Cisco Configuration Assurance Solution - SPM Reference
SP Sentinel Release Notes

Software Release 11.5

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8458-01

Cisco Configuration Assurance Solution - SPM
Reference
SP Sentinel Release Notes

OPNET SP Sentinel 11.5 Release Notes

These release notes give an overview of the differences between OPNET SP Sentinel Release 11.5 and the previous release. If you are upgrading from a previous release, you should review this document.

Because release notes are sometimes updated after the product documentation is distributed, visit the OPNET website (www.opnet.com/support) often to check for the newest version of these release notes and previous release notes.

Contents

Part number: D00278
Version: 6

Release 11.5 Description

OPNET SP Sentinel 11.5 is a significant software update to the OPNET 11.0 major software release. This release contains several new features and enhancements to existing capabilities. This release also fixes many software problems reported in earlier releases.

System Requirements

Be sure to check the latest system requirements on the OPNET website:

www.opnet.com/support

GUI Enhancements

Targeted Operations for Configuring and Running in Automation Mode

Operations have been targeted to meet SP Sentinel's intended purpose of being configured and then run in automation mode. Many new operations have been added to fulfill the intended purpose; a few non-related operations have been removed. Table 11.5-1 lists the operation changes by menu.

Table 11.5-1 Project Editor Operation Changes (Part 1 of 3)

	Operations	
Menus	**Added**	**Removed**
File (See File Menu Operations on page SSU-4-30)	—	—
Edit (See Edit Menu Operations on page SSU-4-33)	—	Select Attached In Subnet Edit Objects Using Template…
View (See View Menu on page SSU-7-16)	—	Background > Set Border Map… Add Image Map… Add MIF Map… Add Image… Map Edit Mode Layout > Scale Node Icons Interactively… Layout Nodes Interactively… Annotations > Show In Subnet

Table 11.5-1 Project Editor Operation Changes (Part 2 of 3)

	Operations	
Menus	**Added**	**Removed**
Scenarios (See Scenarios Menu on page SSU-6-61)	Object/Attribute Difference Report > Generate Report	User-Defined Reports > Open Live Report Table Generate Network Inventory Summary
Topology	Import Topology > Open Import Log Clear Import Log Shared Risk Groups > New Import Export	—
Traffic	Import Traffic Flows > From Spreadsheet Open Import Log Clear Import Log Export Traffic Flows > To Spreadsheet Create Traffic Flows	Modify Traffic Profile Start Times
Protocols	IP > Addressing > Select Node with a Specified IP Address Routing > Enable Reachability Analysis Reachability Analysis Export Routing Tables Demands > Display Routes for Configured Hide Routes Visualize Routability of IP Flows Clear Routability Visualization	—
NetDoctor (See The NetDoctor Menu on page ND-2-2)	—	—

Table 11.5-1 Project Editor Operation Changes (Part 3 of 3)

Menus	Operations	
	Added	**Removed**
Flow Analysis (See The Flow Analysis Menu on page FA-2-2)	Identify Unreachable Interfaces Route Visualization Settings Show Routes Between Selected Nodes Show Multicast Routes from Selected Node Open Route Browser Hide Routes Results > View Statistics Compare Statistics Find Top Statistics View Reports Panels Panel Operations > Arrange Panels > Show All Hide All Distribute Cascade Tile Panel Templates Create From all Panels Load With Latest Results Delete All Panels	—
Windows (See Windows Menu on page SSU-4-38)	—	—
Help (See Help Menu Operations on page SSU-4-39)	—	—
End of Table 11.5-1		

Object Palette Enhancements

The Object Palette has been enhanced to present all available network object models in a tree. You can drag objects directly from the tree view in the same way that you drag objects from the icon view of the Object Palette. However, the Object Palette tree view offers the following additional features:

- View multiple palettes in the same window

- Configure palettes using right-click menu operations
- Display logical groupings of models for quick selection

This tree view is now the default style of the Object Palette. You can switch between the tree view and the icon view. Also, you can make icon view the default style by changing the value of a preference. For details, see network_palette.style on page SSR-3-63 of the *Reference Guide*.

For more information about the Object Palette, see Object Palettes on page SSU-6-8 of the *User Guide*.

Network Browser Enhancements

The Network Browser has been enhanced to expand its ease-of-use. The new features are as follows:

- When you open the Network Browser, your previous option selections are “remembered”. This enhancement allows you to continue using the settings that you previously defined. (Note that search strings and selected objects are not “remembered”.)
- The checkbox options on the Network Browser can be hidden to save space. To display/hide the checkbox options, click the Settings button. By default, the checkbox options are hidden. Additionally, a new checkbox option has been added—Expand Tree. Using this checkbox expands the Network Browser tree to display nodes and links.
- The view filter includes new options that organize networks logically, rather than hierarchically. The following arrangements are available:
  - BGP AS numbers—Arranges nodes by Autonomous System Number.
  - Device types—Arranges nodes by device type.
  - IP subnetworks—Arranges nodes by IP subnetwork.
  - OSPF areas—Arranges nodes by OSPF address.

    When arranged by IP subnetworks or OSPF areas, nodes are identified by IP address, node name, and interface name. When you select a node, all interfaces for that node are selected.
  - Routing protocols—Arranges nodes by routing protocol.
  - Vendor and chassis types—Arranges nodes first by vendor, then by chassis type.
- After importing nodes (for example, device configuration imports (DCI) or VNE Server imports (VNESI)), the Network Browser can be set to open automatically depending on the total number of nodes in the project. Having the Network Browser open after an import can help you find specific nodes,

especially if the network is large. The minimum number of nodes for which to automatically open the Network Browser is specified with a preference. For details about this preference, see show_network_browser_threshold on page SSR-3-71 of the *Reference Guide*.

For more information about the Network Browser, see Network Browser on page SSU-7-9 of the *User Guide*.

Easier Node Model Selection

Editing the “model” attribute of a node is now easier. Previously, when you edited the model attribute of a node, a long list of models appeared. Now, a dialog box similar to the Object Palette treeview appears. By default, the model being edited is selected in the dialog box. The dialog box makes it easier to find and select the model you want. Additionally, you can access model details and create custom models.

Group Nodes into Subnets and Model Assistant Enhancements

The Group Nodes Into Subnets operation has been replaced with a more powerful operation. The new operation includes the following new capabilities:

- Arrange nodes in multi-level subnet hierarchies
- Choose from an expanded list of grouping options, including the ability to group by:
  - AS number
  - OSPF area
  - names (using regular expressions or sub-strings)
- Specify layout and aspect ratio of subnets
- Preview grouping before applying it to your project
- Save the grouping settings to a file and later load the file for re-use
- Apply saved grouping settings to a network using the Model Assistant operation. (This capability is especially useful when a re-imported network includes new nodes.)

For more information, see Grouping Nodes into Subnets on page SSU-6-51 and Model Assistant on page SSU-6-36 of the *User Guide*.

Selecting Objects in a Treeview

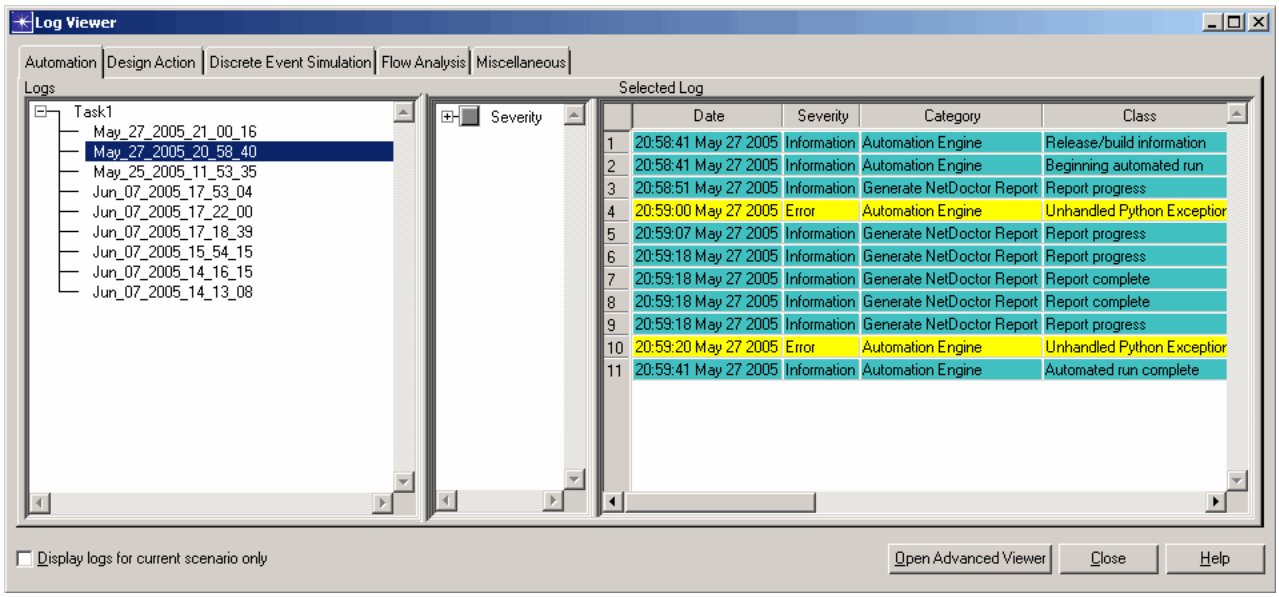
Selecting multiple objects in a treeview has been enhanced to conform to common user interface conventions. To select consecutive objects, click the first object, hold down the Shift key, and then click the last item.

General Enhancements

Log Viewer

A new log viewer provides a central place from which to view SP Sentinel logs. It replaces the individual viewers formerly used for system and error logs, automation logs, import logs, and so on.

Figure 11.5-1 Log Viewer



The new log viewer has a set of tabs that let you select the type of log you want to see. A treeview on the left-hand side of the viewer window lists all available logs of the selected type. You can choose to list all logs or only those for the current scenario in the treeview.

The log viewer can display two kinds of logs:

- Text-based logs. These logs open in a single pane.
- Event-based logs. These logs open in two panes (as shown in Figure 11.5-1). The right-hand pane contains the log data, one event per row. Each row has several columns with different information about the event. Using the filter treeview in the left-hand log pane (in the center of the viewer window), you can restrict the displayed events to only those with specific column values.

You can open the log viewer in three ways:

- From the System window:

  Choose Help > Show All Logs. (All available logs are listed.)

- From a project window:

  Choose Help > Show All Logs. (Only logs for the current scenario are listed.)

- From a specific menu:

  Choose the “show logs” operation from a menu such as Automation or Flow Analysis. (The corresponding tab is preselected and only logs for the current scenario are listed.)

You can open the current log in an advanced log viewer, which provides additional capabilities. With event-based logs, for example, you can:

- Change the way color is used in the log.
- Save the current viewer settings.
- Export the log to a text, comma-separated ASCII, HTML, or XML file.

With text-based logs, the advanced viewer provides all the capabilities of a text-edit pad, including text searches and saving the log to a different file.

License Server Reporting

A new utility lets a license server track license usage statistics and produce statistical reports upon request. When tracking is enabled on the license server, you can generate reports on any client using two new commands in the op_license_util application. Both commands let you specify the number of days on which to report.

- `fldb_stats`—Produces license server statistics, including maximum number of concurrent users, maximum number of concurrent licenses in use, and average number of concurrent licenses in use.
- `license_stats`—Produces license file statistics, including license ID (license number, contract number and program name), total time in use, average checkout time, number of checkouts, number of unique users who accessed the file, and user IDs of those who accessed the file.

The report displays on the screen and a time-stamped `.csv` copy of the file is placed in your `<rel_dir>\op_admin\tmp` directory.

Low Memory Warnings

Sentinel now provides warnings when available RAM is growing short. A warning is triggered when an attempt to allocate memory fails. When this happens, the application frees any unneeded memory and displays a warning.

Preferences

The following preferences have been added:

- flow_spreadsheet_import_filename—Specifies the default file name used when importing spreadsheet traffic.

- flow_spreadsheet_import_overwrite—Specifies the default choice for overwriting traffic when importing spreadsheet traffic.
- network_palette.style—Specifies the default style for the object palette: Tree View or Icon View. The Object Palette Tree View presents network object models in a tree and allows access to multiple palettes simultaneously. The Object Palette Icon View presents network object models with icons and allows access to one palette at a time.
- show_network_browser_threshold—Specifies the minimum number of nodes in a project after an import for which the Network Browser automatically displays.

Topology Import Enhancements

Automated Import of Traffic Flows from Spreadsheet Files

Importing traffic flows from a spreadsheet file can now be automated by creating an automation task. To create an automation task, choose Traffic > Import Traffic Flows > From Spreadsheet… For more information, see Viewing and Editing Traffic Flows in a Spreadsheet on page SSU-8-10 of the *User Guide*.

This enhancement includes the following new spreadsheet import preferences:

- flow_spreadsheet_import_filename—Specifies the default file name used when importing spreadsheet traffic.
- flow_spreadsheet_import_overwrite—Specifies the default choice for overwriting traffic when importing spreadsheet traffic.

VNE Server Import Enhancements

Dual MSFC Support

See Dual MSFCs on page RN-11.5-21 for enhanced support for dual Multilayer Switch Feature Cards (MSFC) on Cisco 6500 multi-layer switches. For more information, see Importing Multi-Layer Switch Configurations on page SSU-10-26 of the Sentinel *User Guide*.

Check Point FireWall-1 Modeling

Check Point FireWall-1 devices can now be imported from VNE Server. Included in this release are the following:

- New device type—“Check Point (Nokia Appliance)”
- Support for Check Point global properties including implied rules, stateful inspection, NAT, and Log and Alert
- Rules in security rule base are mapped to individual access lists in device model

- Support for network address translation (NAT) tables
- Support for automatic ARP configuration in NAT
- Support for bi-directional NAT configuration
- Support for anti-spoofing rules
- Routing configuration for RIP and OSPF are set according to the IPSO configuration for Nokia appliances
- Nokia IPSO access lists are imported as packet filters
- Translation tables support NAT usage in simulations using either Flow Analysis or DES

Nortel Contivity Support

This version includes limited support for Nortel Contivity VPN gateways. Supported features include the following:

- Routing and network addressing
- Branch-office VPN tunnels
- IPSec
- WAN services, including PPP and Frame Relay

Features that are not supported in this release include stateful firewall, QoS, and user tunnels.

Preferences

Three new or modified preferences support VNE Server import:

- vne_import.tunnel_cloud_import
- vne_import.import_voip_configuration
- vne_import.create_serial_cloud

For details, see the descriptions of the similarly named DCI Preferences on page RN-11.5-13.

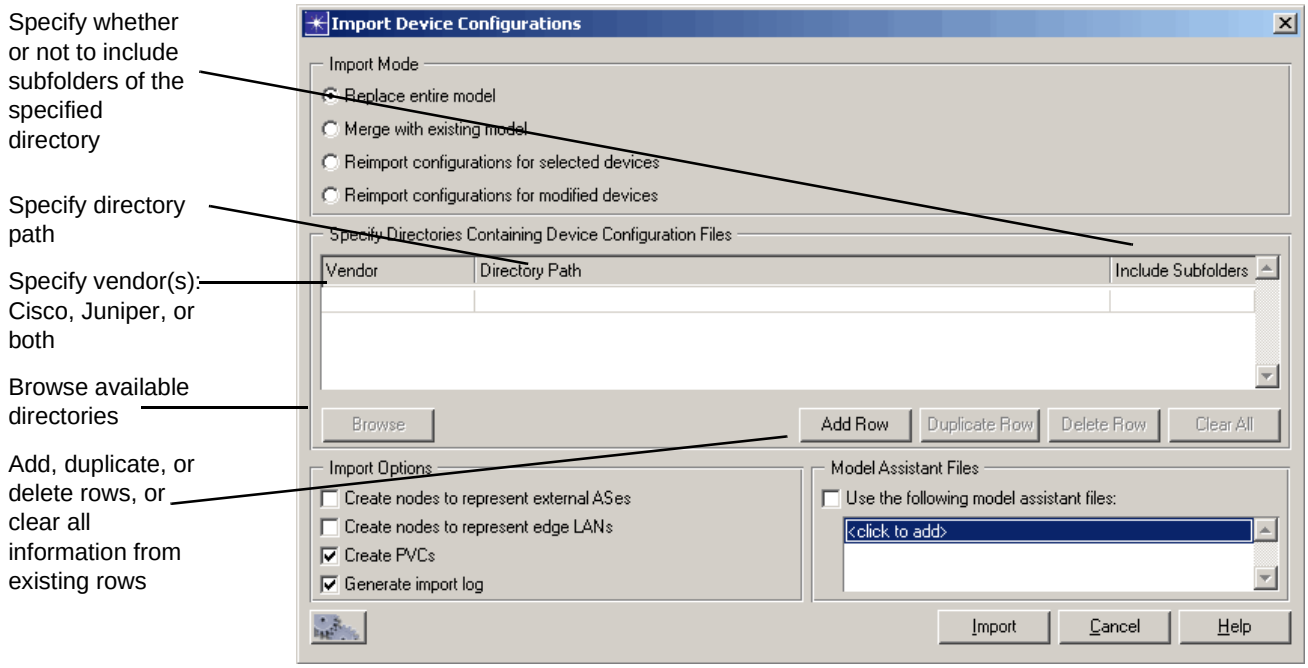
Device Configuration Import Enhancements

Multiple Directory Support

In previous versions of Sentinel, you could specify one configuration file directory per vendor (Cisco or Juniper). All files for a given vendor had to be placed in the specified directory. With this release, you can specify multiple directories per vendor, giving you greater flexibility for import. With the new

dialog box, shown in Figure 11.5-2, you can add, duplicate, or delete rows in the list, or you can clear the information in all rows by using the new buttons provided. A Browse button lets you select your directories from a directory chooser.

Figure 11.5-2 Device Configuration Import Dialog Box



Incremental Device Configuration Import over Import from VNE Server

With this release, you can perform an incremental import of device configuration files to a network model that was originally imported from VNE Server. This gives you the ability to perform “what if” analyses on device configuration files by following this workflow:

1) Import your network from VNE Server and include the device configuration files.

2) Edit the imported device configurations and save them to new files.

3) Import the changed device configuration files using incremental DCI with either the “Reimport configurations for selected devices” or “Reimport configurations for modified devices” option. The attributes for affected devices are reset to default and new attribute values are applied based on information in the configuration files.

Note—During incremental DCI over a model previously imported from VNE Server, no changes affecting topology (such as links and interfaces) are applied. The network preserves the links provided by VNE Server during the initial import.

Enhanced Dual MSFC Support

See Dual MSFCs on page RN-11.5-21 for enhanced support for dual Multilayer Switch Feature Cards (MSFC) on Cisco 6500 multi-layer switches. For more information, see Importing Multi-Layer Switch Configurations on page SSU-10-26 of the Sentinel *User Guide*.

New Supported Show Commands

The following commands are now supported:

- PIX
  - — show version
- Cisco Catalyst Switches
  - — show vlan

Preferences

The following new device configuration import preferences are available.

- device_import.collapse_clouds—Specifies whether or not imported clouds are viewed as a single cloud by collapsing all subnets or as subnet clouds collapsed by protocol. The choices are as follows:
  - — Don’t Collapse—Default behavior that imports clouds with different IP subnets as separate clouds.
  - — Collapse All—Imports all clouds into a single subnet called “Network Cloud”.
  - — Collapse per Protocol—Creates cloud nodes in subnets by protocol. ATM clouds are collapsed into a subnet called “ATM Cloud”. Frame Relay and serial clouds are collapsed into a subnet called “Serial Cloud”.
- device_import.create_serial_cloud—Specifies whether or not to convert a cloud that is a mixture of Frame Relay, ATM, and serial into a serial cloud. Possible selections are as follows:
  - — TRUE: The following mix of interfaces is converted to a serial cloud—ATM + Frame Relay, ATM + Frame Relay + Serial, ATM + Serial, or Frame Relay + Serial.
  - — FALSE: ATM + Frame Relay is imported as a combined FR/ATM switch. Other connectivity is not inferred.
  - — PARTIAL: ATM + Frame Relay + Serial, ATM + Serial, or Frame Relay + Serial are converted to a serial cloud. ATM + Frame Relay is imported as a FR/ATM switch with no conversion necessary.

  If Ethernet interfaces are present, no cloud is inferred.

- device_import.tunnel_cloud_import—Specifies whether or not to infer Layer-3 IP clouds. Possible selections are as follows:
  - TRUE—This is the default value, which will infer Layer-3 IP clouds based on the tunnel interface information in the import file.
  - FALSE—This option will not infer Layer-3 IP Clouds. Tunnel interfaces will not be connected in the network model when there is no information about Layer-2 connectivity between the interfaces.
- device_import.import_voip_configuration—Specifies whether a VoIP device is imported as a multi-service switch or as a router. Possible selections are as follows:
  - ENABLED: (default) If the preference is set to ENABLED, the VoIP device is imported as a multi-services switch. All VoIP configurations are imported, and attributes are set as expected.
  - DISABLED: If the preference is set to DISABLED, the VoIP device is imported as a router. All VoIP configurations are ignored, and a message is created in the import log.

NetDoctor Enhancements

Reporting Enhancements

Device-Centric Reports

This release now supports device-centric reporting for all report types. You have the option to view device-centric information from a tab on a web report or to select and view a device-centric MS Word report (in concise or detailed formats) as an output format. Device-centric reports display the list of rules that are violated for each device. See Table 11.5-2 for a list of the available report types and formats by release.

Table 11.5-2 Available Report Types and Formats

Report Type	Format	Available in Release
Rule-Centric Detailed	MS Word	10.0 or later
	Web	10.0 or later
Rule-Centric Concise	MS Word	New in 11.5
	Web	11.0 or later
Device-Centric Detailed	MS Word	New in 11.5
	Web	New in 11.5
Device-Centric Concise	MS Word	New in 11.5
	Web	New in 11.5
End of Table 11.5-2		

Enhanced Visual Display for Pie Graphs and Bar Charts

NetDoctor supports a new charting package for enhanced visual display for both pie and bar charts.

Internationalization

NetDoctor now supports both Web and MS Word reports in languages other than English. Download the available language libraries from the OPNET Support Center (www.opnet.com/support). Check for the latest versions of the libraries after new releases of the OPNET software. The most up-to-date language libraries might lag the most recent OPNET software release.

Report Comparison

NetDoctor Report Comparison in this release is not valid for reports generated from previous releases. If you enable Report Comparison using a report generated from a previous release, the resulting report shows all rule output as different. Enable Report Comparison only for reports generated by this release.

Notification Plug-ins

This release provides three new notification plug-ins (see Table 11.5-3).

Table 11.5-3 Available Notification Plug-ins

Notification Plug-in	Available in Release
Email (SMTP)	10.5 or later
SNMP Trap	New in 11.5
Syslog	New in 11.5
Trouble Ticket (Remedy)	New in 11.5
End of Table 11.5-3	

If you want NetDoctor to send other types of notifications, you can write your own plug-in using the open notification architecture. Notification settings appear on the Notification tab in the Configure/Run NetDoctor dialog box.

This release has a new advanced checkbox in the Notification tab of the Configure/Run dialog box. When you select this checkbox, additional parameters are available to edit.

NetDoctor Rules

Device Configuration File Validation Rules

Device configuration file validation rules now support matching commands in specific sections of configuration files. For example, you can now specify match or no match commands for specific types of interfaces in your network.

Rule Removed

The Organizational Policies: Missing Prefix Filters rule has been removed. If you are currently using this rule, please contact OPNET Technical Support (e-mail support@opnet.com) for more information.

Customizing NetDoctor

Charting

NetDoctor supports a new charting package with enhanced visual display for both bar graphs and pie charts. NetDoctor utility functions for creating bar graphs and pie charts have been updated to use the new package.

API Enhancements

This release supports the following new functions and methods:

- *Ip.default_redist_metric_exists()*
- *Ip.get_default_redist_metric()*
- *Node.get_machine_type()*
- *Node.vendor_model()*

The API documentation has been reorganized into four general categories: Model Access, IP Graph, Reporting, and Simulation.

Network Difference Report Enhancements

SP Sentinel includes a new Network Difference Report. Use the new network difference report to identify real-world network differences between two network scenarios, such as network protocol and device configuration. Network difference reports are useful when you want to know exactly how a network has evolved from one scenario to the next or how networks imported from different sources vary. Specifically, the new network difference report identifies the following:

- Device configuration settings for routers, switches, and firewalls
- Logical groups, such as BGP Autonomous System, EIGRP Autonomous Systems, and OSPF Areas

You can access the new network difference report by choosing Scenarios > Network Difference Report. The previously available network difference report has been renamed “Object/Attribute Difference Report” and is available from the Scenarios menu.

Don’t confuse the Network Difference Report and the Object/Attribute Difference Report.

- A Network Difference Report identifies only those differences that are likely to affect network behavior, such as differences in network topology and device configurations.
- An Object/Attribute Difference Report identifies all differences in objects and attributes, regardless of whether those differences affect network behavior.

Note—Any 11.0 or earlier automation files created for the Network Difference Report (renamed Object/Attribute Difference Report in 11.5) will still work as expected. In 11.5, the graphical interface will display the old files under the new name. However, to avoid confusion, the label in the task scheduler dialog box has been changed. Older network difference automation files are converted to the new format automatically and are labeled Generate Object/Attribute Difference Report. (Previously, these were labeled Generate Network Difference Report.)

Note—With Report Server 2.0 and earlier, Object/Attribute Difference reports will be listed only under the product-specific folder. On the Report Server web page, click on View by Products and then the product name.

For more information about the new network difference report, see Network Difference Reports on page SSU-11-5 of the *User Guide*.

For more information about the Object/Attribute Difference Report (formerly the Network Difference Report operation), see Object/Attribute Difference Reports on page SSU-11-7 of the *User Guide*.

Flow Analysis Enhancements

Standard and Specialized Model Suites

The Flow Analysis module has been enhanced to support new features in the following model suites. Details can be found in the DES Model Library Enhancements section of this document.

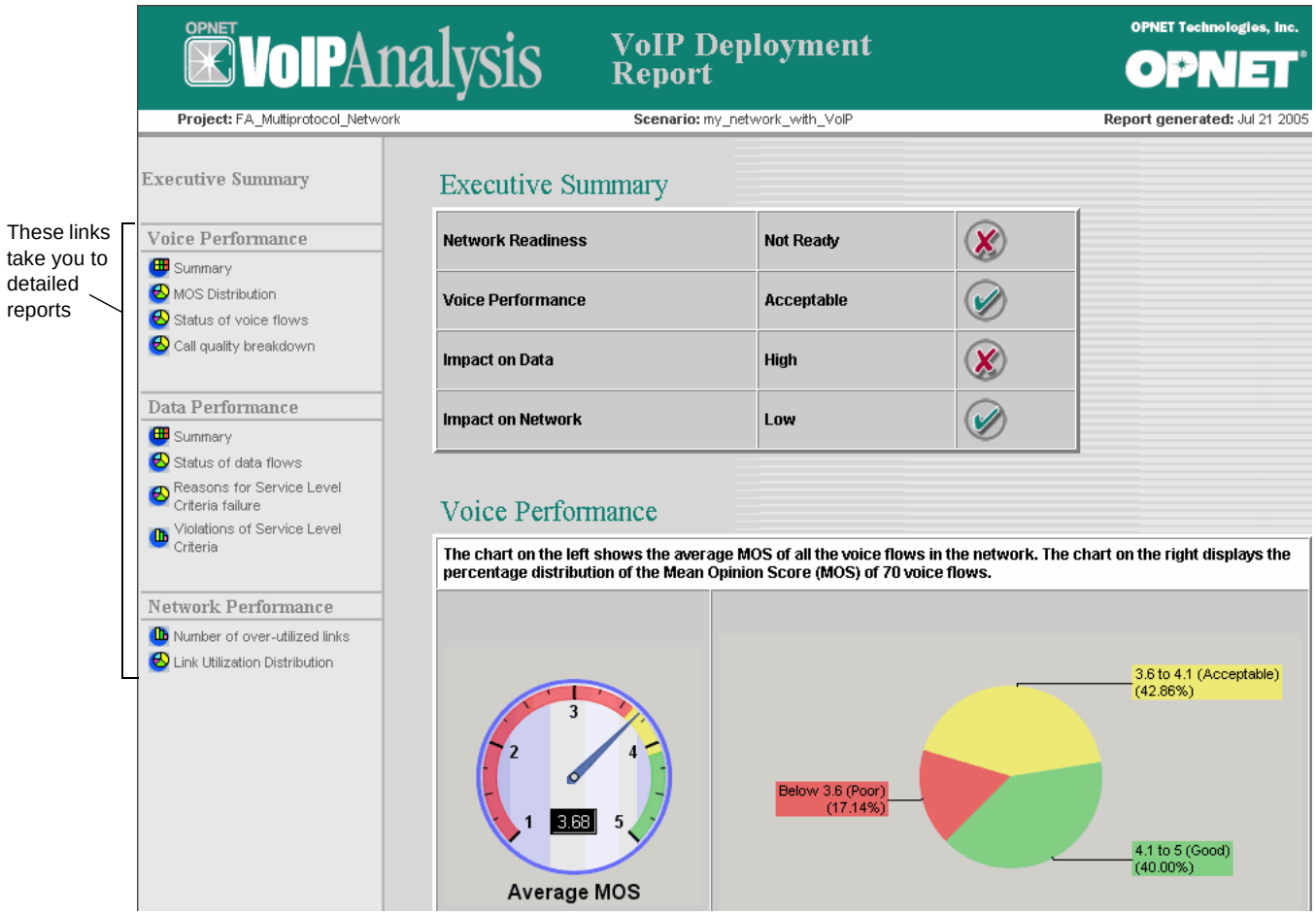
- ATM Enhancements on page RN-11.5-21
- Dual MSFCs on page RN-11.5-21

VoIP Readiness Assessment

The Flow Analysis module now includes a utility that lets you analyze the impact of voice over IP (VoIP) traffic on an existing network.

The VoIP Readiness Assessment workflow uses an easy-to-use interface that guides you through the set up and configuration of VoIP traffic in a network. You can deploy new (proposed) flows or analyze only the existing VoIP flows in the network. The assessment uses several iterations of flow analysis and one or more design actions to generate a comprehensive web report on the network's readiness for VoIP traffic deployment.

Figure 11.5-3 Web Report VoIP Readiness Assessment



In addition to the web report, you can also view the results of the flow analysis and design action runs.

For additional information, see Chapter 5 Using VoIP Readiness Assessment on page FA-5-1 of the *Flow Analysis User Guide*.

Model Library Behavior Changes

Default Metrics for Redistribution

Most imported and manually created projects will generate different results because of new values for the default metrics used for redistribution. For example, flows that were routable in previous releases might no longer be routable.

Unless metrics have been explicitly defined in the device configuration files for imported devices or manually in the Redistribution attribute, the following metrics are used for redistribution. In Table 11.5-5, “None” indicates that redistribution does not occur—even if redistribution is enabled.

Table 11.5-4 Default Redistribution Metrics for all Routers (Except Juniper)

	Redistribution Into				
	BGP	**EIGRP/IGRP**	**ISIS**	**OSPF**	**RIP**
BGP	n/a	none	0	1	none
EIGRP/IGRP	same as RP [1]	native metric	0	20	none
ISIS	same as RP[y[tblFootnote]>	none	same as RP[y[tblFootnote]>	20	none
OSPF	same as RP[y[tblFootnote]>	none	0	same as RP[y[tblFootnote]>	none
RIP	same as RP[y[tblFootnote]>	none	0	20	same as RP[y[tblFootnote]>
Connected	0	formula [2]	0	20	0
Static	0	256/1	0	20	0
End of Table 11.5-4					

1. Same as redistributed protocol.

2. There is a factor of 256 between IGRP and EIGRP in the composite metric computation.

Table 11.5-5 Default Redistribution Metrics for Juniper Models (Part 1 of 2)

	Redistribution Into				
	BGP	**EIGRP IGRP**	**ISIS**	**OSPF**	**RIP**
BGP	n/a	n/a	10	same as RP [1]	1
EIGRP/IGRP	n/a	n/a	n/a	n/a	n/a
ISIS	same as IGP [2]	n/a	same as RP[y[tblFootnote]>	same as RP[y[tblFootnote]>	1

Table 11.5-5 Default Redistribution Metrics for Juniper Models (Part 2 of 2)

	Redistribution Into				
	BGP	**EIGRP IGRP**	**ISIS**	**OSPF**	**RIP**
OSPF	same as IGP[y[tblFootnote]>	n/a	same as RP [3]	same as RP[y[tblFootnote] >	1
RIP	same as IGP[y[tblFootnote]>	n/a	same as RP[y[tblFootnote] >	same as RP[y[tblFootnote] >	same as RP[y[tblFootnote] >
Connected	0	n/a	10	0	1
Static	0	n/a	10	0	1
End of Table 11.5-5					

1. Same as redistributed protocol.

2. Same as IGP route metric.

3. Same as redistributed protocol (max 63)

Default Interface Information for Cisco Routers

The following parameters (bandwidth, delay, MTU, reliability, load) are used to compute the default metric when redistributing directly connected interfaces into EIGRP/IGRP. Bandwidth and delay are dependant on the interface type.

Table 11.5-6 Default Values for Calculating Redistribution Into EIGRP/IGRP

	Bandwidth (Mbps)	**Delay (µsec)**	**MTU (bytes)**	**Reliability**	**Load**
Eth/Fasteth/Giga	10/100/1,000	1,000/100/10	1,500	255	255
FDDI	100	100	4,470	255	255
Token Ring	4/16	100	4,464	255	255
ATM	25	80	4,470	255	255
FR	1.544	20,000	1,500	255	255
IP	1.544	20,000	1,500	255	255
Loopback	8,000	5,000	1,514	255	255
Tunnel	0.9	500,000	1,514	255	255
VLAN	10	1000	1,500	255	255
End of Table 11.5-6					

Model Assistant File Conversion

If you have a model assistant file containing networks imported through device configuration import (DCI) from previous versions of Logger, you must convert your file prior to using it in 11.5. A new conversion utility, **op_ma_conv**, is included in 11.5. The following flags are available to convert individual files, a list of files, or all files:

Table 11.5-7 Flags for op_ma_conv Utility

Flag	Usage
`-all`	(default) Converts all model assistant files in the model directory. If no flag is provided, the utility converts all files.
`-m <model name>, <model name>, ...`	Provide individual filename or a list of filenames separated by commas. Enter the filename without the .ma extension.
End of Table 11.5-7	

WARNING—If you do not convert your pre-11.5 model assistant files containing networks imported through DCI, they will not work in 11.5.

Model Library Enhancements

ATM Enhancements

The ATM model suite now includes the following features for flow analysis (no change to supported features for discrete event simulation).

- Slot-port support
- Per-class load balancing for Nortel devices
- New reports on delays for PVCs

Dual MSFCs

Support for Cisco Catalyst 6500 multi-layer switches with dual Multilayer Switch Feature Cards (MSFCs) is enhanced for device configuration import (DCI), Virtual Network Environment (VNE) Server, discrete event simulation (DES), and flow analysis.

Two new “show” commands are supported that allow you to model dual MSFCs:

- show module
- show redundancy

Redundancy information and configuration attributes of the non-designated MSFC in the dual configuration are now stored in the new MSFC compound attribute.

DES and Flow Analysis

DES and flow analysis support dual MSFCs with the following requirements:

- "config-sync" is enabled.
- MSFC failover in the network model is not supported; both MSFCs are assumed to be up or both MSFCs are down.
- Routing simulates a network that has either both MSFCs running (with no failover) or both MSFCs down (device failure).

IP routing:

- Both MSFCs can serve as sources/destinations to simulate the following:
  - ICMP (ping)
  - IP traffic flows

For HSRP:

- One HSRP process runs on the device using the MSFC with the higher interface priority.
- HSRP uses the preemption status and delay of the MSFC with the higher interface priority (DES only).
- The HSRP traffic sent from the dual MSFC is half the traffic seen in the live network (DES only).

For BGP:

- There is one incoming and one outgoing BGP connection on the designated MSFC for each BGP neighbor.
- No BGP process runs on the non-designated MSFC.
- The BGP control traffic is less than the traffic seen in the live network (DES only).
- The simulation uses the policies configured on the designated MSFC for both BGP neighbors.