analyzer can use for correlation between remote islands to enable layer 2 root cause management.

The following (layer 2) nodes are located within a remote campus and are being monitored for status only:

Switches in remote campus regions can be included in the port status monitoring configuration. If they are, discovery will be limited to learning the active ports. Depending on the outcome of the discovery, these switches will appear in other sections of the summary report also, but connections to these switches will not be discovered.

The following (layer 3) nodes are being monitored for status only:

Layer 3 switches can be included in the port status monitoring configuration. If they are, discovery is limited to learning the active ports. Depending on the outcome of the discovery, these switches appear in other sections of the summary report as well, but connections to these switches are not discovered.

Generating the discovery report

To create a report listing the layer 2 devices discovered by Tivoli Switch Analyzer, use the ITSL2_reports utility. This utility builds a report based on the cached data resulting from the most recent layer 2 discovery of the network. You can use this information, along with the information contained in the summary report, to diagnose and correct topology problems.

You can generate a discovery report either from a command line or from the Tivoli NetView console.

- To create the report from a command line, run this command:
  ```bash
  /usr/04/ITSL2/bin/ITSL2_reports -r layer2 [-s] [-o] [-d]
  ```

  This command has three optional parameters:
  - The `-s` parameter specifies the Tivoli NetView selection name of a switch. If you specify a selection name, the discovery report includes only information for the specified switch.
  - The `-o` parameter specifies the Tivoli NetView object identifier of a switch. If you specify an object identifier, the discovery report includes only information for the specified switch.
  - The `-d` parameter forces an immediate update of the topology cache file before generating the report. Use this option if you want the report to include information discovered since the last cache update. (For more information, see “The layer 2 discovery process” on page 11.)

- To create the report for a single switch from the Tivoli NetView console or Web console, follow these steps:
  1. From the topology map, select a layer 2 device.
  2. Click Monitor → Layer 2 → Discovery from the pop-up menu.

The discovery report lists the discovered switches, sorted by TCP/IP host name. The report also lists the ports discovered on each switch and what device is connected to each port. By verifying the connections listed in the discovery report, you can ensure the accuracy of the layer 2 topology information.
In some cases, incomplete topology information can prevent the itsl2 daemon from discovering the path between a node and the upstream router it is connected to. When this happens, Tivoli Switch Analyzer creates an arbitrary connection between the node and the switch connected to the upstream router. Connections of this type are marked in the report with an asterisk (*). This enables the Tivoli Switch Analyzer product to perform an estimated root cause analysis for the areas where topology information is missing. These connections indicate incomplete topology information and can result in incorrect root cause analysis.

**Note:** The discovery report can include switches that are not part of the connected layer 2 topology (including multi-layer switches and switches within a remote campus). These switches are discovered by the port status monitor based on the configuration of the switch table in the l2_polling.cfg configuration file (see “Configuring which switches to monitor” on page 50). Because topology information is not available for these switches, the discovery report does not list any connections for them.

## Generating an impact analysis report

To see the potential impact of a layer 2 outage, you can generate an impact analysis report. This report lists all of the nodes that are affected if a selected device fails. It displays all nodes downstream of the device from the Tivoli NetView server. You can generate two different impact analysis reports: a report showing all affected nodes, or a report showing only connector devices.

To create an impact analysis report, follow these steps:

1. From the topology map, select a layer 2 device.
2. Click **Monitor** + **Layer 2** + **Impact Analysis** or **Monitor** + **Layer 2** + **Impact Analysis (connectors)**.

## Generating the layer 2 status report

The layer 2 status report lists all layer 2 and multi-layer switches currently managed by the port status monitor. (For information on configuring which switches are managed, see “Configuring which switches to monitor” on page 50.) The report also lists current status information for each switch as detected by the port status monitor and the correlator.

You can generate the layer 2 status report either from a command line, Tivoli NetView native console, or Tivoli NetView Web console.

- To create the report from a command line, run this command:

  ```
  /usr/OV/ITSL2/bin/ITSL2_reports -r status [-s] [-o] [-d]
  ```

  This command has three optional parameters:
  - The `-s` parameter specifies the Tivoli NetView selection name of a switch. If you specify a selection name, the status report includes only information for the specified switch.
  - The `-o` parameter specifies the Tivoli NetView object identifier of a switch. If you specify an object identifier, the status report includes only information for the specified switch.
  - The `-d` parameter forces an immediate update of the topology cache file before generating the report. Use this option if you want the report to include
information discovered since the last cache update. (For more information, see “The layer 2 discovery process” on page 11.)

• To create the report from the Tivoli NetView console, follow these steps:
  1. From the topology map, select a layer 2 device.
  2. Click Monitor \rightarrow Layer 2 \rightarrow Status from the pop-up menu.

• To create the report from the Tivoli NetView Web console, follow these steps:
  1. From the topology map, select a layer 2 device.
  2. Click Monitor \rightarrow Layer 2 \rightarrow Layer 2 Status Report from the pop-up menu.

Layer 2 status report contents

The resulting report provides summary information for the managed switches, followed by detailed information about each managed switch and port. The following is an example of an entry for a switch with two managed ports:

```
cs2950a.tivlab.ibm.com/9.27.139.133/Reachable/Correlated Up
[1/FastEthernet0/1/Interface Up/Correlated Up]
[12/FastEthernet0/12/Interface Down/Correlated Unmanaged]
```

The first line provides the overall status of the switch:

```
hostname/ip_address/psm_status/corr_status
```

The fields are as follows:

hostname
The TCP/IP host name of the switch.

ip_address
The numeric IP address of the switch.

psm_status
The overall status of the switch as determined by the port status monitor. This status is based on the result of the most recent polling attempt. This field has one of the following values:

• Reachable
• Unreachable
• Unset

corr_status
The overall status of the switch as determined by the correlator. This status is based on the most recent status changes detected as the result of impact-based fault detection. This field has one of the following values:

• Correlated Up (the switch is available)
• Correlated Marginal (root cause) (one or more ports are down, and the correlator has identified this outage as a root cause)
• Correlated Down (root cause) (the switch is down, and the correlator has identified this outage as a root cause)
• Correlated Down (the switch is down, but the correlator has not identified this outage as a root cause)

Following the line providing the overall switch status, the report indicates one or more lines indicating the individual status of the managed ports on the switch:

```
if_index/if_type/port_number/psm_status/corr_status
```

The fields are as follows:
**psm_status**

The status of the port as determined by the port status monitor. This status is based on the result of the most recent polling attempt. This field has one of the following values:

- Interface Up
- Interface Down
- Interface AdminDown
- Unset

An event is sent when the status changes to Interface Up, Interface Down and Interface AdminDown. No event is sent for the initial status of Interface Up or Unset.

**corr_status**

The status of the port as determined by the correlator. This status is based on the most recent status changes detected as the result of impact-based fault detection. This field has one of the following values:

- Correlated Up (the port is available)
- Correlated Down (correlating...) (the port is down, but correlation is still in progress)
- Correlated Down (root cause) (the port is down, and the outage has been identified as a root cause)
- Correlated Down (impact) (the port is down as a result of another outage)
- Correlated Unmanaged (the port is unmanaged)

The layer 2 status report includes multi-layer switches or switches within a remote campus, if these switches are being managed by the port status monitor. Status information for these switches includes port status monitor status and correlator status, but the correlator status assumes that any fault on such a switch is a root cause. If a switch within a remote campus is unreachable, it is not managed by Tivoli Switch Analyzer but Tivoli NetView continues to monitor the switch for availability through its management interface.
Chapter 7. Administration

This section describes Tivoli Switch Analyzer administrative tasks.

Starting and stopping Tivoli Switch Analyzer

Tivoli Switch Analyzer starts automatically when the Tivoli NetView product runs. However, you can also start and stop it manually. Because the Tivoli Switch Analyzer itsl2 daemon is implemented as a well-behaved Tivoli NetView daemon, you must use the Tivoli NetView product to start and stop it.

Starting the daemon

You can start the daemon either using the Tivoli NetView console (on Windows systems only) or from a command line.

Starting the daemon using the Windows console

To start the itsl2 daemon using the Tivoli NetView console on a Windows system, follow these steps:
1. Click Options → Server Setup. The Server Setup window opens.
2. On the Daemons page, select itsl2 from the list.
3. Click Start.

Note: The itsl2 daemon is not initially registered with the console if the installation process did not start the daemons automatically (see "Running the installation utility" on page 6). If the daemon is not registered, you must either start all daemons from the console or use the command line to start the itsl2 daemon.

Starting the daemon from a command line

To start the itsl2 daemon from a command line, use the ovstart command. On a Linux or UNIX system, run this command:

```
/usr/0W/bin/ovstart itsl2
```

On a Windows system, run this command:

```
\usr\ov\bin\ovstart itsl2
```

Stopping the daemon

You can stop the itsl2 daemon either using the Tivoli NetView console (on Windows systems only) or from a command line.

Stopping the daemon using the Windows console

To stop the itsl2 daemon using the Tivoli NetView console on a Windows system, follow these steps:
1. Click Options → Server Setup. The Server Setup window opens.
2. On the Daemons page, select itsl2 from the list.
3. Click Stop.
Stopping the daemon from a command line
To stop the itsl2 daemon from a command line, use the ovstop command. On a Linux or UNIX system, run this command:
/usr/OV/bin/ovstop itsl2

On a Windows system, run this command:
\usr\ov\bin\ovstop itsl2

Tivoli Switch Analyzer processes
The itsl2 daemon is made up of the following processes:

- **coordinator**
  - Starts and stops all Tivoli Switch Analyzer processes
  - Routes messages between the processes

- **correlator**
  - Receives raw messages
  - Correlates raw messages to identify root causes
  - Processes polling requests
  - Processes topology requests for layer 2 discovery

- **poll_server**
  - Handles correlator polling

- **event_controller**
  - Manages the event database

- **event_receiver**
  - Starts and stops Tivoli NetView event adapters
  - Receives events from Tivoli NetView event adapters

- **ext_cmd_server**
  - Provides the interface to send events to the Tivoli NetView product

- **l2_event_adapter**
  - Handles port status monitor processing

- **l2_event_receiver**
  - Handles queries and scheduling of polling for the port status monitor

- **ov_cmd_server**
  - Provides the interface to the Tivoli NetView topology database

- **ov_event_adapter**
  - Receives raw events from the Tivoli NetView trapd daemon
  - Filters events and forwards them to the Tivoli NetView event receiver

- **l2_topo_adapter**
  - Queries devices for layer 2 discovery

- **route_server**
  - Determines layer 3 routes for the Point to Point view

- **topo_server**
  - Processes topology user interface requests
Changing the cache frequency

Layer 2 topology reports are generated from cached discovery data. (If you generate a report using the command line interface, you can force an immediate cache update by using the -d option.)

By default, Tivoli Switch Analyzer updates the cached data every 15 minutes. You can modify the configuration to change this interval:
2. Find the [Correlation] section in the file.
3. Modify the topo_cache_freq line:
   topo_cache_freq=seconds

   Specify the number of seconds you want to elapse between cache updates. The default is 900 seconds (15 minutes).

Note: Setting this value too low can affect correlator performance by causing excessive caching. In general, the cache frequency interval should not be less than 2 minutes (120 seconds).

The following line sets the cache frequency to 10 minutes:
topo_cache_freq=600

Cache files

Tivoli Switch Analyzer provides the following cache files:
- corr_cache
  Contains information about open correlated events based on the type of event record as follows:
  - Correlated object records:
    C|node oid|object type|object status|corr event num|ticket num|name

  where:

<table>
<thead>
<tr>
<th>Value</th>
<th>Object type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Interface</td>
</tr>
<tr>
<td>2</td>
<td>Node</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>Object status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Down</td>
</tr>
<tr>
<td>2</td>
<td>Marginal</td>
</tr>
</tbody>
</table>

- topo_cache
  Contains a current dump of the topology database. By default, the database is dumped at 15 minute intervals.
- event_cache
  Contains the event database. This file contains null characters, so it cannot be viewed using a text editor.
Configuring correlator options

You can configure several options that affect the behavior of the correlator.

- To specify a host name for the management system, modify the `mgt_host` option in the `/usr/OV/ITSL2/conf/correlator.ini` file.

In most cases, this option can be left blank; the default behavior is to use the local host. However, if the management system has multiple interfaces, the itsl2 daemon uses the first IP address for the server that is returned from the DNS server. If this does not match the SNMP address for the server found in the server database, the itsl2 daemon does not start.

To avoid this problem, use the `mgt_host` option to specify the SNMP address associated with the server in the Tivoli NetView database. To discover the SNMP address of the server, run the `ovtopodump -r <hostname>` command.

- To configure how frequently the correlator should retry a failed layer 2 request, modify the `retry_interval` option in the Layer 2 section of the `/usr/OV/ITSL2/conf/l2_topo_adapter.ini` file. The value of this option should be an integer specifying an interval (in seconds) that should elapse between retries. The default value is 900 seconds (15 minutes).

- To configure the maximum number of times the correlator should retry a failed layer 2 request, modify the `retry_cnt` option in the Layer 2 section of the `/usr/OV/ITSL2/conf/l2_topo_adapter.ini` file. The value of this option should be an integer. The retry count maximum applies only to retries of the same request; after a layer 2 request completes successfully, the count is reset to 0. Even if the retry count maximum is reached, rediscovery requests can still be submitted from the Tivoli NetView console. The default value for this option is 3.

- To configure the correlation timeout delay for Interface Down events, modify the `interface_timeout` option in the `/usr/OV/ITSL2/conf/correlator.ini` file.

This option specifies the amount of time, in seconds, the correlator should wait after each Interface Down event before beginning the correlation process. (An Interface Down event can be received either from the Tivoli NetView product or from the Tivoli Switch Analyzer polling process.) During the timeout interval, Tivoli Switch Analyzer initiates the polling process to detect impacts of the received Interface Down event. The timeout interval should be long enough for the polling process to detect impact events before attempting to correlate the root cause.

The default value for this option is 300 seconds. Use this value for any network with fewer than 30000 managed objects. For larger networks, the timeout delay might need to be longer; as a general guideline, add two seconds to the timeout delay for each additional 1000 managed objects.

- To configure the interface bounce count, modify the `interface_bounce_count` option in the `/usr/OV/ITSL2/conf/correlator.ini` file. This option specifies the number of times an interface can go down within the interface bounce interval before it is correlated as down. In this case, an interface is considered down only when an Interface Down event is received from the Tivoli NetView product.

- To configure the interface bounce interval, modify the `interface_bounce_interval` option in the `/usr/OV/ITSL2/conf/correlator.ini` file.

This option specifies the length of time, in seconds, against which the accumulated bounce count is measured before an interface is correlated as down. The status of the interface remains down until an Interface Up event is received from the Tivoli NetView product, and the interface remains up until the interface bounce interval has expired. The default value is 3600 seconds (one hour).
For example, if the interface bounce count is set to 3 and the interface bounce interval is set to one hour, the interface is correlated as down after three down events occur within one hour. If the interface then remains up for one hour, its status is reset to up.

- To configure the preferred polling method, modify the `polling_method` option in the `/usr/OV/ITSL2/conf/correlator.ini` file. This option specifies the preferred polling method used by the correlator polling process. The value of this option is either `icmp` or `snmp`. The default is `icmp`. Tivoli Switch Analyzer uses ICMP to ping layer 3 interfaces and SNMP for querying port status. If the specified polling method is not available for a particular device, then the correlator uses the other polling method. For example, ICMP polling cannot be used for an interface that does not have an IP address.

- To specify the polling wait time, modify the `polling_wait_time` option in the `/usr/OV/ITSL2/conf/correlator.ini` file. This option specifies the amount of time in seconds to wait after an interface goes down before starting the correlator polling process. The purpose of the parameter is to wait a small amount of time for the interface to come back up before starting the polling process, or to ensure that it is down due to loss of signaling (for example, the local management interface (LMI) with frame relay circuits).

The polling wait time is included within the interface timeout interval (defined by the `interface_timeout` parameter), so a polling wait time greater than 0 causes the internal polling process to take longer. Therefore, you must increase the value of the `interface_timeout` parameter if a polling wait time is specified.

The default value for the `polling_wait_time` parameter is 0. This is based on the assumption that a timeout or retry mechanism is already being used by the Tivoli NetView product. Specify a value based on known or assumed delays with signaling loss caused by interface down conditions.

For example, specify a value between 15 - 30 seconds to allow for the delay in LMI loss for interfaces before the Tivoli Switch Analyzer starts verifying that the interfaces are down.

- To configure the status polling interval, modify the `status_poll_interval` option in the `/usr/OV/ITSL2/conf/correlator.ini` file. This option specifies the amount of time, in seconds, that the Tivoli Switch Analyzer internal polling process waits between interface polls. (This option refers to polling related to the root cause analysis engine and not port status monitoring.) Any polling result obtained by the polling process is valid for this amount of time specified by the polling interval. The interface is not polled again until this time has expired.

The default value is 15 seconds.

- To specify the polling interval for managed interfaces, modify the `man_poll_interval` option in the `/usr/OV/ITSL2/conf/correlator.ini` file. This option specifies how often Tivoli Switch Analyzer polls an interface if it is currently managing that interface. (This option refers to polling related to the root cause analysis engine and not port status monitoring.) Tivoli Switch Analyzer starts to manage an interface when it is polled down and no interface down event has been received by the Tivoli NetView product. Once the down event is received by the Tivoli NetView product, Tivoli Switch Analyzer stops managing the interface.

The default value is 60 seconds.
Configuring the port status monitor

Several configuration files contain options that affect the operation of the port status monitor. By modifying these files, you can specify which switches you want to manage and customize the behavior of the port status monitor.

Configuring which switches to monitor

By default, the port status monitor polls all switches within the discovered layer 3 Tivoli NetView topology. You can change this behavior by adding or modifying entries in the switch table.

1. Using a text editor, open the /usr/OV/ITSL2/conf/files/l2_polling.cfg configuration file. This file contains the switch table, which determines which devices are monitored.
2. Add or modify the entries in the switch table. For more information, see “Switch table syntax.”
3. Stop and restart the itsl2 daemon. For more information, see “Starting and stopping Tivoli Switch Analyzer” on page 45.

Switch table syntax

The switch table contains one or more entries, each on a separate line. Each entry defines a set of criteria, and specifies whether switches matching those criteria should be polled by the port status monitor.

Each switch table entry has eight fields separated by vertical bar characters (|):

`type|description|layer_2|OID|IP_address|hostname|manage|ports`

The fields are as follows:

- **type**  
The type of entry. In the switch table, this should always be `switch`.
- **description**  
A textual label for the device or devices described by the entry (for example, all switches or Cisco 6509).
- **layer_2**  
Whether the entry applies only to layer 2 switches. A value of `Y` indicates that the entry describes only layer 2 switches; layer 3 devices that otherwise match the entry are excluded. A value of `N` indicates that the entry describes any matching device, including layer 2 switches.

If you want to monitor layer 3 devices, add entries describing those devices and specify `N` in this field.

**Note:** The `layer_2` field should be set to `N` only for entries describing small sets of specific switches. If the matching criteria are too broad, the result could be polling every connector device within the Tivoli NetView topology, causing excessive network traffic. In particular, do not modify the default switch table entry to specify `N` in the `layer 2` field.

- **OID**  
The object identifier of the device. This field can contain wildcard characters (see note).
- **IP_address**  
The IP address of the device. This field can contain wildcard characters.
hostname
The TCP/IP host name (as it displays in the Tivoli NetView topology) of the device. This field can contain wildcard characters.

manage
Whether matching devices are to be polled. If this field is set to Y, devices matching the entry are polled by the port status monitor. If this field is set to N, matching devices are excluded from polling.

ports
Indicates whether to manage all ports or only ports connected to Tivoli NetView objects. If this field is set to A, all ports are managed. If this field is set to C, only ports connected to Tivoli NetView objects are managed.

Note: The OID, IP_address, and hostname fields can contain wildcard characters; an asterisk (*) matches any sequence of characters, and a question mark (?) matches any single character. For example, you might use wildcard characters in the following ways:
- The value 9.27.* in the IP_address field matches any device with an IP address within the 9.27.* subnet.
- The value *.ibm.com in the hostname field matches any device in the ibm.com domain.
- The value * in the OID field matches any OID. (Leaving a field blank is equivalent to specifying an asterisk.)

By default, the switch table contains a single entry specifying that all layer 2 connector devices in the Tivoli NetView topology should be monitored. The fields in this entry have the following values:

<table>
<thead>
<tr>
<th>type</th>
<th>description</th>
<th>layer 2</th>
<th>OID</th>
<th>IP address</th>
<th>hostname</th>
<th>manage</th>
<th>ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch</td>
<td>monitor all layer 2 switches</td>
<td>Y</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Y</td>
<td>A</td>
</tr>
</tbody>
</table>

These values are specified by the following line in the l2_polling.cfg file:

```
switch|monitor all layer 2 switches|Y|*|*|*|Y|A|
```

Precedence

The sequencing of entries in the switch table is significant. For each switch, the port status monitor processes the switch table from the top down and stops when it reaches the first matching entry. Only the first matching entry is applied to that switch.

You can therefore use the sequencing of switch table entries to include or exclude any subset of switches. To exclude certain switches from monitoring, you can add entries for those switches (specifying N in the manage field), placing the new entries above any other matching entry. For example, a switch table containing the following entries would result in monitoring all Cisco layer 2 switches except for those in the 192.168.30 subnet:

```
switch|exclude 192.168.30 subnet|Y|*|192.168.30.*|*|N|A|
switch|monitor all Cisco switches|Y|1.3.6.1.4.1.9.*|*|*|Y|A|
```

Port status monitor polling

The port status monitor uses SNMP queries to determine the status of each managed switch port. By default, the status for the port is calculated based on the administrative status (ifAdminStatus) and operational status (ifOperStatus) SNMP variables:
Configuring port status monitoring options

You can configure several options that affect the behavior of the port status monitor.

- To enable or disable port status monitoring, modify the `manage_layer2` option in the `/usr/OV/ITSL2/conf/correlator.ini` file. You can specify a value of `y` (enabled) or `n` (disabled). The default setting is `y`. If port status monitoring is disabled, switches are not polled for status changes.

- To change the SNMP query timeout, modify the `l2_snmp_timeout` option in the `/usr/OV/ITSL2/conf/correlator.ini` file. This option controls how long the port status monitor waits for responses to SNMP queries before retrying. The value can be any duration in milliseconds; the default value is 5000.

- To specify whether all configured ports managed by the port status monitor are polled during each polling cycle, modify the `poll_all_ports` option in the `/usr/OV/ITSL2/conf/correlator.ini` file. This option can be used to optimize port status monitoring in large network environments. If this option is set to `n`, the port status monitor polls only those ports for which it cannot rely upon the correlation process to detect outages. This would include the following:
  - Any port that is not connected to a managed node. No Tivoli NetView event would result from a layer 2 outage that does not affect a managed node.
  - Any port that is part of a redundant path to a managed node. No Tivoli NetView event would result if the connected node does not become unreachable.

Setting `poll_all_ports` to `n` can help to reduce excessive network traffic in large environments. However, this optimization should be used with caution, because it relies upon the accuracy of the discovered layer 2 topology information. By default, this option is set to `y` (all ports are polled in each polling cycle).

- To change the polling frequency, modify the `poll_cycle` option in the `l2_event_adapter.ini` file. This option defines the length of time between port status monitoring polling cycles. Specify a polling interval in seconds; the default value is 300.

- To change the retry count, modify the `retry_cnt` option in the `l2_event_adapter.ini` file. This option determines how many times the port status monitor attempts to query a device before setting its status to unreachable. The default value is 2.

### Tivoli Switch Analyzer logs

All Tivoli Switch Analyzer log files are stored in the `/usr/OV/ITSL2/log` directory. The following types of messages are provided:

- Debug
- Information
- Warning
- Error
- Abort
For most problems, Tivoli Switch Analyzer creates log files based on the component that caused the problem. The file is named component.log, where component is the name of the Tivoli Switch Analyzer component. For example, if the ext_cmd_server component shuts down unexpectedly, the following message is written to the ext_cmd_server.log file:

component [External Command Server]: shutdown abnormally

If a component log file is not created, browse the coordinator.log file.

If there is no log file, or if the Program started message is not in the log, browse the component.err file in the /usr/OV/ITSL2/bin directory.

Gathering debugging information

If you need to contact IBM Software Support for help with a Tivoli Switch Analyzer problem, you might need to provide log information for debugging purposes. Tivoli Switch Analyzer includes a script you can use to gather the required information in a single file.

To create a debugging file, run one of the following scripts:
• On a Linux or UNIX system, run the /usr/OV/ITSL2/etc/getdebug.sh script.
• On a Windows system, run the \usr\ov\itsl2\bin\getdebug.bat script.

The resulting file is named /usr/OV/ITSL2/alldebug<datetimestamp>.tar.Z. It is a compressed file containing all of the appropriate log files.

IBM Software Support may ask you to enable additional debugging information. You can do this without stopping the daemons by running the turnondebug.sh script. Running the turnoffdebug.sh script disables the additional debugging information.

Log descriptions

The following logs are provided:

/usr/OV/ITSL2/log/coordinator.log
This log is for the Tivoli Switch Analyzer component. Browse this log first if Tivoli Switch Analyzer or a component stops unexpectedly. The log file contains the following information:
• The times when components were stopped or started
• Messages passed between components

/usr/OV/ITSL2/log/correlator.log
This log is for the correlator component. Use this log to determine when and how events were correlated. The log contains the following information:
• Raw events received
• Which devices were polled and the polling results
• Correlated events that were opened, updated, or closed

/usr/OV/ITSL2/log/event_controller.log
This log is for the event controller. The log contains the following information:
• A log of all events received (for example: raw, correlated, updates, traps, and so on)
This log is for the event receiver component. Use this log to determine information about raw events that were received from the OV/NV event adapter.

This is the log for the ext_cmd_server component. This log contains information about traps or events that were sent to the Tivoli NetView product.

This log is for the l2_topo_adapter component. The log contains information about processing of topology requests. Use this log to investigate topology processing and to debug errors in discovery for specific switches.

This log is for the Tivoli NetView command server component. Use this log to find information about topology dumps and requests. The log contains the following information:

- Times when a topology database dump was requested
- Information on how and when a topology dump was started or stopped and the number of rows retrieved
- Information on the topology requests made against the Tivoli NetView database (for example, interface additions)

This log is for the Tivoli NetView event adapter component. Use this log to browse information about raw event information that is received from the Tivoli NetView product. The log contains the following information:

- Connections with the Tivoli NetView trapd daemon
- Information on all events or traps that were received from the Tivoli NetView trapd daemon

This log is for the polling server component. Use this log to browse information about polling activity. The log file contains the following information:

- Information on what devices or interfaces were polled.
- Results of all device polls.
- Errors from SNMP poll requests.

This log is for the topo_server component. The log contains information about topology requests for the topology views. Use this log to investigate unexpected behavior in the layer 2 views.

This log is for the route_server component. The log contains information
about routing requests for the Point to Point view. Use this log to investigate unexpected behavior in the Point to Point layer 3 path. This log contains information resulting from dynamic network requests to build the layer 3 path, such as request failures.

**Correlator client**

Use the correlator client to display Tivoli Switch Analyzer information. To start the correlator client, run the `/usr/OV/ITSL2/bin/corrcl` command. The Correlator Client Menu is displayed:

```
Correlator Client Menu
1) Print Network Object
2) Dump Topology Database
3) Query Network Object (Impact Analysis)
4) Layer 2 Discovery Request
q) Quit
Please enter choice:
```

**Print network object**

Menu option 1 prompts you to type the object type and the node ID as follows:

```
Enter Object ID: 7029
```

When you press Enter, the following information is displayed:

```
name: 192.168.47.3
IP address: 192.168.47.3
object status: up
redundant object: N
up interface count: 0
layer 2: 0
correlated object count: 0
IP forwarding: N
snmp enabled: N
community: 
layer 2 status: 
L2 Managed Object: Y
```

Press <ENTER> to continue...

**Dump topology database**

Menu option 2 dumps the topology database to the topo_db.out file located in the `/usr/OV/ITSL2/cache` directory.

**Query network object**

Menu option 3 provides impact analysis results for a specific interface or node.

Menu option 3 prompts you to type the following information:

```
Enter Object ID: 622
Enter output string [inst]:
Enter object qualifier [c]
```

**Note:**

1. Leave output string blank to use the default value.
2. The default value for object qualifier is blank, which means to return all objects. Specify c to return only connector objects.

The following is a sample of the impact analysis that is displayed:

```
--------------------------------------------------
Impact Analysis
--------------------------------------------------
192.168.30.254
192.168.30.254
--------------------------------------------------
```

press <ENTER> to continue...

---

**Configuring the Web servlet**

Under normal operating conditions, you should not need to modify the Tivoli Switch Analyzer Web servlet parameters. These parameters should only be modified with the advice and guidance of IBM Software Support.

The following Web servlet parameters may be modified by editing the `/usr/OV/www/webapps/netview/WEB-INF/web.xml` file on the Tivoli NetView server machine:

- **ClientPollInterval**
  Determines how often Web consoles poll the Web server for updates after a view is opened. The default value is 5 seconds.

- **ClientTimeout**
  Determines how long messages are kept on the Web server for a Web console before they are removed. The default value is 60 seconds. This means that any updates sent to that Web console are lost, and any views the Web console had open will be closed if that Web console polls again. This setting protects the memory on the Web server from handling too many updates for a Web console that may disconnect without appropriately closing.

- **ClientRequestTimeout**
  Determines how long the Web console waits for Tivoli Switch Analyzer to respond before timing out. The default setting is 120 seconds. You might need to increase this value for larger networks. See "Configuring the ClientRequestTimeout value" for information on how to adjust this setting.

---

**Configuring the ClientRequestTimeout value**

When opening a layer 2 view, the Web console communicates with the server for information. If the Web console does not receive a reply after two minutes, a timeout message is displayed. Under normal circumstances, the 2 minute default timeout is sufficient, and does not require modification. If you are experiencing occasional timeouts, especially on the longer Point to Point paths, you might want to increase this value.

To adjust the ClientRequestTimeout, do the following steps:

1. Open the web.xml file.
2. Look for the following block of lines and modify the number of seconds:

   ```xml
   <init-param>
   <param-name>ClientRequestTimeout</param-name>
   <param-value>120</param-value>
   </init-param>
   ```
Web servlet and console debugging

This section describes Web servlet and console debugging.

It includes the following sections:

- "Server logging"
- "Web console logging"
- "Web console logging"

Server logging

All logging for the Tivoli Switch Analyzer server is handled by the existing getdebug scripts, see "Gathering debugging information" on page 53. The topo_server.log file is specific to the layer 2 views.

Web servlet logging

To capture data in the servlets, edit the /usr/OV/www/classes/log4j.properties file on the Tivoli NetView server machine and modify the following line:

log4j.category.com.magnum_tech=INFO, ITSA

Change the word INFO to DEBUG, shown in the following example:

log4j.category.com.magnum_tech=DEBUG, ITSA

You also need to make sure that the following statements exist in this file. If they do not, add them to the file:

log4j.appender.ITSA=org.apache.log4j.RollingFileAppender
log4j.appender.ITSA.File=/usr/OV/ITSL2/log/ITSAUIservlet.log
log4j.appender.ITSA.MaxFileSize=10MB
log4j.appender.ITSA.MaxBackupIndex=2
log4j.appender.ITSA.layout=org.apache.log4j.PatternLayout
log4j.appender.ITSA.layout.ConversionPattern=%d{ISO8601} [%t] %-5p %c %x - %m%n

Stop and restart the Tivoli NetView Web server after editing this file.

Web console logging

To capture data on the Web consoles, do the following steps:

1. Open the following file:
   - If the Web console is running on the Tivoli NetView Server machine, edit the /usr/OV/www/webapps/netview/log4j.properties file.
   - If the Web console is running on a different machine, the log4j.properties file is located in the following directory:
     - On Windows systems: \program files\Tivoli Systems\Tivoli NetView Web Console\lib\log4j.properties
     - On UNIX or Linux systems: MYWEBDIR/nvwc/lib/log4j.properties
       Where MYWEBDIR is the directory where you installed the Tivoli NetView Web console.

   You cannot log to a file if you are running the Web console as an applet through a Web browser. Run the Web console as an application by typing nvwc.sh on UNIX or Linux, or for Windows, using the Start menu or typing nvwc.bat.

2. Modify the following line:

log4j.category.com.magnum_tech=INFO, A1
Change this line to the following or add it if it does not exist in this file:

```java
log4j.category.com.magnum_tech=DEBUG, ITSAC
```

**Note:** A1 indicates logging is displayed on the screen and not saved to a file. Changing A1 to ITSAC logs to the file specified by the `log4j.appender.ITSAC.File` property shown below in 3. You cannot run the Web console as an applet through a Web browser when ITSAC is set for the `log4j.category.com.magnum_tech` property.

3. Check that the following lines exist in the file, or add them if they do not:

```java
log4j.appender.ITSAC=org.apache.log4j.RollingFileAppender
log4j.appender.ITSAC.File=/usr/OV/ITSL2/log/ITSAUIclient.log
log4j.appender.ITSAC.MaxFileSize=10MB
log4j.appender.ITSAC.MaxBackupIndex=2
log4j.appender.ITSAC.layout=org.apache.log4j.PatternLayout
log4j.appender.ITSAC.layout.ConversionPattern=%d{ISO8601} [%t] %-5p %c %x - %m%n
```

If you are running the Web console on a machine other than the Tivoli NetView server, you need to specify a different file name than `/usr/OV/ITSL2/log/ITSAUIclient.log` for the `log4j.appender.ITSAC.File` property, in the lines for 3 above.

4. Stop and restart the Tivoli NetView Web console after changing this file.
Chapter 8. Reference information

This chapter provides reference information for Tivoli Switch Analyzer.

Tivoli Switch Analyzer scripts

On UNIX systems, the Tivoli Switch Analyzer program provides the following scripts:

```
/usr/OV/ITSL2/etc/getdebug.sh
    The debug script that is used to collect and compress log files for IBM Software Support. See "Gathering debugging information" for information on this script.
```

```
/usr/OV/ITSL2/etc/turnondebug.sh
    This script is used to activate debugging. The itsl2 daemon does not need to be recycled.
```

```
/usr/OV/ITSL2/etc/turnoffdebug.sh
    This script is used to deactivate debugging. The itsl2 daemon does not need to be recycled.
```

```
/usr/OV/ITSL2/bin/L2_lookup
    This script is used for quick lookups of layer 3 devices. See "Using the L2_lookup script" for more information on this script.
```

On Windows systems, the Tivoli Switch Analyzer program provides the following scripts:

```
\usr\ov\itsl2\bin\getdebug.bat
    This script is used to package the logs and cache prior to sending to IBM Software Support. See "Gathering debugging information" for information on this script.
```

```
\usr\ov\itsl2\bin\turnondebug.bat
    This script is used to activate debugging dynamically. The itsl2 daemon does not need to be recycled.
```

```
\usr\ov\itsl2\bin\turnoffdebug.bat
    This script is used to deactivate debugging dynamically. The itsl2 daemon does not need to be recycled.
```

```
\usr\ov\itsl2\bin\L2_lookup.bat
    This script is used for quick lookups of layer 3 devices. See "Using the L2_lookup script" for more information on this script.
```

Using the L2_lookup script

The L2_lookup script is a command line utility used for quick look-ups of layer 3 devices. You can use any combination of search criteria, to obtain layer 3 IP interfaces.

To use the L2_lookup script, run one of the following commands:

- On a Windows system, from a command line run
  
  \usr\ov\itsl2\bin\L2_lookup.bat

  Add the appropriate parameters.
On a Linux or UNIX system, from a command line run

```
/usr/0V/ITSL2/bin/L2_lookup
```

Add the appropriate parameters.

This command launches the L2_lookup script which uses the following syntax:

```
L2_lookup [-s switchname] [-o switchOID] [-p port_ifindex] [-i IPaddress]
[-m MACaddress][-M][-h]
```

The L2_lookup script has the following parameters:

- The `-s` parameter specifies the Tivoli NetView selection name of a switch. If you specify a selection name, the output includes only information for the specified switch.
- The `-o` parameter specifies the Tivoli NetView object identifier of a switch. If you specify an object identifier, the output includes only information for the specified switch.
- The `-p` parameter specifies the switch port ifIndex. If you specify a switch port ifIndex, the output includes only information for the specified port.
- The `-i` parameter specifies the interface IP address. If you specify IP address, the output includes only information for the specified IP address.
- The `-m` parameter specifies the interface MAC address. If you specify MAC address, the output includes only information for the specified MAC address.
- The `-M` parameter includes MAC addresses in the output.
- The `-h` parameter displays the L2_lookup script usage statement.

For example, to find out which switch/port 1.168.0.12 is connected to, type the following from a command line:

```
L2_lookup -i 1.168.0.12 -M
```

```
1.168.0.12, 00096B7C4506,rtp-cs50b.lab.com,12
```

To discover which nodes are connected to ifIndex 12 on rtp-cs50b.lab.com type the following from a command line:

```
L2_lookup -s rtp-cs50b.lab.com -p 12
```

```
1.168.0.12,rtp-cs50b.lab.com,12
```

---

**Traps and events**

This section provides information about traps and events sent and received by Tivoli Switch Analyzer:

**Tivoli Switch Analyzer traps**

The following Tivoli Switch Analyzer traps are generated with ITSL2 enterprise ID 1.3.6.1.4.1.5593:

1. Interface_Down
2. Node_Down
3. Node_Marginal
4. Interface_Up
5. Interface_Unmanaged
6. Interface_Deleted
7. Node_Up
8. Node_Unmanaged
9. Node_Resolved
10. Node_Deleted
Tivoli Switch Analyzer traps use the following common set of variable bindings (varbinds):

**Varbind**

<table>
<thead>
<tr>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
</tbody>
</table>

**Tivoli NetView traps**

Tivoli NetView traps provide topology layer 2 status updates for switches. The following traps are generated with Tivoli NetView enterprise ID 1.3.6.1.4.1.2.6.3:

- Layer 2 Device Up
- Layer 2 Device Marginal
- Layer 2 Device Down

Tivoli NetView traps use the following standard Tivoli NetView varbinds:

**Varbind**

<table>
<thead>
<tr>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
</tbody>
</table>

**Tivoli Enterprise Console events**

By default, Tivoli Switch Analyzer is configured to forward events to the Tivoli Enterprise Console product. This section provides information about Tivoli Enterprise Console events that are forwarded.

See the Tivoli NetView for UNIX library or the Tivoli NetView for Windows library for information about filtering traps.
Tivoli Enterprise Console rules determine how these events are managed as follows:

- Clearing a previous event for same object
- Determining the severity of an event
- Correlating the event with other Tivoli NetView events for the same object, and closing other events if this is considered the root cause

See the Tivoli Enterprise Console library and netview.rls file for more information about the rules.

The following events are forwarded to Tivoli Enterprise Console:

**TEC_ITS_SA_STATUS**

Traps from the Tivoli Switch Analyzer are converted to the TEC_ITS_SA_STATUS event class. The following attributes are used:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter_host</td>
<td>The node name of the Tivoli NetView management station.</td>
</tr>
<tr>
<td>hostname</td>
<td>Varbind 7: The node name or IP address</td>
</tr>
<tr>
<td>hostaddr</td>
<td>Varbind 16: Node IP address</td>
</tr>
<tr>
<td>msg</td>
<td>Varbind 12: Description</td>
</tr>
<tr>
<td>category</td>
<td>Vendor-related</td>
</tr>
<tr>
<td>sastatus</td>
<td>The status number:</td>
</tr>
<tr>
<td></td>
<td><strong>Status number</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Status message</strong></td>
</tr>
<tr>
<td></td>
<td>1  Interface Down</td>
</tr>
<tr>
<td></td>
<td>2  Node Down</td>
</tr>
<tr>
<td></td>
<td>3  Node Marginal</td>
</tr>
<tr>
<td></td>
<td>4  Interface Up</td>
</tr>
<tr>
<td></td>
<td>5  Interface Unmanaged</td>
</tr>
<tr>
<td></td>
<td>6  Interface Deleted</td>
</tr>
<tr>
<td></td>
<td>7  Node Up</td>
</tr>
<tr>
<td></td>
<td>8  Node Unmanaged</td>
</tr>
<tr>
<td></td>
<td>9  Node Resolved</td>
</tr>
<tr>
<td></td>
<td>10 Node Deleted</td>
</tr>
<tr>
<td>saticketnumber</td>
<td>Varbind 3: Ticket number</td>
</tr>
</tbody>
</table>

**TEC_ITS_L2_STATUS**

Layer 2 status traps from Tivoli NetView are converted to the TEC_ITS_L2_STATUS event class. The values are:

- Up
- Down
- Marginal
Chapter 9. Messages

Messages are sorted in numerical order to make them easier to locate.

For each message, the following information is presented:

Severity
Can be the following:

- informational
  No user action is required. A message number that ends with the letter I is an informational message.

- warning
  Determine whether you need to change anything. A message number that ends with the letter W is a warning message.

- error
  Correct the specific process or application and restart it. A message number that ends with the letter E is an error message.

Explanation
The explanation describes the condition that was detected.

Action
The action describes the steps that can often remedy the problem. You may want to add annotations to this section to document actions specific to your site.

When you view a message online, you see words or phrases in the Explanation or Action paragraphs that are highlighted in blue. These are links to more information about the highlighted term. For example, links on daemon names typically show you the man page for that daemon. Use these links to find more information about the correct use of Tivoli NetView components.

Some messages represent logic problems that should not occur. The action for these messages is to contact IBM Customer Support.

Messages

**AMU00000001E** You must select exactly one object.

Explanation: The requested action can only be performed with one object selected.

Problem Determination: Some of the JAR files or WARF files may be out of sync, or some other problem is occurring. Verify that no changes have been made to the WARF files.

**AMU00000002E** You must select one or two objects.

Explanation: The requested action can only be performed with one or two objects selected.

Problem Determination: Some of the JAR files or WARF files may be out of sync, or some other problem is occurring. Verify that no changes have been made to the WARF files.
AMU00000003E  Tivoli Switch Analyzer cannot find node [0]. Reopen the current view or wait for the update to occur.

Explanation: The object selected for this request does not exist in the Tivoli Switch Analyzer topology database. This might occur because the object was removed and is not reflected in the current view.

Problem Determination: Try using a fully-qualified name, opening the current view again or waiting for the update to occur.

AMU00000004E  Tivoli Switch Analyzer cannot find object [0]. Reopen the current view or wait for the update to occur.

Explanation: The object selected for this request does not exist in the Tivoli Switch Analyzer topology database. This might occur because the object was removed and is not reflected in the current view.

Problem Determination: Try using a fully-qualified name, opening the current view again or waiting for the update to occur.

AMU00000005E  Invalid object [0] for request. Reopen the current view or wait for the update to occur.

Explanation: The object selected for this request does not exist in the Tivoli Switch Analyzer topology database. This might occur because the object was removed and is not reflected in the current view.

Problem Determination: Try using a fully-qualified name, opening the current view again or waiting for the update to occur.

AMU00000006I  The node [0] has no VLANs.

Explanation: This is an unexpected situation.

Problem Determination: Error logs can be produced by running the following command:

On Windows systems: %W_DRIVE%\usr\OV\ITSL2\bin\getdebug
On UNIX systems: /usr/0V/ITSL2/etc/getdebug.sh

Please contact IBM Software Support and forward the logs. See “Support information” on page 71 for more information about contacting IBM Software Support.

AMU00000007E  VLAN id [0] is not valid.

Explanation: This is an unexpected situation.

Problem Determination: Error logs can be produced by running the following command:

On Windows systems: %W_DRIVE%\usr\OV\ITSL2\bin\getdebug
On UNIX systems: /usr/0V/ITSL2/etc/getdebug.sh

Please contact IBM Software Support and forward the logs. See “Support information” on page 71 for more information about contacting IBM Software Support.

AMU00000008E  Tivoli Switch Analyzer cannot find VLAN [0].

Explanation: This is an unexpected situation.

Problem Determination: Error logs can be produced by running the following command:

On Windows systems: %W_DRIVE%\usr\OV\ITSL2\bin\getdebug
On UNIX systems: /usr/0V/ITSL2/etc/getdebug.sh

Please contact IBM Software Support and forward the logs. See “Support information” on page 71 for more information about contacting IBM Software Support.
<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Explanation</th>
<th>Problem Determination</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMU00000009E</td>
<td>Invalid hop count {0}.</td>
<td>Tivoli Switch Analyzer received a request for an invalid hop count.</td>
<td>Error logs can be produced by running the following command: On Windows systems: %NV_DRIVE%\usr\OV\ITSL2\bin\getdebug On UNIX systems: /usr/0V/ITSL2/etc/getdebug.sh Please contact IBM Software Support and forward the logs and a copy of the WARF files. See <a href="#">Support information</a> on page 71 for more information about contacting IBM Software Support. Send logs with full debugging and a copy of the WARF files.</td>
</tr>
<tr>
<td>AMU00000010E</td>
<td>Tivoli Switch Analyzer is unavailable.</td>
<td>The Tivoli NetView server cannot contact the Tivoli Switch Analyzer daemon.</td>
<td>Verify that the Tivoli Switch Analyzer daemon (itsl2) is running by clicking <strong>Tools</strong> –&gt; <strong>Server Status</strong> from the Web console.</td>
</tr>
<tr>
<td>AMU00000011E</td>
<td>Tivoli Switch Analyzer topology is unavailable. Try running the command again in a few minutes.</td>
<td>The topology database is currently unavailable, so requests cannot be processed.</td>
<td>Try running the command again in a few minutes.</td>
</tr>
<tr>
<td>AMU00000012I</td>
<td>View {0} has been deleted.</td>
<td>This message is displayed when a view is no longer valid. A view could become invalid if the node is deleted or unmanaged from Tivoli NetView.</td>
<td>Request a view on a different node.</td>
</tr>
<tr>
<td>AMU00000013E</td>
<td>The view is already waiting for an update. Wait for the update before requesting a new update.</td>
<td>An update was requested to a view that is still waiting for a previously requested update.</td>
<td>Wait for the update before requesting a new update.</td>
</tr>
<tr>
<td>AMU00000014E</td>
<td>The request for view {0} has timed out. The view will be closed.</td>
<td>A view has timed out.</td>
<td>Open the view again.</td>
</tr>
<tr>
<td>AMU00000015E</td>
<td>The start and end nodes are the same. Choose start and end nodes that are different.</td>
<td>A point to point view was requested with the same start and end nodes.</td>
<td>Choose start and end nodes that are different.</td>
</tr>
<tr>
<td>AMU00000016E</td>
<td>Internal error processing request.</td>
<td>An internal error prevented the topology server from processing the request.</td>
<td>Error logs can be produced by running the following command: On Windows systems: %NV_DRIVE%\usr\OV\ITSL2\bin\getdebug On UNIX systems: /usr/0V/ITSL2/etc/getdebug.sh Please contact IBM Software Support and forward the logs and a copy of the WARF files. See <a href="#">Support information</a> on page 71 for more information about contacting IBM Software Support. Send logs with full debugging and a copy of the WARF files.</td>
</tr>
</tbody>
</table>
On Problem Explanation: AMU00065540E

Explanation: A point to point view was requested but the start node does not have a valid IP address and a reverse lookup is not possible using the specified end node.

Problem Determination: Choose at least one device that is SNMP-enabled, has a valid IP address and is not a L2 switch and try again.

On Problem Explanation: AMU00065539E

Explanation: A point to point view was requested but the start node is not SNMP-enabled and a reverse lookup is not possible using the specified end node.

Problem Determination: Choose at least one device that is SNMP-enabled, has a valid IP address and is not a L2 switch and try again.

On Problem Explanation: AMU00065538E

Explanation: The start node is a L2 switch. The end node either does not have a valid IP address, is not SNMP-enabled, or is a L2 switch. Choose at least one device that is SNMP-enabled, has a valid IP address and is not a L2 switch and try again.

Problem Determination: Choose at least one device that is SNMP-enabled, has a valid IP address and is not a L2 switch and try again.

On Problem Explanation: AMU00065537E

Explanation: The start node does not support SNMP. The end node either does not have a valid IP address, is not SNMP-enabled, or is a L2 switch. Choose at least one device that is SNMP-enabled, has a valid IP address and is not a L2 switch and try again.

Problem Determination: Choose at least one device that is SNMP-enabled, has a valid IP address and is not a L2 switch and try again.

On Problem Explanation: AMU00065536E

Explanation: The start node does not have a valid IP address. The end node either does not have a valid IP address, is not SNMP-enabled, or is a L2 switch. Choose at least one device that is SNMP-enabled, has a valid IP address and is not a L2 switch and try again.

Problem Determination: Choose at least one device that is SNMP-enabled, has a valid IP address and is not a L2 switch and try again.

Tivoli Switch Analyzer cannot change the directory to %1$s. Verify that this directory exists and has the correct permissions.

Problem Determination: Verify that this directory exists and has the correct permissions.

Tivoli Switch Analyzer cannot open the coordinator.err file.

Explanation: Tivoli Switch Analyzer cannot open the file named in the message.

Problem Determination: Verify the permissions on the following directory:

- On Windows systems: %NV_DRIVE%\usr\ov\itsl2\bin
- On UNIX systems: /usr/OV/ITSL2/bin

Tivoli Switch Analyzer cannot open the coordinator.ini file.

Explanation: Tivoli Switch Analyzer cannot open the file named in the message.

Problem Determination: Verify that the following file exists and has the correct permissions:

- On Windows systems: %NV_DRIVE%\usr\ov\itsl2\conf\coordinator.ini
- On UNIX systems: /usr/OV/ITSL2/conf/coordinator.ini

Tivoli Switch Analyzer cannot process the coordinator.ini file.

Explanation: The coordinator file contains an unexpected value.

Problem Determination: Check the following file for the specific error:

- On Windows systems: %NV_DRIVE%\usr\ov\itsl2\bin\coordinator.err
- On UNIX systems: /usr/OV/ITSL2/bin/coordinator.err
Tivoli Switch Analyzer cannot open the coordinator.log file.

**Problem Determination:** Verify the permissions on the following directory:

- On Windows systems: `%NV_DRIVE%\usr\ov\itsl2\log`
- On UNIX systems: `/usr/OV/ITSL2/log`

Tivoli Switch Analyzer cannot connect to the Tivoli NetView trap daemons: `%1$s`.

**Problem Determination:** Verify that the Tivoli NetView daemons are running.

Tivoli Switch Analyzer failed.

**Problem Determination:** Check the following file for errors:

- On Windows systems: `%NV_DRIVE%\usr\ov\itsl2\log\coordinator.log`
- On UNIX systems: `/usr/OV/ITSL2/log/coordinator.log`

When checking for Tivoli Switch Analyzer errors, do the following steps:

1. Search for the word `Error` starting from the end of the file. The first line that you find often contains an error message that indicates which component failed. For example: `Error: component [Correlator]: shutdown abnormally`.

2. Search for the word `Abort`. These lines often indicate what the actual problem is. For example: `Abort: cannot find node for management system host: bos-lnx03-rhas30 [172.30.130.133]`

Tivoli Switch Analyzer cannot switch to NV_DRIVE.

**Explanation:** The selected drive cannot be accessed.

**Problem Determination:** Verify that the NV_DRIVE environment variable is set, and that the drive is accessible.

Tivoli Switch Analyzer cannot open the ITSL2 message catalog.

**Problem Determination:** Verify that the following message catalog exists:

- Windows: `%NV_DRIVE%\usr\ov\nls\%LANG%\itsl2.dll`
- UNIX: `/usr/OV/nls/C/ITSL2.cat`

Option `-%1$s` requires an argument.

**Explanation:** The arguments used to start a component are incorrect or missing.

**Problem Determination:** Verify the arguments used to start the component listed. This error occurs only if a change is made to the default settings in the ini files.

Unrecognized option: `-%1$s`

**Explanation:** The arguments used to start a component are incorrect or missing.

**Problem Determination:** Verify the arguments used to start the component listed. This error should only occur if a change is made to the default settings in the ini files.

Invalid menu choice

**Explanation:** Invalid option selected while running the correlator client (corrcl).

**Problem Determination:** Use one of the following valid options:

- Print Network Object
- Dump Topology Database
- Query Network Object (Impact Analysis)
- Layer 2 Discovery Request
- Quit
**AMU00393261W**  Invalid object ID

**Problem Determination:** Verify the object ID entered for the correlator client (corrcl). The object ID must be a positive integer.

**AMU00393262W**  Invalid object type

**Explanation:** This error can occur for option 3 (Query Network Object) in the correlator client (corrcl).

**Problem Determination:** Verify that the object ID entered is for an interface or node object and not a segment or network object.

**AMU00393263W**  Tivoli Switch Analyzer is unable to establish a connection with the correlator server: %1$s.

**Explanation:** Tivoli Switch Analyzer cannot connect to the correlator server.

**Problem Determination:** Verify that the correlator component is running by using the following command:

Windows: %NV_DRIVE%\usr\ov\bin\ovstatus itsl2
UNIX: /usr/OV/bin/ovstatus itsl2

**AMU00393264W**  Tivoli Switch Analyzer cannot connect to the correlator server: %1$s.

**Explanation:** Tivoli Switch Analyzer cannot connect to the correlator server.

**Problem Determination:** Verify that the correlator component is running by using the following command:

Windows: %NV_DRIVE%\usr\ov\bin\ovstatus itsl2
UNIX: /usr/OV/bin/ovstatus itsl2

**AMU00393265W**  Tivoli Switch Analyzer cannot send a request to correlator server: %1$s.

**Problem Determination:** Verify that the correlator component is running by using the following command:

On Windows systems: %NV_DRIVE%\usr\ov\bin\ovstatus itsl2
On UNIX systems: /usr/OV/bin/ovstatus itsl2

**AMU00393266W**  There is an error in the reply from the correlator server.

**Problem Determination:** Verify that the correlator component is running by using the following command:

On Windows systems: %NV_DRIVE%\usr\ov\bin\ovstatus itsl2
On UNIX systems: /usr/OV/bin/ovstatus itsl2

**AMU00393267W**  Tivoli Switch Analyzer cannot receive a reply from the correlator server.

**Problem Determination:** Verify that the correlator component is running by using the following command:

On Windows systems: %NV_DRIVE%\usr\ov\bin\ovstatus itsl2
On UNIX systems: /usr/OV/bin/ovstatus itsl2

**AMU00393268W**  Request timed out.

**Problem Determination:** Verify that the correlator component is running by using the following command:

On Windows systems: %NV_DRIVE%\usr\ov\bin\ovstatus itsl2
On UNIX systems: /usr/OV/bin/ovstatus itsl2
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Problem Determination</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMU00393269W</td>
<td>Object [%1$s] does not exist in the Tivoli Switch Analyzer topology database.</td>
<td></td>
<td>Verify that the object id was entered correctly.</td>
</tr>
<tr>
<td>AMU00393270W</td>
<td>The topology database is currently unavailable.</td>
<td></td>
<td>Run the command again in a few minutes.</td>
</tr>
<tr>
<td>AMU00655469E</td>
<td>Error: Tivoli Switch Analyzer cannot open the [%1$s] topology file.</td>
<td></td>
<td>Verify that the following file exists:</td>
</tr>
<tr>
<td>AMU00655470E</td>
<td>Error: Tivoli Switch Analyzer cannot parse the interface record in the [%1$s] topology file.</td>
<td></td>
<td>Try waiting a few seconds and rerun the report. If the error still occurs, try running the ITSL2_reports command with the -d option to force a database dump. This creates the topo_db.out file before the report runs.</td>
</tr>
<tr>
<td>AMU00655471E</td>
<td>Error: Tivoli Switch Analyzer cannot parse the node record in the [%1$s] topology file.</td>
<td></td>
<td>Try waiting a few seconds and run the report again. If the error still occurs, try running the ITSL2_reports command with the -d option to force a database dump. This creates the topo_db.out file before the report runs.</td>
</tr>
<tr>
<td>AMU00655472E</td>
<td>Error: Tivoli Switch Analyzer cannot parse the segment record in the [%1$s] topology file.</td>
<td></td>
<td>Try waiting a few seconds and run the report again. If the error still occurs, try running the ITSL2_reports command with the -d option to force a database dump. This creates the topo_db.out file before the report runs.</td>
</tr>
<tr>
<td>AMU00655475E</td>
<td>Error: Computer is out of memory.</td>
<td></td>
<td>Check memory usage to see if processes are running correctly.</td>
</tr>
<tr>
<td>AMU01048726E</td>
<td>%1$s: Option %2$s requires an argument.</td>
<td></td>
<td>Verify script arguments. Run script with the -h option to get a list of valid arguments.</td>
</tr>
<tr>
<td>AMU01048729E</td>
<td>%1$s: Missing report name.</td>
<td></td>
<td>Verify script arguments. Run script with the -h option to get a list of valid arguments.</td>
</tr>
</tbody>
</table>
AMU01048730E  %1$s: Invalid report name.
Explanation: You tried to run a script with incorrect syntax. One of the script arguments is not valid.
Problem Determination: Verify script arguments. Run script with the -h option to get a list of valid arguments.

AMU01048731E  %1$s: Missing object id or selection name.
Explanation: You tried to run a script with incorrect syntax. One of the script arguments is missing.
Problem Determination: Verify arguments to script. Run script with -h to get a list of valid arguments.

AMU01048732W  Layer 2 topology data is currently not available.
Explanation: This problem usually occurs after the itsl2 daemon has started but before it has created the topo_db.out file from which the reports are generated. By default this file is generated at 15 minute intervals.
Problem Determination: Verify that the following file exists:
On Windows systems: %NV_DRIVE%\usr\ov\itsl2\cache\topo_db.out
On UNIX systems: /usr/OV/ITSL2/cache/topo_db.out
If it does not exist, try running the ITSL2_reports command with the -d option to force a database dump. This creates the topo_db.out file before the report runs. Check /usr/OV/ITSL2/log/correlator.log for possible error messages.

AMU01048733E  %1$s: Invalid option %2$s
Explanation: You tried to run a script with incorrect syntax. One of the script arguments is not valid.
Problem Determination: Verify the script arguments. Run the script with the -h option to get a list of valid arguments.

AMU01048737E  Tivoli Switch Analyzer cannot find object named %1$s for layer 2 report.
Explanation: Cannot find the object requested for a layer 2 report.
Problem Determination: The command is exiting. Verify that the object exists in Tivoli NetView.
Support information

This section describes the following options for obtaining support for IBM products:

- “Searching knowledge bases”
- “Obtaining fixes”
- “Contacting IBM Software Support” on page 72

Searching knowledge bases

If you have a problem with your IBM software, you want it resolved quickly. Begin by searching the available knowledge bases to determine whether the resolution to your problem is already documented.

Search the information center on your local system or network

IBM provides extensive documentation that can be installed on your local computer or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

Search the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, expand the product folder in the navigation frame to the left and select Web search. From this topic, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks™
- IBM developerWorks®
- Forums and newsgroups
- Google

Obtaining fixes

A product fix might be available to resolve your problem. You can determine what fixes are available for your IBM software product by checking the product support Web site:

2. Under Products A - Z, select your product name. This opens a product-specific support site.
3. Under Self help, follow the link to All Updates, where you will find a list of fixes, fix packs, and other service updates for your product. For tips on refining your search, click Search tips.
4. Click the name of a fix to read the description and optionally download the fix.

To receive weekly e-mail notifications about fixes and other news about IBM products, follow these steps:
1. From the support page for any IBM product, click My support in the upper-right corner of the page.

2. If you have already registered, skip to the next step. If you have not registered, click register in the upper-right corner of the support page to establish your user ID and password.

3. Sign in to My support.

4. On the My support page, click Edit profiles in the left navigation pane, and scroll to Select Mail Preferences. Select a product family and check the appropriate boxes for the type of information you want.

5. Click Submit.

6. For e-mail notification for other products, repeat Steps 4 and 5.

For more information about types of fixes, see the Software Support Handbook [http://techsupport.services.ibm.com/guides/handbook.html].

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

• For IBM distributed software products (including, but not limited to, Tivoli, Lotus, and Rational® products, as well as DB2® and WebSphere® products that run on Windows or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:
  - Online: Go to the Passport Advantage Web page [http://www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home] and click How to Enroll
  - By phone: For the phone number to call in your country, go to the IBM Software Support Web site [http://techsupport.services.ibm.com/guides/contacts.html] and click the name of your geographic region.

• For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries®, pSeries®, and iSeries™ environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page [http://www.ibm.com/servers/eserver/techsupport.html].

If you are not sure what type of software maintenance contract you need, call 1-800-IBMESERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web [http://techsupport.services.ibm.com/guides/contacts.html] and click the name of your geographic region for phone numbers of people who provide support for your location.

Follow the steps in this topic to contact IBM Software Support:

1. Determine the business impact of your problem.

2. Describe your problem and gather background information.

3. Submit your problem to IBM Software Support.
Determine the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

<table>
<thead>
<tr>
<th>Severity 1</th>
<th>Critical business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 2</td>
<td>Significant business impact: The program is usable but is severely limited.</td>
</tr>
<tr>
<td>Severity 3</td>
<td>Some business impact: The program is usable with less significant features (not critical to operations) unavailable.</td>
</tr>
<tr>
<td>Severity 4</td>
<td>Minimal business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.</td>
</tr>
</tbody>
</table>

Describe your problem and gather background information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

Submit your problem to IBM Software Support

You can submit your problem in one of two ways:

- **Online**: Go to the “Submit and track problems” page on the IBM Software Support site [http://www.ibm.com/software/support/probsub.html](http://www.ibm.com/software/support/probsub.html]. Enter your information into the appropriate problem submission tool.
- **By phone**: For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook on the Web (techsupport.services.ibm.com/guides/contacts.html) and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

For more information about problem resolution, see Searching knowledge bases and Obtaining fixes.
Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX  78758    U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Trademarks

IBM, the IBM logo, AIX®, DB2, IBMlink™, Informix®, OS/2®, Tivoli, the Tivoli logo, Tivoli Enterprise Console, and TME® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft® and Windows are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Intel®, the Intel Inside logos, MMX™, and Pentium® are trademarks of Intel Corporation in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET™ and the SET Logo are trademarks owned by SET Secure Electronic Transaction™ LLC.

Other company, product, and service names may be trademarks or service marks of others.
Index

A
accessibility vi
actions 32
adding new device types 12
administration 45

B
books
  see publications  v

C
cache files 47
cache frequency 47
cache frequency, changing 47
ClientPollInterval 56
ClientRequestTimeout 56
ClientTimeout 56
communityNames.conf file 5
configuring correlator options 48
configuring NetView Web server 8
configuring port status monitoring 52
configuring the Web servlet 56
conventions
  typeface vii
  coordinator process 46
  coordinator.log 53
  corcl command 55
  correlated layer 2 status, viewing 22
  correlation timeout delay for Interface
    Down events 48
  correlation timing 21
  correlation, layer 3 19
  correlator 17
  correlator client 55
  correlator frequency 48
  correlator options 48
  correlator options, configuring 48
  correlator process 46
  correlator processing 20
  correlator.ini file 47
  correlator.log 53
  customer support
    see Software Support 72

D
debugging 53
debugging Web servlet and console 57
deleted views 34
device types, adding 12
directory names, notation viii
disabling discovery 12
discovering the layer 3 network 4
discovery interval parameter 13
discovery report 40
discovery reports 14
discovery, disabling 12

E
education
  see Tivoli technical training vi
environment variables, notation viii
event_controller process 46
  event_controller.log 53
  event_receiver process 46
  event_receiver.log 54
events, Tivoli Enterprise Console 61
  ext_cmd_server process 46
  ext_cmd_server.log 54

F
fault detection 15
  fault detection, impact-based 15, 16
  finding missing switches 5
  fixes, obtaining 71

G
g flag 11
generating reports 37
  getdebug.bat 59
  getdebug.sh 59
  getting help 33

H
help, getting 33
  help, Tivoli NetView 33
  help, Tivoli Switch Analyzer 33
  hop count 27
  hop count, adjusting 27
  host name, specify 48

I
IBM Global Services ITSATool 3
impact analysis 2
  impact analysis report 41
  impact-based fault detection 15, 16
  importNvOids 12
information centers, searching to find
  software problem resolution 71
  installation verification 7
  installing Tivoli Switch Analyzer 3, 6
  installing Tivoli Switch Analyzer
    silently 7
  interface bounce count, configure 48
  interface bounce interval 48
  interface_bounce_count option 48
  interface_bounce_interval option, configure 48
  interface_timeout option 48
Internet, searching to find software
  problem resolution 71
  island 4
  itsl2 daemon processes 46
  itsl2 daemon, starting 45
  itsl2 daemon, stopping 45, 46
  ITSL2 Enterprise traps 20
  ITSL2_reports utility 40

K
knowledge bases, searching to find
  software problem resolution 71

L
l2_event_adapter process 46
  l2_event_adapter.log 54
  l2_event_receiver process 46
  l2_event_receiver.log 54
  l2_lookup 59
  l2_lookup script 59
  l2_lookup.bat 59
  l2_oids.cfg file 11, 12, 13
  l2_polling.cfg configuration file 50
  l2_topo_adapter process 46
  l2_topo_adapter.ini file 13
  l2_topo_adapter.log 54
  l2_topo_adapter.log file 12
  layer 2 discovery 11
  layer 2 status report 41, 42
  layer 2 status symbol 22
  layer 2 status, viewing 22
  layer 2 switches, unmanaging 12
  layer 2 topology, viewing 25
  layer 2 views 31
  layer 3 correlation 19
  Layer2Status field 20, 22
  log descriptions 53
  log/l2_topo_adapter.log file 14
  logs 52
  logs, coordinator 53
  logs, correlator 53
  logs, event_controller 53
  logs, event_receiver 54
  logs, ext_cmd_server 54
  logs, l2_event_adapter 54
  logs, l2_event_receiver 54
  logs, l2_topo_adapter 54
  logs, ov_cmd_server 54
  logs, ov_event_adapter 54
  logs, poll_server 54
  logs, route_server 54
  logs, topo_server 54

M
man_poll_interval option 49
managing layer 2 devices 1
manuals
  see publications  v
  MaximumCommunityNames option 5
  mgt_host_option 48
  missing switches 5

© Copyright IBM Corp. 2005