NETWARS

Traffic Modeling and Importing Traffic 2005-1 Final User's Guide (OPNET 235)

Contract DASW01 03 D 0008



September 2, 2005

Prepared for: Defense Contracting Command -Washington Washington, DC 50310-5200 Prepared by: OPNET Technologies, Inc. 7255 Woodmont Avenue Bethesda, MD 20814-7904



Identification

Document Identification

Document Title: Traffic Modeling and Importing Traffic Version: Final (OPNET 235)

Software Identification

Product Name: NETWARS Product Release: 5.1

Documentation Conventions

This documentation uses specific formatting and typographic conventions to present the following types of information:

- Objects, examples, and system I/O
- Object hierarchies
- Computer commands
- · Lists and procedures

Objects, Examples, and System I/O

• Directory paths and file names are in standard Courier typeface:

C:\Netwars\User_Data\Projects

• Function names in body text are in italics:

op_dist_outcome()

• The names of functions of interest in example code are in bolded Courier typeface:

/* determine the object ID of packet's creation module */
src_mod_objid = op_pk_creation_mod_get (pkptr);

• Variables are enclosed in angle brackets (< >):

<NETWARS path>\Scenario_Builder\op_admin\err_log

Object Hierarchies

Menu hierarchies are indicated by right angle brackets (>); for example: Edit > Preferences > Advanced

Computer Commands

These conventions apply to Windows systems and navigation methods that use the standard graphical-user-interface (GUI) terminology such as click, drag, and dialog box.

• Key combinations appear in the form "press **<button>+x**"; this means press the **<button>** and **x** keys *at the same time* to do the operation.

• The mouse operations *left-click* (or *click*) and *right-click* indicate that you should press the left mouse button or right mouse button, respectively.

Lists and Procedures

Information is often itemized in bulleted (unordered) or numbered (ordered) lists:

- In bulleted lists, the sequence of items is not important.
- In numbered lists, the sequence of items is important.

Procedures are contained within procedure headings and footings that indicate the start and end of the procedure. Each step of a procedure is numbered to indicate the sequence in which you should do the steps.

Document Revision History

Release Date	Product Version	Chapter	Description of Change
September 2, 2005	5.1 Final	3 & 4	Changed file name paths from C:\op_models\ to C:\Netwars\
			Verified that NetDoctor and Virtual CLI are available in NETWARS if you have the appropriate license.
June 22, 2005	5.1 Draft	All	Preliminary version.

Contents

	Identification	UG3-FM-iii
	Documentation Conventions	UG3-FM-iii
	Document Revision History	UG3-FM-v
	List of Figures	UG3-FM-ix
	List of Procedures	UG3-FM-xiii
1	Introduction	UG3-1-1
	NETWARS Overview	UG3-1-1
		UG3-1-1
		UG3-1-1
		UG3-1-2
	Traffic Types	UG3-1-2
	Sources of Explicit Traffic	UG3-1-2
	Sources of Aggregated Traffic	UG3-1-2
		UG3-1-3
	Simulation Techniques	UG3-1-3
		UG3-1-4
	Discrete Event Simulation	UG3-1-4
	Hybrid Simulation	UG3-1-4
	Importing Traffic	UG3-1-5
	Importing IP and Layer 2 Networks with MVI	UG3-1-5
	Importing Network Traffic Data with MVI	UG3-1-5
2	Traffic Modeling Techniques	UG3-2-1
	Comparing Traffic Modeling Approaches	UG3-2-1
	Simulation with Explicit Traffic	UG3-2-2
	Simulation with Background Traffic	UG3-2-10
	Simulation with Hybrid Traffic	UG3-2-13
	Conclusion	UG3-2-16
	Using Hybrid Simulation to Model New Application Performance	UG3-2-16
	Implementing QoS in the Network and Prioritizing Application Traffic	UG3-2-31
3	Importing IP and Layer 2 Networks with MVI	UG3-3-1
	Introduction	UG3-3-1
	Import an Example Network	UG3-3-1
	Exploring the OPNET Network Model	UG3-3-3
	Conclusions	UG3-3-12
	Using the Model Assistant	UG3-3-12
	Apply the Model Assistant File after the Import	UG3-3-20
	Conclusions	UG3-3-21
	Incremental Import: Selected Devices Re-import	UG3-3-22
	Incremental Import: Selected Devices Re-import Find Configuration Errors	UG3-3-22 UG3-3-22

Conclusions	UG3-3-29
Troubleshooting the Imported Network	UG3-3-29
Find Configuration Errors	UG3-3-29
Conclusions	UG3-3-34

4 Importing Network Traffic Data with MVI	UG3-4-1
Importing Network Traffic Data with MVI	UG3-4-1
Introduction	UG3-4-1
Examining Loads and Flows	UG3-4-1
Importing Link Loads	UG3-4-8
Summary	UG3-4-13
Importing Traffic Flows and Running Flow Analysis	UG3-4-14
Summary	UG3-4-23

List of Figures

Figure 2-1	Example Network Model	UG3-2-1
Figure 2-2	Demands Object Palette	UG3-2-2
Figure 2-3	IP Demand Connected	UG3-2-3
Figure 2-4	Selected Object's Attributes dialog box	UG3-2-3
Figure 2-5	Configuring the Traffic (bits/second) Attribute	UG3-2-4
Figure 2-6	Configuring the Traffic (packets/second) Attribute	UG3-2-4
Figure 2-7	Copying/Pasting Demand Objects	UG3-2-5
Figure 2-8	IP Traffic Flow Characterization dialog box	UG3-2-5
Figure 2-9	Node's Attributes dialog box	UG3-2-6
Figure 2-10	Selecting the Packet ETE Delay (sec) Statistic	UG3-2-6
Figure 2-11	Selecting the IP Interface / Queuing Delay (sec) Statistic	UG3-2-7
Figure 2-12	Simulation Sequence dialog box	UG3-2-7
Figure 2-13	Selecting Throughput Statistics to Show	UG3-2-8
Figure 2-14	Throughput Results Graph	UG3-2-8
Figure 2-15	View Results dialog box	UG3-2-9
Figure 2-16	Showing Queuing Delay Results	UG3-2-9
Figure 2-17	Showing the Packet ETE Delay (sec) Statistic Graph	UG3-2-10
Figure 2-18	Changing the Traffic Mix Attribute	UG3-2-11
Figure 2-19	Showing Queuing Delays Graph	UG3-2-12
Figure 2-20	Comparing Queuing Delays	UG3-2-12
Figure 2-21	Inaccessible Packet ETE Delay (sec) Statistic	UG3-2-13
Figure 2-22	Changing the Traffic Mix Attribute	UG3-2-14
Figure 2-23	Comparing Queuing Delays	UG3-2-15
Figure 2-24	Comparing Packet ETE Delay (sec) Statistics	UG3-2-15
Figure 2-25	Treeview window	UG3-2-17
Figure 2-26	Data Exchange Chart	UG3-2-17
Figure 2-27	Displaying app user only	UG3-2-18
Figure 2-28	Configure ACE Application dialog box	UG3-2-19
Figure 2-29	Deploy Tiers dialog box	UG3-2-19
Figure 2-30	Configure Nodes with Selected Tier dialog box	UG3-2-20
Figure 2-31	Selecting the Task Response Time (sec) Statistic	UG3-2-21
Figure 2-32	Task Response Time Statistics	UG3-2-21
Figure 2-33	View Results dialog box	UG3-2-22
Figure 2-34	Average Task Response Time Statistics	UG3-2-22
Figure 2-35	Link Attributes dialog box	UG3-2-23
Figure 2-36	Background Load Attributes dialog box	UG3-2-23
Figure 2-37	Profile dialog box	UG3-2-24
Figure 2-38	View Results dialog box	UG3-2-25
Figure 2-39	Task Response Time Statistics	UG3-2-25
Figure 2-40	ACE Traffic Import: Specify Tasks dialog box	UG3-2-26
Figure 2-41	ACE Traffic Import: Assign Nodes dialog box	UG3-2-26
Figure 2-42	ACE Traffic Import: Configure Initiating Node dialog box	UG3-2-27
Figure 2-43	Node Assignments (web client) List	UG3-2-27
Figure 2-44	Node Assignments (web server) List	UG3-2-28
Figure 2-45	Node Assignments (database_server) List	UG3-2-28

Figure 2-46	Network Traffic Demands	1163-2-28
Figure 2-47	Task Besnonse Time Statistics	1163-2-29
Figure 2-47	Select Statistic for Ton Besults dialog hox	LIG3-2-29
Figure 2-49	Ton Objects Point-to-Point I litilization dialog box	LIG3-2-30
Figure 2-50	Oos Configuration dialog box	LIG3-2-31
Figure 2-51	Attributes dialog box	LIG3-2-32
Figure 2-52	Annie Config Attributes dialog box	LIG3-2-32
Figure 2-52	Applic Coming Attributes dialog box	
Figure 2-54		LIG3-2-33
Figure 2-54		
Figure 2-56		LIG3-2-34
Figure 3-1		LIG3-3-2
Figure 3-2	Sample Network	LIG3-3-3
Figure 3-3		LIG3-3-4
Figure 3-4		LIG3-3-4
Figure 3-5	Notwork Browsor	LIG3-3-5
Figure 2-6		
Figure 2-7	Attributes dialog box	
Figure 2-7		
Figure 3-0		
Figure 3-9	Attributes dialog box	
Figure 3-10	Aundules dialog box	
Figure 3-11		
Figure 3-12	Subinternace information Attribute	0G3-3-9
Figure 3-13	Log Browser Showing Skipped Commands for Albany	0G3-3-10
Figure 3-14	Log Browser Showing Skipped Commands for FasiEtherneto/0	0G3-3-10
Figure 3-15		0G3-3-11
Figure 3-16		0G3-3-11
Figure 3-17		0G3-3-13
Figure 3-18		UG3-3-14
Figure 3-19		UG3-3-14
Figure 3-20		UG3-3-15
Figure 3-21		UG3-3-15
Figure 3-22		UG3-3-16
Figure 3-23	Import Assistant with at-0/1/0 Selected	UG3-3-17
Figure 3-24		UG3-3-18
Figure 3-25		UG3-3-19
Figure 3-26		UG3-3-19
Figure 3-27		UG3-3-20
Figure 3-28		UG3-3-21
Figure 3-29		UG3-3-23
Figure 3-30	NetDoctor Report's Rules Section	UG3-3-23
Figure 3-31		UG3-3-24
Figure 3-32		UG3-3-24
Figure 3-33	Nodes with Duplicate IP Addresses	UG3-3-25
Figure 3-34	Device Configuration Source Data	UG3-3-25
Figure 3-35	Import Device Configuration dialog box	UG3-3-26
Figure 3-36	Virtual Command Line interface	UG3-3-27

Figure 3-37	Virtual Command Line interface	UG3-3-28
Figure 3-38	Import Summary (Concise) dialog box	UG3-3-30
Figure 3-39	Sample Network	UG3-3-31
Figure 3-40	Attributes dialog box	UG3-3-31
Figure 3-41	Sample Network Topology Diagram	UG3-3-32
Figure 3-42	Sample Network	UG3-3-34
Figure 4-1	Sample Network	UG3-4-2
Figure 4-2	Profile Editor for Atlanta-pixfirewall	UG3-4-3
Figure 4-3	Color Links by Load dialog box	UG3-4-3
Figure 4-4	Sample Network with Colored Links	UG3-4-4
Figure 4-5	Sample Network with Hidden Flows	UG3-4-5
Figure 4-6	Profile Editor for Boston_Bkup_IDC-DC	UG3-4-5
Figure 4-7	Sample Network Showing All Demands and Flows	UG3-4-6
Figure 4-8	Profile Editor for Core (172_20_1_5)>DC (192_168_50_10)	UG3-4-6
Figure 4-9	Profile Editor for Core (172_20_1_5)>DC (192_168_50_10)	UG3-4-7
Figure 4-10	Sample Network in Flows Browser	UG3-4-7
Figure 4-11	Sample Network in Flows Browser	UG3-4-8
Figure 4-12	Sample Network	UG3-4-9
Figure 4-13	Import Link Baseline Loads from InfoVista Reports dialog box	UG3-4-10
Figure 4-14	Traffic Load Summary dialog box	UG3-4-10
Figure 4-15	Sample Network with Colored Links	UG3-4-11
Figure 4-16	Background Load Attribute	UG3-4-12
Figure 4-17	Profile Editor for Atlanta-Access-192_168_50_64/29	UG3-4-12
Figure 4-18	Edit Attributes dialog box	UG3-4-13
Figure 4-19	Node A Interface Aliases	UG3-4-13
Figure 4-20	Sample Network	UG3-4-15
Figure 4-21	Sample Network with Colored Links	UG3-4-16
Figure 4-22	Edit Attributes dialog box	UG3-4-16
Figure 4-23	Profile Editor for layer2_switch_32-NY_Pri_IDC	UG3-4-17
Figure 4-24	Traffic Flows Import	UG3-4-18
Figure 4-25	Traffic Flow Import Statistics	UG3-4-18
Figure 4-26	Sample Network with Traffic Flow Demands	UG3-4-19
Figure 4-27	Sample Network in Flows Browser	UG3-4-20
Figure 4-28	Sample Network in Flows Browser	UG3-4-21
Figure 4-29	Sample Network in Flows Browser	UG3-4-21
Figure 4-30	Find Top Statistics	UG3-4-23

List of Procedures

Procedure 2-1	Create a Simple Network with Explicit TrafficUG3-2-2
Procedure 2-2	Configure Demands with Background TrafficUG3-2-10
Procedure 2-3	Configure Demands with Hybrid TrafficUG3-2-13
Procedure 2-4	Use Hybrid Simulation to Model Application PerformanceUG3-2-16
Procedure 2-5	Implement QoS in the Network and Prioritize TrafficUG3-2-31
Procedure 3-1	Import Device Configuration FilesUG3-3-1
Procedure 3-2	Explore the OPNET Network ModelUG3-3-3
Procedure 3-3	View Skipped CommandsUG3-3-10
Procedure 3-4	Visualize the Network ModelUG3-3-11
Procedure 3-5	Import the Configuration FilesUG3-3-12
Procedure 3-6	Use Import Assistant to Connect Interfaces and Specify Data RatesUG3-3-14
Procedure 3-7	Apply Model Assistant File to Move Nodes from Logical to Geographic Positions UG3-3-18
Procedure 3-8	Export Site Locations and Hierarchy for Re-use in Future ImportsUG3-3-18
Procedure 3-9	Apply the Model Assistant File after the ImportUG3-3-20
Procedure 3-10	Find Configuration ErrorsUG3-3-22
Procedure 3-11	Clear Configuration ErrorsUG3-3-24
Procedure 3-12	Re-import Modified Configuration FilesUG3-3-25
Procedure 3-13	Verify that Configuration Errors are ClearedUG3-3-26
Procedure 3-14	Use Virtual CLIUG3-3-27
Procedure 3-15	Verify that Warnings are ClearedUG3-3-28
Procedure 3-16	Find Configuration ErrorsUG3-3-29
Procedure 3-17	Providing the Missing InformationUG3-3-33
Procedure 4-1	Examine Loads and FlowsUG3-4-2
Procedure 4-2	Import Link LoadsUG3-4-8
Procedure 4-3	Visualize and Inspect Link LoadsUG3-4-14
Procedure 4-4	Import Traffic FlowsUG3-4-17
Procedure 4-5	View Flows Using the Flows BrowserUG3-4-19
Procedure 4-6	Run DESUG3-4-22
Procedure 4-7	Find the Over-Utilized LinkUG3-4-22

NETWARS Overview

The Command, Control, Communications, and Computer Systems Directorate of the Joint Staff, in partnership with the Defense Information Systems Agency, Directorate for Technical Integration Services, developed Network Warfare Simulation (NETWARS). NETWARS provides modeling and simulation (M&S) capabilities for measuring and assessing information flow through strategic, operational, and tactical military communications networks. Analyzing the results from NETWARS can provide considerable utility in determining which communication systems might be overloaded during selected times in a particular scenario, and can assist with making prudent acquisition planning decisions.

Document Overview

NETWARS provides several options for representing, generating, and simulating traffic. Understanding the available options and selecting the appropriate traffic modeling technique is crucial to simulation performance. This user's guide, *Traffic Modeling and Importing Traffic*, describes how you can tune the fidelity of traffic being modeled using different traffic representations. How you choose to model traffic depends on the type of study being done.

This guide also provides example scenarios to show you how to import network traffic using the Multi-Vendor Import (MVI) module, which extends the built-in traffic and topology import features of NETWARS.

Note—For additional information about MVI, refer to the MVI User Guide (packaged with the IT Guru product documentation) available in NETWARS via the System Editor or Scenario Builder's **Help** menu.

Referenced Documents

• MVI User Guide, OPNET Technologies.

Traffic Modeling Techniques

This section presents guidelines for selecting the appropriate traffic modeling method given the type of study you are doing.

The following topics are covered:

- Traffic types in NETWARS: Explicit (packet-by-packet) traffic, and aggregated traffic, and
- Simulation techniques in NETWARS: Analytical simulation, discrete event simulation, and hybrid simulation.

Refer to chapter 2 in this guide for example scenarios that compare different traffic modeling approaches.

Traffic Types

There are several types of traffic (WAN, LAN, application traffic) represented in NETWARS. Your choice of representation depends on your modeling purpose (see Table 1-1 below.)

	e Typee
Traffic Type	NETWARS Representation

Traffic Types

Traffic Type	NETWARS Representation	Modeling Purpose
Packet-by-Packet	Explicit Traffic	End-to-end delays, protocol details, segmentation effects
Aggregated Traffic	Traffic Flows (routed background traffic), Device/Link Loads (static background traffic)	Capacity planning, steady-state routing analysis

Sources of Explicit Traffic

Table 1-1

Explicit traffic injected at the application layer includes email, HTTP, FTP, etc., and ACE, app demands. Explicit traffic at the network layer includes IP traffic flows and RPG (self-similar traffic generator.) Explicit traffic at the lower layers includes native protocol sources (Ethernet, ATM, Frame Relay, etc.)

Sources of Aggregated Traffic

One type of aggregated traffic is traffic flows (or routed background traffic.) Traffic flows are injected at the application layer as app demands. Aggregated traffic at the network layer are IP traffic flows. Aggregated traffic at the lower layers include ATM traffic flows and ATM PVC loads. Traffic flows need to be propagated (via tracer packets) to each node in the flow path.

The second type of aggregated traffic is element loads (or static background traffic.) Element loads include CPU utilization, and link loads. They do not require source models.

Traffic Data Import

Network monitoring software samples traffic periodically using probes, and exports the data to text files or other NETWARS recognizable formats for importing into NETWARS.

You can import explicit traffic using packet traces captured using a network analyzer such as Sniffer analyzer, tcpdump, windump, or the Application Characterization Editor (ACE).

You can import aggregated traffic using link load information from Concord NetworkHealth, MRTG, or spreadsheets (text info), etc. that can be converted into traffic flows.

Simulation Techniques

The following list (and Table 1-2) provide a brief comparison of the various NETWARS traffic modeling approaches:

- Analytical simulation
 - Abstract queue performance using mathematical equations
 - Model traffic as state information in various network elements
- Discrete event simulation
 - Model all traffic (data, signaling, management) using packets
 - Account for all timers in every protocol layer
 - Perform every state/event transitions of all protocol layers

- · Hybrid simulation
 - Mix of modeling approaches (discrete event + analytical)
 - Mixture of traffic types (explicit traffic + aggregated traffic)

Table 1-2	Comparison of Simulation Techniques
-----------	-------------------------------------

	Analytical	Discrete	Hybrid
Capabilities	Capacity Planning	Protocol Dynamics	All from Discrete and Analytical
	Device and Link Load Measurement	Packet-by-packet Analysis for New Application Development	
		End-to-end Traffic Analysis	
		Capacity Planning	
		Device and Link Load Measurement	
Methods	Mathematical	Event-based Simulation Kernel	Micro-Simulation
	Equations to Compute Performance Metrics		Analytical Simulation
	Tabular Data Constructed from Empirical Data		

Analytical Simulation

Analytical simulation uses traffic flow and static device load information for its traffic input. The advantage of using analytical simulation is its fast numerical computations. Its disadvantages are in its assumptions, leading to inaccuracies, and the fact that it's not available for all systems.

Discrete Event Simulation

Discrete event simulation uses explicit traffic generator models and ACE for its traffic input. The advantage of using discrete event simulation is its accuracy and high fidelity. Its disadvantages are in its long simulation run-time and large memory requirements.

Hybrid Simulation

Hybrid simulation uses both or one of the traffic inputs used by discrete and analytical simulation techniques. The advantage of using hybrid simulation is that it is more accurate than analytical simulation and faster than discrete simulation. Its disadvantage is that it does not model all protocol dynamics such as feedback, flow control, congestion control, and policing.

Importing Traffic

Importing IP and Layer 2 Networks with MVI

The Multi Vendor Import module (MVI) allows you to import network topology using device configuration files. Chapter 3 provides example scenarios to show you how to:

- Use MVI to build a network model by importing from device configuration files,
- Use the Model Assistant to provide supplemental information such as interface data rates and device locations that do not exist in the device configuration files, and
- Evaluate the status of the configuration import, and use the information to troubleshoot the network.

Importing Network Traffic Data with MVI

The MVI module can also be used to leverage real-world traffic data and build accurate and efficient models by importing time-varying link and PVC load data as well as end-to-end flow data from various data sources. Chapter 4 provides example scenarios to show you how to:

- Perform traffic flow and link/pvc baseline load imports, and
- Learn about the workflow options available when performing network analyses using data from various sources.

2 Traffic Modeling Techniques

Comparing Traffic Modeling Approaches

In this section, we compare the speed and accuracy of different traffic representations: explicit traffic, background traffic and hybrid traffic. First we create a simple network with explicit traffic, then we replace the explicit traffic with background traffic, and finally we replace the background traffic with hybrid traffic, running simulations each time. In doing so, we can predict the delay for each class of service and compare the results obtained using the different traffic modeling approaches.

Note—The following example was presented at OPNETWORK 2004 in Session 1302, Traffic Modeling Techniques, as Lab 1. If you do not have access to the files that this procedure uses, you can still follow the procedure using the sample screens provided in this user's guide.

This section uses the following example scenario:

 The network is a model of a company that provides video-on-demand services to 100 users. The company would like to introduce three classes of service for its clients: Gold (ToS = 3), Silver (ToS = 2) and Bronze (ToS = 1). To provide differentiated treatment for the different service classes, Weighted Fair Queuing (WFQ) has been configured on the access router.



Figure 2-1 Example Network Model

Note—Source nodes (video servers) with different ToS (1,2,3) are shown on the left-hand side of the Network Model figure; destination nodes on the right. Router B provide the interface with WFQ.

Simulation with Explicit Traffic

Procedure 2-1 Create a Simple Network with Explicit Traffic

- 1 Open the project.
 - 1.1 Launch NETWARS, if not already opened.
 - **1.2** From the System Editor's File menu, choose Open Editor.
 - **1.3** From the Open Editor drop-down menu, select **Scenario Builder**, and then click **OK**. The Scenario Builder window displays.
 - 1.4 Select File > Open Project. The Open Project dialog box displays.
 - **1.5** Select the project named 1302_lab1 (or if you want to follow along without actually performing the steps in this procedure, select the project named 1302_lab1_ref instead), and then click Open.

Scenario "Explicit_traffic" appears as the first scenario.

Note—If you do not have access to these files, simply view the screens provided in this user's guide to follow along with the procedure.

2 Create explicit traffic using IP Traffic Flows.

We will create three traffic flows representing the traffic downloaded by the three classes of clients. In this scenario, all traffic will be modeled as explicit traffic.

- 2.1 Click the Open Object Palette toolbar button.
- 2.2 Select the "demands" object palette from the drop-down list.

H Object Palette: (demands) X
€ demands Configure Palette
AAL5_G723_Voice AAL5_G726 AAL5_G728_Voice AAL5_G729_Voice AAL5_GSM
application_demand atm_traffic_flow fc_traffic_flow IP_G711_Voice IP_G723_Voice
IP_G726_Voice IP_G728_Voice IP_G729_Voice IP_GSM_Voice ip_ping_traffic ip_security
ip traffic flow

Figure 2-2 Demands Object Palette

2.3 Click on IP demand "ip_traffic_flow" to define an IP-to-IP background traffic flow.

2.4 Connect the IP demand between src_1 and dest_1 (in the same way you would create a link object).



Figure 2-3 IP Demand Connected

- **2.5** Right-click on the workspace and select **Abort Demand Definition** to exit demand operation.
- 2.6 Right-click on the demand object and select Edit Attributes.
- **2.7** In the Attributes dialog box, edit the traffic specification for both bits/second and packets/second values as described below.

Attribute	Value
7 mame	src_1> dest_1
P hodel	ip_traffic_flow
⑦ - Description	Represents IP Traffic
Autonomous System Information	
Destination IP Address	Auto Assigned
Overhead/Segmentation	None
⑦	Not Set
Source IP Address	Auto Assigned
Traffic (bits/second)	NONE
Paraffic (packets/second)	NONE
⑦ ± Traffic Characteristics	Best Effort
⑦	End Of Simulation
⑦	All Background
Traffic Scaling Factor	Same As Global Setting
Traffic Start Time	Same As Global Setting
 ⑦ ⊢Traffic Scaling Factor ⑦ └Traffic Start Time 	Same As Global Setting Same As Global Setting
<[
A	 □ Advance

Figure 2-4 Selected Object's Attributes dialog box

 Configure the "Traffic (bits/second)" attribute with a value of 6.0 Mbps from 0 to 600 seconds. (The profile name may be different in your case.) The graph is updated when you press Enter after typing the values.

<mark>₩</mark> Profile: 18	×
Profile name: 18	
☑ <u>U</u> niform X intervals 600	seconds/step
Use start time 13:14:43.000 /	Aug 13 2004
seconds bits/second	6,000,000 bits/second 4,000,000
	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
<u> </u>	Show calendar time
Export	<u> </u>

Figure 2-5 Configuring the Traffic (bits/second) Attribute

- Click **OK** to commit changes.
- Configure the "Traffic (packets/second)" attribute with a value of 500 packets/second from 0 to 600 seconds. (The profile name may be different in your case.) The graph is updated only if you press Enter after typing the values.

🛞 Profile: 19	X
Profile name: 19	
☑ <u>U</u> niform×intervals 600	seconds/step
Use start time 13:32:11.000/	Aug 13 2004
seconds packets/second 0.0 500 600 0.0	packets/second 600 400 200 0 0 0 5m 10m
Export	<u>O</u> K <u>C</u> ancel

Figure 2-6 Configuring the Traffic (packets/second) Attribute

• Click **OK** to commit changes.

Note that the average packet size implied by the configured traffic volumes (6,000,000 bps and 500 pps) is 6,000,000 bps / 500 pps = 12,000 bits = 1,500 bytes.

- 2.8 In the Attributes dialog box, set the "Traffic Mix" attribute to "All Explicit".
- **2.9** Click **OK** to close the Attributes dialog box.

2.10 Click on the demand object to select it, press Ctrl+C to copy it, and then press Ctrl+V to paste it in the same direction from src_2 to dest_2 and from src_3 to dest_3 (as shown below.)



Figure 2-7 Copying/Pasting Demand Objects

- 3 Configure the Type of Service on each demand.
 - 3.1 Select Protocols > IP > Demands > Characterize Traffic Demands.
 - **3.2** Set the Type of Service for the demands originating from WFQ_net.src_1, WFQ_net.src_2, and WFQ_net.src3 to "Background (1)", "Standard (2)" and "Excellent (3)," respectively.

IP Traffic Flow Cl	haracterization						
Source	Destination	Demand Identifier	Type of Service	Packet Size Distribution	Packet Interarrival Time	Tracer Pack	Record R
WFQ_net.src_1	WFQ_net.dest_1	src_1> dest_1	Background (1)	uniform (1000, Auto_Calc	uniform (0.0019, Auto_C	Default	Once per
WFQ_net.src_2	WFQ_net.dest_2	src_2> dest_2	Standard (2)	uniform (1000, Auto_Calc	uniform (0.0019, Auto_C	Default	Once per
WFQ_net.src_3	WFQ_net.dest_3	src_3> dest_3	Excellent Effort (3)	uniform (1000, Auto_Calc	uniform (0.0019, Auto_C	Default	Once per
							J.
<u> </u>							
Disable Record Rout	e on All <u>R</u> ecord Route for A	All Packets				<u>0</u> K	<u>C</u> ancel

Figure 2-8 IP Traffic Flow Characterization dialog box

3.3 Click OK.

4 Configure the packet size and packet inter-arrival time distributions.

Next we will configure additional traffic generation parameters, such as statistical distributions used for packet sizes and packet inter-arrival times. Note that these can be configured either individually for each demand, under the "Traffic Characteristic" attribute, or globally for all the demands using the Background Traffic Config utility. We will use the latter approach in this lab and configure the distributions by modifying the global settings.

- 4.1 Right-click on the "bkg_config" node and select Edit Attributes.
- 4.2 Set the "Packet Inter-arrival Time Variability" to "exponential".

4.3 Set the "Packet Size Variability" to "constant".

★(bkg_config) Attributes	
Type: utilities	
Attribute	Value
⑦ ⊢ name	bkg_config
(?) - model	Background Traffic Config
⑦ ± Congestion Areas	Disabled
⑦	Default
Packet Interarrival Time Variability	exponential (Auto_Calculated,)
Packet Size Variability	constant (Auto_Calculated,)
⑦	()
🕐 🛨 Traffic Modeling Approach	Default

Figure 2-9 Node's Attributes dialog box

Note that the average values for both distributions are already determined by the settings in the traffic profile and therefore appear as "Auto_Calculated". The traffic volume of 500 packets/second in the profile translates into an average packet inter-arrival time of 0.002 seconds. The average packet size is also already determined to be 1,500 bytes.

- 4.4 Click OK to commit changes.
- 5 Choose statistics.

We will monitor the queuing delay statistics for each service class on the outgoing interface of "router_B". This interface is the access interface to the core network and has WFQ scheduling enabled to provide QoS treatment to different service classes. We will also collect the packet end-to-end delay statistics for all the traffic flows.

- 5.1 Right-click anywhere in the project editor and select Choose Individual DES Statistics.
- **5.2** Expand "Demand Statistics" by clicking on the (+) next to it, and select the "Packet ETE Delay (sec)" statistic.



Figure 2-10 Selecting the Packet ETE Delay (sec) Statistic

5.3 Expand "Node Statistics" by clicking on the (+) next to it, and select the "IP Interface / Queuing Delay (sec)" statistic.





5.4 Click OK.

- 6 Run the simulation.
 - **6.1** Click the **Configure/Run Simulation** toolbar button. The simulation is set to run for 10 minutes.

Simulation Sequence: 1302_lab1-Explicit_traffic		×		
Simulation runs to go: 0	Elapsed Time -	Estimated Remaining Time		
Running: Explicit_traffic	6m 38s.	0:00		
Simulation progress				
Simulation completed.				
Simulated Time: 10m 00s. Events: 25,074,011 Simulation Log: 3 entrie	s	Lindate Progress Info		
Speed: Average: 62,941 events/sec. Current: 64,667 events/sec.		<u>Share Linglace line</u>		
Simulation Speed Messages Memory Usage Memory Stats Invocation				
Beginning simulation of 1302_lab1-Explicit_traffic at 19:27:12 Thu Aug 05 20 Kernel: optimized, sequential Simulation Completed - Collating Results. Events: Total (25,074,011), Average Speed (62,941 events/sec.) Time: Elapsed (6 min. 38 sec.), Simulated (10 min. 0 sec.) Simulation Log: 4 entries DES log messages have been generated. These typically report on simulation behavior, misconfiguration issues, etc. You may wish to examine these log messages by selecting DES->Open DES	log.	*		
Save output when pausing or stopping simulation Pause Resume Stop Run Stop Seque	nce	<u>C</u> lose <u>H</u> elp		

6.2 Click Run to start the simulation. (The simulation runs for about 3 minutes.)

- Figure 2-12 Simulation Sequence dialog box
 - 6.3 Close the Simulation Sequence dialog box after the simulation runs.
 - 7 View the results.

- **7.1** Right-click on the "router_B \leftrightarrow IP_CLOUD" link, and select View Results.
- 7.2 Expand the "point-to-point" group and select the "throughput (packets/sec) ←" and "throughput (bits/sec) ←" statistics. Click Show.



Figure 2-13 Selecting Throughput Statistics to Show

The graph shows that the total traffic entering the IP cloud is 18 Mbps at the rate of 1500 packets per second (pps) – remember each of the three flows is sending traffic at 6 Mps and 500 pps.



Figure 2-14 Throughput Results Graph

7.3 Click Close to close the View Results dialog box.

🛨 Yiew Results	
Discrete Event Graphs Flow Analysis Graphs Flow Analysis Tables D	isplayed Panel Graphs
WFQ_net.router_B WFQ_Det.router_B WFQ_Queuing Delay (sec) IF10 02 WFQ Queuing Delay (sec) IF10 03 WFQ Queuing Delay (sec) IF10 01 WFQ Queuing Delay (sec) IF10 00 (Default Queue	✓ Show preview 0.010
Results Generated: 17:42:49 Aug 11 2004	Uverlaid Statistics This Scenario average Image Unselect Add
·	

7.4 Right-click on "router_B", and select View Results.

Figure 2-15 View Results dialog box

- **7.5** Expand the "IP Interface" group, and select the statistics below in the following order:
 - "WFQ Queuing Delay (sec) IF10 Q3"
 - "WFQ Queuing Delay (sec) IF10 Q2"
 - "WFQ Queuing Delay (sec) IF10 Q1"
- 7.6 Change the display mode from "Statistics Stacked" to "Overlaid Statistics".
- 7.7 Change the "As Is" filter to "average".
- 7.8 Click Show.

As expected, the queues with higher priority (ToS) exhibit smaller queuing delays at the access router "router_B".



Figure 2-16 Showing Queuing Delay Results

- 7.9 Click Close to close the View Results dialog box.
- 7.10 Right-click on the demand going from "src_2" to "dest_2", and select View Results.
- 7.11 Select the "Packet ETE Delay (sec)" statistic, and click Show.

<mark>∭</mark> src_	2> dest_2
0.0025	Packet ETE Delay (sec)
0.0020	monor monor white
0.0015	
0.0010	
0.0005	
0.0000	
	lm 5m 10m

Figure 2-17 Showing the Packet ETE Delay (sec) Statistic Graph

The graph shows that the packet end-to-end delay for the "src_2 \rightarrow dest_2" demand is about 0.0019 seconds.

End of Procedure 2-1

Simulation with Background Traffic

In the following scenario, we replace the explicit traffic with purely background traffic, run the simulation, and compare the results and the simulation speed.

Procedure 2-2 Configure Demands with Background Traffic

- **1** Replace explicit traffic with background traffic.
 - 1.1 Switch to the "Background_traffic" scenario (select Scenario > Switch to Scenario > Background_traffic).
 - **1.2** Right-click on the demand going from "src_1" to "dest_1" and choose **Select Similar Demands**. Note that the other two demands were also selected.
 - 1.3 Right-click on the demand again and choose Edit Attributes.

Attribute	Value
⑦ ⊢ name	src_1> dest_1
P model	ip_traffic_flow
Pescription	Represents IP Traffic
E Autonomous System Information	1
Destination IP Address	Auto Assigned
Overhead/Segmentation	None
T SLA Parameters	Not Set
Source IP Address	Auto Assigned
Traffic (bits/second)	1_3
Traffic (packets/second)	/TV- 2
🕐 🗄 Traffic Characteristics	()
Traffic Duration	End Of Simulation
Traffic Mix	All Background
Traffic Scaling Factor	Same As Global Setting
Traffic Start Time	Same As Global Setting
•	
Apply changes to selected objects	

1.4 Change the "Traffic Mix" attribute to "All Background".

Figure 2-18 Changing the Traffic Mix Attribute

- **1.5** Check the **Apply changes to selected objects** checkbox, and click **OK**.
- **2** Run the simulation.
 - **2.1** Click the **Configure/Run Simulation** toolbar button. The simulation is set to run for 10 minutes.
 - 2.2 Click Run to start the simulation. (The simulation runs for about 10 seconds.)
 - **2.3** Close the Simulation Sequence dialog box after the simulation runs.
- **3** Compare results with those of the previous scenario (with explicit traffic).
 - 3.1 Click the Hide/Show Graph Panels button.
 - 3.2 Load the panels with latest results by selecting DES > Panel Operations > Panel Templates > Load with Latest Results.

The first graph panel displays the queuing delays for various queues at the access router_B obtained in this scenario.



Figure 2-19 Showing Queuing Delays Graph

The second panel compares the individual queuing delays between the two scenarios. Observe that queuing delays for all the queues in both scenarios (explicit and background) are similar.

route	er_B of WFQ_net	
	 Explicit_traffic Background_traffic average (in IP Interface WEO Queuing Delay (ser) IE10.03) 	
0.0006		
0.0003		_
0.0000		
	 Explicit_traffic Background_traffic average (in IP Interface WEO Queuing Delay (sec) IE10.02) 	
0.002		
0.001		_
0.000	Touchas have 60	
	Explicit_traffic Background_traffic surgers (in TR Tablefore WEO Overvice Delay (see) TE10.01)	
0.012	average (in the tricen ace, why Queding Delay (sec) 1F10 Q1)	
0.006		
0.000		
0	m 5m	10m

Figure 2-20 Comparing Queuing Delays

Note that using purely background traffic we were able to significantly reduce the simulation time (from 3 minutes to 10 seconds) and still obtain accurate result for the local queuing delays.

- 4 Compare end-to-end delay statistics.
 - **4.1** Right-click on the demand going from "src_2" to "dest_2" and select View **Results**.

Note that the "Packet ETE Delay (sec)" statistic is shaded out and cannot be selected. The delay effects of the background traffic load are simulated only locally on each traffic element (node or link). Because of this, the purely background traffic mode does not provide for end-to-end delays.

🛞 View Results
Discrete Event Graphs Flow Analysis Graphs
E- src_2> dest_2 └────────────────────────────────────

Figure 2-21 Inaccessible Packet ETE Delay (sec) Statistic

In the next scenario, we will see how we can overcome this shortcoming by using hybrid traffic (mixture of background and explicit traffic).

End of Procedure 2-2

Simulation with Hybrid Traffic

In the next scenario, we configure the demands to use a mixture of explicit traffic (1%) and background traffic (99%). This way we can obtain end-to-end statistics and still achieve significant simulation speedup (compared to the purely explicit traffic scenario).

Note that the explicit traffic is only a small fraction of the total traffic. This is the recommended configuration. For flows with large traffic volumes, very small fractions, such as 0.01% or 0.1% explicit, should be used. Configurations such as 30% explicit + 70% background traffic do not result in significant simulation speedup and should be avoided.

Procedure 2-3 Configure Demands with Hybrid Traffic

- **1** Replace background traffic with hybrid traffic.
 - 1.1 Switch to the "Hybrid_traffic" scenario (select Scenario > Switch to Scenario > Hybrid_traffic).
 - **1.2** Right-click on the demand going from "src_1" to "dest_1" and choose **Select Similar Demands**. Note that the other two demands were also selected.
 - **1.3** Right-click on the demand again and choose Edit Attributes.

(src_1> dest_1) Attributes		_ <u>_</u> _ ×
Attribute	Value	4
7 name	src_1> dest_1	
model	ip_traffic_flow	
Description	Represents IP Traffic	
Destination IP Address	Auto Assigned	
Overhead/Segmentation	None	
🕐 🕀 SLA Parameters	Not Set	
Source IP Address	Auto Assigned	
Traffic (bits/second)	1_3	
Traffic (packets/second)	177 2	
🕽 🗄 Traffic Characteristics	()	
Traffic Duration	End Of Simulation	
Traffic Mix	1.0% Explicit	
Traffic Scaling Factor	Same As Global Setting	
Traffic Start Time	Same As Global Setting	
 	Same As Global Setting Same As Global Setting	
Apply changes to selected objects		Ad <u>v</u> ance

1.4 Change the "Traffic Mix" attribute to "1.0 % Explicit".

Figure 2-22 Changing the Traffic Mix Attribute

- 1.5 Check the Apply changes to selected objects checkbox, and click OK.
- 2 Run the simulation.
 - **2.1** Click the **Configure/Run Simulation** toolbar button. The simulation is set to run for 10 minutes.
 - 2.2 Click Run to start the simulation. (The simulation runs for about 15 seconds.)
 - 2.3 Close the Simulation Sequence dialog box after the simulation runs.
- **3** Compare results with those of the other scenarios.
 - 3.1 Click the Hide/Show Graph Panels button.
 - 3.2 Load the panels with latest results by selecting DES > Panel Operations > Panel Templates > Load with Latest Results.

The first panel compares the queuing delays between the three scenarios. The queuing delays obtained in this scenario using hybrid traffic match with those from previous scenarios.

Fout	er_B of WFQ_net	<u>- ×</u>
	Explicit_traffic Background_traffic Hybrid_traffic versage (in IP Interface, WEO Queuing Delay (sec) IE10 Q3)	
0.0006		
0.0003		
0.0000		
	Explicit_traffic Background_traffic Hybrid_traffic	
0.002	average (in IP Interface, WFQ Queuing Delay (sec) IF10 Q2)	1
0.001	Provide the second s	_
0.000		
	Explicit_traffic Background_traffic Hybrid_traffic average (in IP Interface WEO Queuing Delay (sec) IE10.01)	
0.012		
0.006		
0.000		
0	m 5m	10m

Figure 2-23 Comparing Queuing Delays

The second graph panel compares the packet end-to-end delays for the three traffic demands obtained using explicit traffic and hybrid traffic (no ETE delays were available in the purely background traffic scenario). The results obtained using the two traffic types match closely.



Figure 2-24 Comparing Packet ETE Delay (sec) Statistics

End of Procedure 2-3

Conclusion

In this section, we have demonstrated how using background and/or hybrid traffic can help reduce the simulation time without significant losses in the accuracy of the results.

Using Hybrid Simulation to Model New Application Performance

In this section, we study the performance of a new application deployed in a Wide Area Network (WAN). The preexisting baseline traffic in the network is modeled using link loads. The new application is recreated from an actual traffic trace and converted into OPNET application traffic using ACE.

In the first scenario, we deploy one instance of the new application in an empty network (without the baseline traffic). The application user is modeled using discrete traffic. We assess the application performance and verify whether it conforms to the Service Level Agreement (SLA) requiring that the application response time is below 30 seconds. Next we add the baseline traffic (modeled as link loads) and observe its impact on the application response time. After that, we use ACE and deploy additional application users, modeled not as discrete traffic, but using background traffic flows. We monitor the application response time and apply QoS to improve the application performance.

Procedure 2-4 Use Hybrid Simulation to Model Application Performance

- 1 Examine the new application trace in ACE.
 - 1.1 Launch NETWARS, if not already opened.
 - 1.2 From the System Editor's File menu, choose Open Editor.
 - **1.3** From the Open Editor drop-down menu, select ACE, and then click OK. The ACE Import WIzard displays the ACE Import: Choose Capture File(s) dialog box.
 - **1.4** Click Add Capture File. The Select Capture File for Import dialog box displays.
 - **1.5** In the Select Capture File for Import dialog box, select the file named cwd_local, and then click **Open**. The selected file name displays in the **Capture File** column of the ACE Import: Choose Capture File(s) dialog box.

Note—If you do not have access to this file, simply view the screens provided in this user's guide to follow along with the procedure.
1.6 Continue to follow the ACE Import Wizard screens as they are presented to you until the Treeview window displays.

ACE: cwd_local									
File Edit View AppDoctor Graph Repo	orts Window:	s Help							
🗄 🍉 🛨 🍱 rջ 🔀 🕯	ICK OUICK	K 🔄 🕯) <mark>.</mark>						
	App Bytes ->	App Bytes <-	Start Time	End Time D	1	0.0s , 2s	⁴ 5	, 65 , , 85	
web_client <-> web_server	752	37849	-0.000058	8.343527 8	.3				
	<u> </u>			b					Ŀ
Application payload size: 0 byte	s	1-100	10	1-500	501-	1000	1001-1459	>= 1460	
View by: Tier Pairs - Network Packets		-							

Figure 2-25 Treeview window

- Application chart only E Show Dependencies Application Message Chart 8s 6 web_client database_serve Application payload size: 1 0 bytes 101-500 1 501-1000 1001-1459 1-100 >= 1460 Dependency delays: Network delay Application delay Close Help
- **1.7** Click the Data Exchange Chart button.



The Data Exchange Chart shows the application traffic patterns between the different tiers. Note that there are 3 tiers in this application: web_client, web_server and database_server. The horizontal lines represent the tiers - the topmost line corresponds to the web_client, the middle line to the web_server, and the bottom line represents the database_server. The color arrows connecting the three horizontal lines represent individual packet exchanges between the tiers. The horizontal axis visualizes the time of the transaction in seconds. The application is a typical database query. Initially the web_client contacts the web_server with a request and the two exchange



several packets. After that the bulk of the traffic exchange is between the web_server and the data_server. At the end of the application the web_server sends replies to the web_client. Note that the duration of the whole application is about 8.1 seconds.

- 1.8 Click Close to close the Data Exchange Chart.
- **1.9** Close the ACE editor.
- 2 Deploy one application user running discrete traffic.

Configure the network to use one instance of the ACE application. The following nodes will be used as the application tiers: web_client \rightarrow San Diego, web_server \rightarrow Los Angeles, and database_server \rightarrow Houston.

- 2.1 Launch NETWARS, if not already opened.
- 2.2 From the System Editor's File menu, choose Open Editor.
- **2.3** From the Open Editor drop-down menu, select **Scenario Builder**, and then click **OK**. The Scenario Builder window displays.
- 2.4 Select File > Open Project. The Open Project dialog box displays.
- **2.5** Select the project named 1302_lab2 (or if you want to follow along without actually performing the steps in this procedure, select the project named 1302_lab2_ref instead), and then click Open.

Scenario "app_user_only" appears as the first scenario.

Note—If you do not have access to these files, simply view the screens provided in this user's guide to follow along with the procedure.



Figure 2-27 Displaying app_user_only

- 2.6 Click Protocols > Applications > Deploy ACE Application on Existing Network > as Discrete Traffic. The Configure ACE Application dialog box displays.
- 2.7 In the Configure ACE Application dialog box:
 - Set the application "Name" to "my_app"
 - Set the "Repeat" to "20 times per hour"
 - Click the Add Task button and select the "cwd_local.atc.m" ACE trace file.

K Configure ACE Application		x
Application details		_
Name: my_app	Specify:	I
Repeat: 20 times per hour using the following limit Infinite C Count: 1	ilt 1. Application name. 2. Application repetition per user. 3. Maximum number of repetitions	
Contained tasks		-
Task ACE Trace File Tier 1 [cwd_local.atc.m]	 Click 'Add Task' to select the ACE trace file(s) to be contained as part of this application. Note: All contained tasks must have the name first talker (i.e. 'client'). The first talker is the tier that sends the first packet in the trace. The file list popup is filtered based on the 'client' tier. By default, tasks are executed in a serial order. You can edit the 'Application Config' object to change this order. 	
Add Task Delete Task		
	Next > Cancel	

Figure 2-28 Configure ACE Application dialog box

2.8 Click Next.

In the next step we will assign application tier functionality to existing nodes in the network.

2.9 Click "Select Nodes" for the "web_client" tier.

🛨 Deploy Tiers		×
Tier Name	Select Nodes	4
web_client		
web_server	N	
database_server		
		-
First talker: web_client		
(Nodes specified for this tier will initiate application traffic	2)	
	<u>D</u> eploy <u>C</u> ancel	

Figure 2-29 Deploy Tiers dialog box

2.10 Select "San Diego" from the node list by clicking on the "Deploy" column value.

```
2.11 Click OK.
```

K Configure Nodes with Selected Tier	×
Select nodes from the list below to represent the tier:	web_client
Nodes	Deploy 🔺
HartfordH	No
Boston	No
New York	No
Miami	No
Tampa	No
Jacksonvile	No
Birmingham	No
New Orleans	No
Houston	No
San Diego	Yes
Los Angeles	No ^{NS}
San Jose	No
Seattle	No
Deploy on All	<u>O</u> K <u>C</u> ancel

Figure 2-30 Configure Nodes with Selected Tier dialog box

2.12 In a similar fashion, choose "Los_Angeles" to function as the web_server and "Houston" to represent the database_server.

2.13 Click Deploy.

- **3** Run the simulation and view results.
 - **3.1** Click the **Configure/Run Simulation** toolbar button. The simulation is set to run for 1 hour.
 - **3.2** Click **Run** to start the simulation.
 - **3.3** Close the Simulation Sequence dialog box after the simulation runs.
 - 3.4 Click DES > Results > View Statistics.

3.5 In the View Results dialog box, expand "Global Statistics / ACE" and select the "Task Response Time (sec)" statistics.



Figure 2-31 Selecting the Task Response Time (sec) Statistic

3.6 Click Show.

Note the application response time varies around 23.2 seconds. This conforms to the 30 second limit required by the SLA.



Figure 2-32 Task Response Time Statistics

3.7 In the View Results dialog box, change the display filter from "As Is" to "average".

₩ Yiew Results						
Discrete Event Graphs Flow Analysis Graph	s Flow A	nalysis Tables D	isplayed Panel Gra	aphs		
Global Statistics	🔽 Sho	w <u>p</u> review				
CE C	25					
Traffic Sent (bytes/sec)	20 -					
Traffic Received (bytes/	15 -					
E Custom Application	10 -					
Diject Statistics						
	5 -					
Atlanta <-> Washington DC						
Birmingham <-> Atlanta Acc	°г					
Boston <-> DU Access [U]	0	1	,000	2,000	3,000	4,000
Lincago <-> Washington Dt						time (sec)
	Stack	ed Statistics	▼ This Scenar	o 🔽		
	ľ——			_		
	averag	je				
Results Generated: 14:29:15 Aug 10 2004				<u>U</u> nselect	Add	<u>S</u> how
☐ <u>Ig</u> nore views						<u>C</u> lose

Figure 2-33 View Results dialog box

3.8 Click Show.

The graph shows the average response time for the new application.



Figure 2-34 Average Task Response Time Statistics

Note—Remember that the duration of the application in the ACE editor was about 8.1 seconds. However, the application response time statistics now show that it takes about 23.2 seconds to complete the applications. Why the difference? The application trace was captured on a local network and all the tiers were part of the same LAN. In this scenario the application is deployed in a WAN and the application tiers are placed in different geographical locations (San Diego, Los Angeles, Houston). This causes addition latency in the communication between the tiers, and as a result of this the application response time increases.

4 Include pre-existing baseline traffic.

In the next scenario, we add the baseline traffic (modeled as link loads) and observe its impact on the new application.

4.1 Switch to the "app_user_and_linkloads" scenario (select Scenario > Switch to Scenario > app_user_and_linkloads).

This scenario already includes the application traffic we configured in the previous scenario. In addition there are background loads configured on the links that represent the pre-exiting baseline traffic (link loads can be configured manually or imported from a variety of traffic management tools).

4.2 To view an example traffic load profile, right-click on the Salt Lake City ↔ Dallas link and select Edit Attributes.

★ (Salt Lake City <-> Dallas) Attribute	s _ O X
Attribute	Value
⑦ ⊢ name	Salt Lake City <-> Dallas
? - model	ppp_adv
⑦ ⊞ Background Load	[]
Propagation Speed	Speed of Light
⑦ L data rate	0C3
	•
Apply changes to selected objects	☐ A <u>d</u> vanced
<u>Find Next</u>	<u> </u>

4.3 Click the "Background Load" attribute and select Edit....

Figure 2-35 Link Attributes dialog box

4.4 Click the "Intensity (bps) [Salt Lake City → Dallas]" attribute and select Edit....

K (Background Load) Table	×
Attribute	Value 🔺
Average Packet Size (bytes) [Salt Lake City	Default
Average Packet Size (bytes) [Dallas -> Salt	Default
Intensity (bps) [Salt Lake City -> Dallas]	/ [†] V ⁻ 91_94_95_102_1
Intensity (bps) [Dallas -> Salt Lake City]	NONE
	Select
	Edit
	v
Details Promote	<u> </u>

Figure 2-36 Background Load Attributes dialog box

The profile captures the WAN link traffic during business hours on May 6 (from 8am to 6pm). Note the green vertical line in the profile whose position indicates the current network time. The current network time can be configured in the Time Controller tool (invoked by Ctrl+Alt+T). In this scenario the current network time has been pre-configured to 11 am, so that the 1-hour simulation that we will run includes the busiest period of the workday (from 11 am to 12 pm).

₩ Profile: 91_94_95_102_118_120_145_149		×
Profile name: 91_94_95_102_118_120_145_149		
☑ Uniform X intervals 3,600		
✓ Use start time 08:00:00.000 May 06 2004		
seconds bits/second	bits/second	
0.0 42,331,678.19	150,000,000	
3,600 35,331,678.19		
7,200 50,798,013.83		
10,800 140,957,616.59	100,000,000	
14,400 73,149,139.91		
18,000 137,778,967.89	F0 000 000	
21,600 105,334,761.47	50,000,000	
25,200 126,401,713.77		
28,800 91,682,056.52		
32,400 42,018,467.83		
36,000 18,422,161.39	45, ⁶ 0, ⁷ 0,	
	0-37 ⁴ 4 77	
	A	
	🖂 🔽 Show calendar time	
Export	<u>D</u> K	<u>C</u> ancel

Figure 2-37 Profile dialog box

4.5 Click Cancel until you have closed all the Attribute dialog boxes.

- 5 Run the simulation and view the results.
 - 5.1 Click the Configure/Run Simulation toolbar button.
 - 5.2 Click Run to start the simulation.
 - 5.3 Close the Simulation Sequence dialog box after the simulation runs.
 - 5.4 Click DES > Results > View Statistics.

5.5 Expand "Global Statistics / ACE" and select the "Task Response Time (sec)" statistics.

\star View Results	
Discrete Event Graphs Flow Analysis Graphs Flow Analysis Tables	letwork Inventory Tables Displayed Panel Graphs
Global Statistics	Show preview 23.95 23.85
Task Response Time (sec) <ace (my_app)="" <="" application="" atlanta="" custom="" my_s="" object="" statistics=""> Atlanta Access [0] Atlanta <> Washington DC [0]</ace>	23.80 23.75 0 2,000 4,000 time (sec)
Birmingham <-> Atlanta Access [0] Boston <-> DC Access [0] Results Generated: 10:17:49 Aug 13 2004	Stacked Statistics This Scenario As Is Unselect Add Show
Ignore views	Close

Figure 2-38 View Results dialog box

5.6 Click Show.

Compared to the previous scenario, as a result of including the baseline traffic load, the application response time increased by about 0.7 seconds to 23.9 seconds. The response time is still, however, well below the SLA limit (30 seconds).



Figure 2-39 Task Response Time Statistics

Note—The above result indicates that under current traffic conditions the network has sufficient spare capacity to support one new application within the SLA limits. Will the network capacity be enough to support thousands of new users? Continue on to the next scenario.

6 Deploy additional application users modeled as traffic flows.

In the following scenario, we configure an additional 1,690 application users in the network. This time, however, the users will not be modeled using discrete traffic, but rather as background traffic flows. We could model all the new users as explicit traffic, but that might result in a long simulation time. To get a quick answer, we use mixed traffic and hybrid simulation.

- 6.1 Select Scenario > Duplicate Scenario.
- 6.2 Name the new scenario "add_app_users_as_flows".
- 6.3 Select Protocols > Applications > Deploy ACE Application on Existing Network > as Traffic Flows.
- 6.4 In the ACE Traffic Import: Specify Tasks dialog box under "Tasks", click on "Click here to add new task", select the "cwd_local" trace file, and then click Next.

품 ACE Traffic Import: Specify Tasks		×
Choose task(s):		
Tasks cwd_local		Choose the ACE tasks you want to deploy as traffic flows.
cwd_local cwd_remote		NOTE: All selected tasks must have the same first talker, although the other tiers can be different.
	-	For each tier pair, OPNET will merge the traffic in all selected tasks and create two unidirectional
Tiers included in task(s):		flows. You will assign this traffic to specific nodes
web_client	A	in die fiext window.
web_server database_server		
1		<u>N</u> ext > <u>C</u> ancel

Figure 2-40 ACE Traffic Import: Specify Tasks dialog box

6.5 Assign nodes for each of the application tiers. Click on "ACE Tier web_client <initiating_tier>" to select it.



Figure 2-41 ACE Traffic Import: Assign Nodes dialog box

Next, assign all thirteen end-nodes in the network to support one hundred and thirty web_clients each (1,690 users total).

- 6.6 Go to the project editor, right-click on Seattle, and choose Select Similar Nodes.
- 6.7 Return to the ACE Traffic Import: Assign Nodes dialog box, and click Assign Selected Nodes.
- 6.8 In the ACE Traffic Import: Configure Initiating Node dialog box:
 - Set the "Number of users" to "130".
 - Set "Repetitions per user per hour" to "20".
 - Check the Apply to remaining nodes (12) checkbox.

🛞 ACE Traffic Import: Configure Ini	tiating Node 🛛 🕅
Configure Traffic Load for "Seattle"	
Number of users: 130 Demand type: ip_ace_traffic_flow	Start time: 0 Hours
Task	Repetitions per user per hour
cwd_local	20
	y
Apply to remaining nodes (12)	<u>K</u>



6.9 Click OK.

Note that the 13 selected nodes were added to the web_client list.



Figure 2-43 Node Assignments (web_client) List

- **6.10** Next we will assign five nodes to support the web_server functionality. Click on "ACE Tier web_server" to select it.
- **6.11** Go to the project editor. Click in the workspace to unselect the previously selected nodes. While holding the **Shift** key, click on the following five nodes to select them: Seattle, Los Angeles, Houston, Miami, New York.
- 6.12 Return to the ACE Traffic Import: Assign Nodes dialog box, and click Assign Selected Nodes.

The five nodes should now appear listed under the web_server.

CH ACE Tier: web_server	Ι
Seattle	L
Los Angeles	L
Houston	I
Miami	L
New York	I
🗄 📲 ACE Tier: database_server	
🛛 🛶 😵 No nodes assigned yet.	1

Figure 2-44 Node Assignments (web_server) List

6.13 Finally, click on the "ACE Tier database_server" to select it. Select Houston in the project editor, and click Assign Selected Nodes. Houston will be added to the list.



Figure 2-45 Node Assignments (database_server) List

6.14 Click **Finish**. Observe the purple traffic demands added to the network to represent the traffic generated by the new application users.



Figure 2-46 Network Traffic Demands

- 7 Run the simulation and view the results.
 - 7.1 Click the Configure/Run Simulation toolbar button.
 - 7.2 Click Run to start the simulation.
 - 7.3 Close the Simulation Sequence dialog box after the simulation runs.
 - 7.4 Click DES > Results > View Statistics.
 - **7.5** Expand "Global Statistics / ACE" and select the "Task Response Time (sec)" statistics. Click **Show**.



Figure 2-47 Task Response Time Statistics

Note that the application response time increased dramatically and some of the values are above the 30-second Service Level Agreement limit.

7.6 To find the reason for this increase, select DES > Results > Find Top Statistics. Expand the "Link Statistics / point-to-point" group and select "utilization". Click Find Top Statistics.



Figure 2-48 Select Statistic for Top Results dialog box

7.7 Observe that as a result of adding new ACE application users, several links in the network become over 97% utilized. The link utilization for the "Dallas Access ↔ Dallas" link reaches 99.4%.

Top Objects: point-to-point.utilization					×
Object Name	Minimum	Average /\	Maximum	Std Dev	
Dallas_Access <-> Dallas [0]>	88.288	98.648	99.437	1.7263	
Salt Lake City <-> Dallas [0] <	90.305	95.326	97.303	1.0896	
Salt Lake City <-> Phoenix [0]>	87.759	92.858	97.204	1.4197	
Dallas_Access <-> Dallas [0] <	88.061	91.761	95.275	1.3816	
Salt Lake City <-> Dallas [0]>	86.590	91.632	95.838	1.7058	
Salt Lake City <-> Phoenix [0] <	86.763	91.236	96.710	1.6207	
Denver <-> Kansas City [0]>	76.414	84.596	94.752	3.6874	
Salt Lake City <-> Kansas City [0] <	73.292	84.276	92.116	3.9334	
Kansas City <-> Washington DC [0]>	74.989	84.006	90.335	3.0427	
Dallas <-> Denver [0] <	75.498	83.610	92.947	3.3889	
Atlanta <-> Washington DC [0] <	64.327	71.780	79.345	3.1723	
Salt Lake City <-> Denver [0]>	64.276	71.188	76.941	3.1430	
Kansas City <-> Oklahoma City [0]>	63.204	71.138	78.414	3.2083	
Denver <-> Oklahoma City [0] <	63.834	71.017	78.369	2.8510	-
Report on top 10 statistics whose		Graphs Stacked 💌	As Is	<u>▼</u> <u>G</u> raph	
Average V				<u>I</u> ext Report	
Ignore views				<u>Find</u> Object	

Figure 2-49 Top Objects Point-to-Point Utilization dialog box

- 7.8 Close the above window showing link utilizations.
- 7.9 Close the Select Statistic for Top Results dialog box.

The above results indicate that the current network bandwidth will not be enough to support the new application on top of the pre-existing traffic. This problem can be solved either by increasing the network capacity or applying some QoS techniques to prioritize the critical traffic. We will try out the latter approach and apply Quality of Service in the next scenario.

End of Procedure 2-4

Implementing QoS in the Network and Prioritizing Application Traffic

In the following scenario, we apply Weighted Fair Queuing (WFQ) to all the routers in the network. We will configure a high-priority Type of Service on the ACE application traffic (both discrete and flow based) and thus give it preferential treatment over the pre-existing traffic (link loads).

Procedure 2-5 Implement QoS in the Network and Prioritize Traffic

- 1 Choose Scenario > Duplicate Scenario.
- 2 Name the new scenario "with_qos".
- 3 Apply WFQ on all the interfaces in the network.
 - 3.1 Select Protocols > IP > QoS > Configure QoS.
 - **3.2** In the QoS Configuration dialog box:
 - Set the "QoS Scheme" to "WFQ (Class Based)".
 - Set the "Qos Profile" to "ToS Based".
 - Uncheck the Visualize QoS configuration checkbox.

🛨 Qo5 Configuration 🔀		
This operation will overwrite existing QoS configurations on IP interfaces.		
QoS Scheme: WFQ (Class Based)		
QoS Profile: ToS Based		
Apply selection to subinterfaces		
Apply the above selection to		
 All connected interfaces 		
C Interfaces across selected link(s)		
C Interfaces on selected router(s)		
└── <u>V</u> isualize QoS configuration		
<u> </u>		

Figure 2-50 QoS Configuration dialog box

• Click OK.

- 4 Set the Type of Service on all the traffic representing the new application (i.e. both the discrete traffic and the flows) to give it a preferential treatment over the baseline traffic.
 - **4.1** To set the Type of Service on the traffic flows, right-click on any demand in the network and choose **Select Similar Demands**.
 - 4.2 Right-click on the same demand and select Edit Attributes.
 - **4.3** Expand the "Traffic Characteristics" attribute group by clicking on the (+) sign next to it. Set the "Type of Service" attribute to "Interactive Multimedia (5)".

🛣 (Boston> Seattle) Attributes	
Attribute	Value
Image:	ip_ace_traffic_flow
⑦ – Description	This demand was created by Ace to FI
Autonomous System Information	
⑦ Destination IP Address	Auto Assigned
⑦ - Overhead/Segmentation	None
⑦ SLA Parameters	Not Set
Ource IP Address	Auto Assigned
⑦	/TV- 311
⑦	/TV- 312
🕐 🗆 Traffic Characteristics	()
⑦	Interactive Multimedia (5)
Packet Size PDF	Default ^K
Packet Interarrival Time PDF	Default
⑦	Same As Global Setting
Record Route Option	Once per Flow
⑦	End Of Simulation 👻
•	
Apply changes to selected objects	☐ Ad <u>v</u> anced
<u></u> Eind Next	<u> </u>

Figure 2-51 Attributes dialog box

- 4.4 Check the Apply changes to selected objects check box, and click OK.
- 5 Change the Type of Service on the discrete application traffic.
 - 5.1 Right-click on the "Applic Config" utility node and select Edit Attributes.
 - 5.2 Click on the "Application Definitions" value and select Edit.

⊀ (Applic Config) Attributes	_ _ _ _ _ _
Type: utility	
Attribute	Value
⑦ ⊢ name	Applic Config
	Application Config
① Application Definitions	[]
⑦	() Default None
•	Edit
Apply changes to selected objects	r∿ A <u>d</u> vanced
<u></u> ind Next	<u> </u>

Figure 2-52 Applic Config Attributes dialog box

5.3 Edit the Description for "my_app".



5.4 Edit the Value for "Custom".

K (Description) Table	×
Attribute	Value 🔺
Custom	()
Database	()
Email	Off
Ftp	
Http	Off
Print	Off
Remote Login	Off
Video Conferencing	Off
Details Promote	<u> </u>

Figure 2-54 Descriptions Table

6 Change the "Type of Service" attribute to "Interactive Multimedia (5)".

2	K (Custom) Table	×
	Attribute	Value 🔺
	Task Description	()
	Task Ordering	Serial (Ordered)
	Transport Protocol	TCP
	Type of Service	Interactive Multimedia (5)
	Connection Policy	Refresh After Application
	RSVP Parameters	None
	ACE Task Interdependency	Final Response Arrival at
	<u>D</u> etails <u>P</u> romote	<u>O</u> K <u>C</u> ancel

Figure 2-55 Custom Table

- 6.1 Click OK as often as needed to close all the open dialog boxes.
- 7 Run the simulation and view the results.
 - 7.1 Click the Configure/Run Simulation toolbar button.
 - 7.2 Click Run to start the simulation.
 - 7.3 Close the Simulation Sequence dialog box after the simulation runs.
 - 7.4 Click DES > Results > View Statistics.

7.5 Expand "Global Statistics / ACE" and select the "Task Response Time (sec)" statistics. Click **Show**.



Figure 2-56 Task Response Time Statistic

We can see that applying QoS and prioritizing the new application helped achieve the goal. The application response time is about 23.5 seconds, which is below the 30-second SLA limit.

End of Procedure 2-5

3 Importing IP and Layer 2 Networks with MVI

Introduction

The Multi-Vendor Import (MVI) module gives you a practical way to import topology and traffic data from the production network environment. The Device Configuration Import (DCI) feature of the MVI module lets you automatically create high-fidelity network models by importing router and switch configuration data.

This chapter shows you how to use the DCI features to import from switch, router, and security appliance configuration files. DCI's current platform support includes Cisco IOS, Cisco CatOS, Cisco PIX, and Juniper JunOS devices.

Note—The following examples were presented at OPNETWORK 2004 in Session 1617, Importing IP and Layer 2 Networks with MVI. If you do not have access to the files that these procedures use, you can still follow along using the sample screens provided in this user's guide.

Import an Example Network

A set of router configuration files is provided for an enterprise scale network. In this example, we will import the device configuration files to create a network model and explore it using available visualization features.

Procedure 3-1 Import Device Configuration Files

- 1 Launch NETWARS, if not already opened.
- 2 From the System Editor's File menu, choose Open Editor.
- 3 From the Open Editor drop-down menu, choose Scenario Builder, and then click OK.
- 4 Create a new project.
 - 4.1 Choose File > New Project, and click OK.
 - **4.2** Name the project *Session_1617*.
 - **4.3** Name the phase *Lab_1*, and click **OK**.
 - 4.4 Choose Topology > Import> Device Configuration Files... The Import Device Configurations dialog box opens.
- **5** Specify folders for device configuration files [we will look into in detail on vendor types later in the procedure].

- 5.1 Select the checkbox for Cisco (IOS, CatOS, PIX).
- **5.2** Click the **Browse** button for Cisco (IOS, CatOS, PIX), and select the folder: C:\Netwars\User_Data\Projects\Session_1617\Lab_1\Cisco
- 5.3 Select the checkbox for Juniper (JunOS).
- 5.4 Click the **Browse** button for Juniper (JunOS) and select the folder:

C:\Netwars\User_Data\Projects\Session_1617\Lab_1\Juniper

- **5.5** Specify import options [we will look into in detail on import options later in the procedure].
- 5.6 Select the checkbox for Generate import log.
- 5.7 Select the checkbox for Create PVCs.
- **5.8** Leave other options unchecked.
- 6 Import.
 - 6.1 Make sure your settings are as shown below:

K Import Device Configurations		×	
Import Mode			
• Replace entire model			
C Merge with existing model			
C Reimport configurations for selected devices			
C Reimport configurations for modified devices			
Specify Directories Containing Device Configuration Files			
Cisco (IOS, CatOS, PIX) C:\Netwars\User_Data\Projects\	Session_1617\Lab_1\Cisco	Browse	
✓ Juniper (JUNOS) C:\Netwars\User_Data\Projects\	Session_1617\Lab_1\Juniper	Browse	
- Import Options	Model Assistant Files		
Create nodes to represent external ASes	☑ Use the following model assistant files:		
Create nodes to represent edge LANs	<click add="" to=""></click>	A	
Create PVCs			
Generate import log			
metho	Import Cancel	<u>H</u> elp	

Figure 3-1 Import Device Configurations dialog box

6.2 Click Import.

- 7 The Open Import Assistant dialog box displays. It reports that the network has unnumbered interfaces and connected interfaces with data rates unspecified. For now, click Cancel to close the dialog box; you will come back to this in a later procedure.
- 8 Save the project.
 - 8.1 Choose File > Save Project.



The imported network should look as follows:

Figure 3-2 Sample Network

The import process is now complete.

End of Procedure 3-1

Exploring the OPNET Network Model

In this section you will explore different parts of the imported network model using built-in visualization tools.

Procedure 3-2 Explore the OPNET Network Model

- 1 Zoom to the core of the network in the network editor by:
 - **1.1** Clicking the **Zoom In** toolbar button.

1.2 Drag the cursor to create a box around the area of interest.



Figure 3-3 Zoom In

Note—If you want to zoom to another area, you can come back to the original view by clicking the **Zoom Out** toolbar button.

- Figure 3-4 Link Types in Color

PVCs are shown using dashed lines in the same color as the corresponding link types.

- 3 Hide all logical connections. Right-click on a demand object, and select Hide Similar Demands.
- 4 Click the Zoom Out button to go back to the top-level view, and choose View > Show Network Browser (Ctrl + B).



Figure 3-5 Network Browser

- **5** View link tool tip:
 - **5.1** In the network browser, choose **Links** from the top drop-down list. The network browser shows the list of links in the network ordered alphabetically.
 - 5.2 In the browser, choose the link Albany / Serial0/0 <-> 172_16_249_12/30(+).
 - **5.3** The link between *Albany* and the FR cloud gets selected in the project editor. Point your mouse at this link for a few seconds.
 - **5.4** If you can't find the link in the network, double-click on it for the editor to auto-zoom to that part of the network.



Link tool tip displays link type; node, interface, and IP address; and data rate.

Figure 3-6 Link Tool Tip

- 6 In the network browser, change back to **Nodes** from the top drop-down list; Select the router *Albany*, observe that the node is selected on the network browser at the top left corner of the network.
- 7 Choose View > Show Network Browser again to close the network browser.
- 8 View command mappings for interface FastEthernet0/0.
- 9 Right-click on router *Albany*, and select Edit Attributes.
- 10 Expand the attribute group IP.

11 Go to the **Interface Information** attribute under **IP Routing Parameters**. Each physical interface of the router is mapped to a single row under this attribute.

	± HSRP		Γ
	I IP		l
1	IP Processing Information	Default	 l
1		None	
2	IP Routing Parameters	()	
2	– Router ID	172.16.103.1	
1	Autonomous System Number	65000	
2	 Interface Information 	[]	
2	 Aggregate Interfaces 	None K	
2	 Loopback Interfaces 	()	

Figure 3-7 Attributes dialog box

FastEthernet0/0 Serial0/0
erial0/0

Figure 3-8 Interface Information Attribute

- 12 Observe the values set on the attributes **IP Address** and **Subnet Mask** for interface *FastEthernet0/0*. They are 172.16.114.1 and 255.255.255.0 respectively. These are the same values as you noticed before in the configuration file.
- **13** Click **Cancel** to close the dialog box that shows interface information.
- 14 Click Cancel to close the dialog box that shows attributes for node Albany.
- **15** View subinterface information.
- 16 Right-click on router *Albany* again, and select View Device Configuration Source Data.

17 Scroll down to see the subinterfaces configured for the device.

41	interface Serial0/0
43	hondwidth 1544
42	Bandwiden 1544
43	encapsulation frame-relay
44	no ip address
45	no ip directed-broadcast
46	no fair-queue
47	
4.8	interface Serial0/0.101 point-to-point
49	bandwidth 512
50	clockrate 512000
51	encapsulation frame-relav
52	ip address 172.16.101.5 255.255.255.252
53	ip ospf cost 500
54	frame-relay interface-dlci 214
55	
56	interface SerialO/0.102 point-to-point
57	bandwidth 100
5.8	encapsulation frame-relay
59	ip address 172.16.149.5 255.255.255.252
60	clockrate 512000
61	frame-relav interface-dlci 215

Figure 3-9 Device Subinterfaces

- 18 Interface *Serial0/0* has subinterfaces *Serial0/0.101*, *Serial0/0.102*. Notice on line 53 that *Serial0/0.101* has an OSPF cost set to 500.
- **19** Close the window that shows the configuration file.
- 20 Right-click on router Albany and select Edit Attributes.
- 21 Expand the attribute group IP Routing Protocols.
- 22 Go to the Interface Information attribute under OSPF Parameters.
- 23 Choose Subinterface Information for interface *Serial0/0*. Each subinterface of the physical interface is mapped to a single row under OSPF Parameters > Interface Information > Subinterface Information.

24 You can notice subinterfaces *Serial0/0.101, Serial0/0.102*, etc., configured here. Note that the *Cost* field of interface *Serial0/0.101* is set to 500, as noted in the configuration file.

E	IP Routing Protocols	
0	BGP Parameters	()
0	EIGRP Parameters	()
0	IGRP Parameters	()
0		()
0	OSPF Parameters	()
	Processes	()
0	 Interface Information 	()
0	 Aggregate Interfaces 	None
0	🛨 Loopback Interfaces	()
0		None
0	└─VLAN Interfaces	None
0		()

Figure 3-10 Attributes dialog box

★ (Interface Information) Table							
•	Router Priority	Area ID	Process Tag(s)	Cost	Timers	Neighbor List	Subinterface Infor 📥
adcast	1	0.0.0.1	100	Auto Calculate	[]	None	None
adcast	1	0	1	Auto Calculate	[]	None	[]
_							•
2	Rows <u>D</u> elete	Insert	Duplicate Move	Up <u>Mo</u> ve Dow	'n		
D <u>e</u> tails	Dgtails Promote OK Cancel						

Figure 3-11 Interface Information Attribute

Name	Status	Silent Mode	Туре	Router Priority	Area ID	Process Tag(s)	Cost	Timers
Serial0/0.101	Enabled	Disabled	Point To Point	1	0.0.0.1	100	500	()
Serial0/0.102	Enabled	Disabled	Point To Point	1	0.0.0.1	100	Auto Calculate	()

Figure 3-12 Subinterface Information Attribute

- 25 Click Cancel to close the dialog box that shows subinterface information.
- 26 Click Cancel to close the dialog box that shows interface information.
- 27 Click Cancel to close the dialog box that shows attributes for node Albany.

End of Procedure 3-2

Procedure 3-3 View Skipped Commands

- **1** View log messages:
 - **1.1** Right-click on router *Albany* and select **View Detailed Import Log**. The following dialog box displays.

🛞 Log Browser -	(Session_16)	17-Lat	o_1-rci) [Cis	co Systems;C:\op	_models	Lab_1_Configs	Cisco\Albany.cfg]
E─ Device Conf	iguration Import	L	Line Number	Category	Class	Subclass	Message
			1	Skipped Command	Global	<no subclass=""></no>	()
			6	Skipped Command	Global	<no subclass=""></no>	no service password-encryption
			22	Skipped Command	Global	<no subclass=""></no>	ip http server
			23	Skipped Command	Global	<no subclass=""></no>	ip http authentication aaa
			29	Skipped Command	Global	<no subclass=""></no>	memory-size iomem 25
			30	Skipped Command	Global	<no subclass=""></no>	ip subnet-zero
			32	Skipped Command	Global	<no subclass=""></no>	noip finger
			39	Skipped Command	Interface	Loopback0	no ip directed-broadcast
			45	Skipped Command	Interface	Serial0/0	no ip directed-broadcast
			46	Skipped Command	Interface	Serial0/0	no fair-queue
			68	Skipped Command	Interface	FastEthernet0/0	no ip directed-broadcast
			77	Skipped Command	BGP	AS: 65000	()
			78	Skipped Command	BGP	AS: 65000	()
			80	Skipped Command	BGP	AS: 65000	ip classless
			81	Skipped Command	BGP	AS: 65000	noip http server
			83	Skipped Command	Global	<no subclass=""></no>	snmp-server engineID local 000000090200
			155	Skipped Command	Global	<no subclass=""></no>	()
			225	Skipped Command	Global	<no subclass=""></no>	()
			229	Skipped Command	Global	<no subclass=""></no>	tacacs-server directed-request
			237	Skipped Command	Global	<no subclass=""></no>	()
			249	Skipped Command	Global	<no subclass=""></no>	()
1	1	الشر	250 4	outra a communa	CLEAR	AND COMPLEX.	an anti-adular allerate (
Select displayed col	umns:						
I Line Number							Chur
Category	🔽 Class		✓ Subclas:	5			Liose

Figure 3-13 Log Browser Showing Skipped Commands for Albany

Skipped commands are shown according to their class and subclass.

- **1.2** Expand the tree-view in the left to see the various categories of skipped commands.
- **1.3** Choose subclass *FastEthernet0/0*, under *Interface* class in the tree-view to view the skipped commands for this particular interface. These are commands that are currently not supported by DCI.





1.4 Click **Close** to close the dialog box that shows log messages.

End of Procedure 3-3

Procedure 3-4 Visualize the Network Model

 Choose View > Visualize Protocol Configuration > IP Routing Domains (Ctrl+Shift+V) to visualize the routing domains in the network. The network's routing domains display as follows.



Figure 3-15 Sample Network's Routing Domains

- 2 Scale the icons in the network.
 - 2.1 Choose View > Visualize Protocol Configuration > Clear Visualization to clear routing domain visualization.
 - 2.2 Left-click in an empty space in the project editor to deselect all objects.
 - 2.3 Choose View > Layout > Scale Selected Icons.

★Scale All Icons			X			
C <u>F</u> ix icons at full size						
C Scale icons, minimize overlap						
Scale icons, ignore overlap						
Scale factor: 73		—Ţ—				
Smallest			Largest			
Set Icons to Uniform Size	<u>0</u> K	<u>C</u> ancel	<u>H</u> elp			

Figure 3-16 Scale All Icons dialog box

2.4 Set Scale factor value to 25.

Notice, the icons become smaller; in many cases where you have a very large topology, scaling can help to get a better view of the network and its topology.

2.5 Click Cancel to close the Scale All Icons dialog box.

3 Choose File > Save Project to save the project.

End of Procedure 3-4

Conclusions

The Multi Vendor Import module (MVI) allows you to import network topology using device configuration files. Using the "Import Logging" feature, you can view the commands that the Device Configuration Import (DCI) does not use during the import.

The network browser is useful for navigating through the network. NETWARS provides several visualization features that make it easy to understand the network topology and configuration.

Importing from device configuration files provides the ability to build a network model, however all the relevant info is not contained in the configuration files. In the following procedure, you will learn how to provide supplemental information to deal with these inadequacies.

Using the Model Assistant

The device configuration files obtained from a network may not always contain all of the necessary information to model the network accurately. In this section, we will import a new set of configuration files with missing information and see how we can provide additional information during and after the import process using the Model Assistant.

Procedure 3-5 Import the Configuration Files

- 1 Launch NETWARS, if not already opened.
- 2 From the System Editor's File menu, choose Open Editor.
- 3 From the Open Editor drop-down menu, choose Scenario Builder, and then click OK.
- 4 Select File > Open Project. The Open Project dialog box displays.
- 5 In the Open Project dialog box, select the project file named Session_1617, and then click Open.

Note—If you do not have access to this file, simply view the screens provided in this user's guide to follow along with the procedure.

- 6 Create a new scenario: Choose Scenario > New Scenario, name the scenario Lab_2, and click OK.
- 7 Choose Topology > Import> Device Configuration Files... The Import Device Configurations dialog box opens.
- 8 Specify import settings:

Note—The Import Device Configurations dialog box retains its settings from the previous import; the following steps will direct you based on the retained settings in the dialog box from the previous procedures in this chapter.

- 8.1 Keep the checkbox for Cisco (IOS, CatOS, PIX) checked.
- 8.2 Click the Browse button for Cisco Router IOS and select the folder:

 $\label{eq:linear} C: \end{tabular} C: \end{tabular} Data \end{tabular} Projects \end{tabular} Session_1617 \end{tab}_2 \end{tabular} Cisco_R outers$

- 8.3 Keep the checkbox for Juniper (JunOS) checked.
- 8.4 Click the Browse button for Juniper JunOS and select the folder:

C:\Netwars\User_Data\Projects\Session_1617\Lab_2\Juniper _Routers

- 8.5 Toggle off the import option Generate Import Log.
- 8.6 Keep the Create PVCs option checked.
- 8.7 Check that the dialog box appears as follows:

* Import Device Configurations	×					
- Import Mode						
Replace entire model						
C Merge with existing model						
C Reimport configurations for selected devices						
O Reimport configurations for modified devices						
Specify Directories Containing Device Configuration Files						
Cisco (IOS, CatOS, PIX) C:\Netwars\User_Data\Projects	Session_1617\Lab_2\Cisco_Routers Browse					
✓ Juniper (JUNOS) C:\Netwars\User_Data\Projects\	Session_1617\Lab_2\Juniper_Routers Browse					
Import Options	Model Assistant Files					
Create nodes to represent external ASes	✓ Use the following model assistant files:					
Create nodes to represent edge LANs	<click add="" to=""></click>					
Create PVCs	_					
Generate import log						
	Import Cancel Help					

Figure 3-17 Import Device Configurations dialog box

- 9 Import:
 - 9.1 Click the Import button.

9.2 After import of the network model, the following dialog box displays:



Figure 3-18 Open Import Assistant

The Open Import Assistant dialog box displays automatically when the import process detects that all of the necessary information cannot be found within the device configuration files. The Import Assistant requests, but does not require, that you provide supplemental information.

9.3 Click Open. The following dialog box displays:

🛨 Import Assistant		
Show: Routers with unnumbered interfaces]	
Select interface A to connect or specify data rate:	Select interface B to connect:	
Boston_Bkup_IDC	Connect/disconnect selected interfaces: Disconnect Apply data rate to selected interfaces: DS0	X
व	Legend: SSE Needs data SSE OK (modified) SSE OK	*
Eind Selected Routers in Project Editor	Save changes Apply changes QK	Cancel



End of Procedure 3-5

Procedure 3-6 Use Import Assistant to Connect Interfaces and Specify Data Rates

1 Connect unnumbered interfaces.

- **1.1** Make sure that the **Show** pull-down menu is set to **Routers with unnumbered interfaces.**
- **1.2** In the interface A pane, click on the (+) sign next to the router icon for **Boston_Bkup_IDC** to expand the view of the router to include its name and interfaces.

Select interface A to connect or specify data rate:								
E- <mark>-</mark>	Boston Bkup	IDC			A			
	Name	Data Rate	Connected to	Shutdown				
E- 🚾	🛛 Serial2/1	2.688 Mbps	<unconnected></unconnected>	no				
	- (<ip td="" unnumb<=""><td>ered>) to NY</td><td></td><td></td><td></td></ip>	ered>) to NY						

Figure 3-20 Unnumbered Interfaces

Note that the interface description appears and reads "to NY". The interface description is populated in the table to provide extra information useful in connecting unnumbered interfaces.

- 1.3 In the interface A pane, select the unnumbered interface, Serial2/1 of Boston_Bkup_IDC; in the interface B pane, an entry appears for NY_Pri_IDC.
- **1.4** In the interface B pane, expand the view of router **NY_Pri_IDC** and select interface **Serial2/2**.
- 1.5 Click Connect.

The two interfaces are connected as the interface disappears from the right pane; the icons in the interface A pane change from red (Needs data) to light green (OK, modified).



Figure 3-21 Modified Interfaces

2 Specify unknown data rates.

2.1 Set the **Show** pull-down menu to **All devices**. The following dialog box appears showing all devices in the network model:

∐mport A	ssistant			
Show:	All devices		Y	
	Atlanta Boston_Bkup_IDC Name ATM1/0 FastEthernet3/0 FastEthernet3/1 FastEthern	Data Rate <n a=""> SONET/OC3 100 Mbps 2.688 Mbps 2.688 Mbps T1 2.015 Mbps <n a=""> <n a=""></n></n></n>	Connected to <loopback> 10_10_13_0/30(+) <unconnected> <unconnected> Genuity.Serial0/0 NY_Pri_IDC.Serial <unconnected> 10_10_12_0/30(+) <subinterface> <subinterface></subinterface></subinterface></unconnected></unconnected></unconnected></loopback>	Apply data rate to selected interfaces: DS0 Apply
	Leenuity Houston LA London NY_Pri_IDC Paris cc	Editor	 	Legend: Needs data DK (modified) changes. <u>QK</u> <u>Cancel</u>

Figure 3-22 Import Assistant Showing All Devices

Notice that most devices are green (OK), the connected unnumbered interfaces are light green (OK, modified), and only the device named **DC** is red (Needs data).

- 2.2 Set the Show pull-down menu to Devices with unspecified interface data rates.
- **2.3** In the window, click on the (+) sign next to the router icon for DC to expand the view of the router to include its name and interfaces.

2.4 Select interface at-0/1/0.

K Import A	ssistant			
Show:	Devices with unspecified interfation of the default data rate will be assi	ace data rates 📃		
	DC Name Data Rate at-0/1/0 SONET/DC3 (10.10.3.1/30)	Connected to 10_10_13_0/30(+)	Shu no	Apply data rate to selected interfaces: DS0 Apply
■ Eind Se	lected Devices in Project Editor		Save ch	Legend: Needs data OK (modified) OK anges Apply changes QK

Figure 3-23 Import Assistant with at-0/1/0 Selected

Note that the default data rate for the ATM interface is specified as SONET/OC3. If no supplemental information is provided, ATM interfaces default to SONET/OC3 data rates.

- 2.5 Choose the data rate SONET/OC1 from the Data Rate pull-down menu, and click Apply; the icons change from red (Needs data) to green (OK, modified).
- 3 Save changes to Model Assistant file.
 - 3.1 Click Save changes...
 - 3.2 Specify the filename to be *session1617_links_and_data_rates*, and click OK.
 - **3.3** Click **OK** in the Import Assistant dialog box to apply the changes to the network model.
- 4 Import Summary (Concise) displays. Click Close. We will come back to this in a later procedure.
- 5 Choose File > Save Project to save project.

End of Procedure 3-6

Procedure 3-7 Apply Model Assistant File to Move Nodes from Logical to Geographic Positions

The network model created has nodes placed in logical locations (non-geographic) -i.e., nodes "London", "LA" etc., appear next to each other instead of being placed in correct geographic location (as indicated by their names).

- **1** Duplicate the scenario:
 - 1.1 Choose Scenario > Duplicate Scenario.
 - **1.2** Name the new scenario *Lab_2b*, and click **OK**.
- **2** To position them geographically:
 - 2.1 Choose Topology > Model Assistant > Apply File...

米 Select	a Model Assistant File to Apply	×
Filename:	kclick to select>	
		-
	<u> </u>	<u>C</u> ancel

Figure 3-24 Select a Model Assistant File to Apply dialog box

- 2.2 Click <click to select> and choose *session1617_geographic_locations* from the popup list.
- 2.3 Click OK.
- 3 View the network model.
- 4 Choose File > Save Project to save project.

End of Procedure 3-7

Procedure 3-8 Export Site Locations and Hierarchy for Re-use in Future Imports

- 1 Export hierarchy and location information to Model Assistant file:
 - 1.1 Choose Topology > Model Assistant > Save Current Topology to File.
 - 1.2 Choose to export Locations (X/Y coordinates), Threshold (displayed icon size), and Subnet hierarchy.
1.3 Verify that the dialog box reads as below, and click **Save**.



Figure 3-25 Model Assistant Conversion dialog box

- **1.4** Leave the name of the MA file to *Session_1617-Lab2b-ma_export,* and click **Save**.
- 2 Re-import using Model Assistant file.
 - 2.1 Choose Topology > Import > Device Configuration files...
 - Under Model Assistant Files, click on <click to add> and choose session1617_links_and_data_rates.
 - Again click on <**click to add**> and choose Session_1617-Lab_2b-ma_export.
 - 2.2 Check that the dialog box appears as follows:

* Import Device Configurations	X			
Import Mode				
Replace entire model				
C Merge with existing model				
C Reimport configurations for selected devices				
C Reimport configurations for modified devices				
Specify Directories Containing Device Configuration Files	Specify Directories Containing Device Configuration Files			
Cisco (IOS, CatOS, PIX) C:\Netwars\User_Data\Projects\Session_1617\Lab_2\C	isco_Routers Browse			
✓ Juniper (JUNOS) C:\Netwars\User_Data\Projects\Session_1617\Lab_2\Ju	uniper_Routers Browse			
Import Options Model Assistant Files				
Create nodes to represent external ASes 🔽 Use the following r	nodel assistant files:			
Create nodes to represent edge LANs session1617_links_and_data_rates				
Create PVCs Session_1617-Lab	o2b-ma_export			
Generate import log <click add="" to=""></click>				
Import	<u>Cancel</u> <u>H</u> elp			

Figure 3-26 Import Device Configuration dialog box

- 2.3 Click Import, and notice that no additional information was requested.
- 2.4 Click Close in the Import Summary (Concise) dialog box.
- 2.5 Choose File > Save Project to save the project.

End of Procedure 3-8

Apply the Model Assistant File after the Import

The geographical layout is only one method of viewing the network model. The network can also be viewed in a logical layout.

Procedure 3-9 Apply the Model Assistant File after the Import

- 1 Choose Scenario > Switch to Scenario, and choose scenario Lab_2.
- 2 Choose Topology > Model Assistant > Apply File ...

米 Select	a Model Assistant File to Apply	×
Filename:	<click select="" to=""></click>	
	<u> </u>	<u>C</u> ancel

Figure 3-27 Select a Model Assistant File to Apply dialog box

- 3 Click <click to select> and choose *session1617_logical_locations* from the popup list.
- 4 Click OK.
- 5 Choose File > Save Project.

The network now looks as follows:



Figure 3-28 Sample Network

Conclusions

The import process sometimes requires supplemental information such as interface data rates and device locations that do not exist in the device configuration files. You used the Import Assistant to provide connectivity for unnumbered interfaces and to provide data rates for interfaces. You used the Model Assistant to introduce subnet hierarchy into the network model, and your task required using the Model Assistant to place devices both logically and geographically. Finally, you learned how to switch quickly and easily between two views of the network by using the Model Assistant in a manner independent of the import process.

Incremental Import: Selected Devices Re-import

A network model is given which might have some configuration errors. Your job is to detect such errors in the network and clear them by modifying the device configuration files or by using the virtual command line interface (Virtual CLI). The modified files are to be reimported to create a network model that has no configuration errors.

Find Configuration Errors

Procedure 3-10 Find Configuration Errors

- 1 Launch NETWARS, if not already opened.
- 2 From the System Editor's File menu, choose Open Editor.
- 3 From the Open Editor drop-down menu, choose Scenario Builder, and then click OK.
- 4 Do one of the following:
 - **4.1** If you haven't completed all the steps in the previous section of this chapter:
 - Select File > Open Project. The Open Project dialog box displays.
 - In the Open Project dialog box, select the project file named Session_1617_ref, and then click Open.
 - 4.2 If you have completed all the steps in the previous section of this chapter:
 - Select File > Open Project. The Open Project dialog box displays.
 - In the Open Project dialog box, select the project file named Session_1617, and then click Open.

Note—If you do not have access to this file, simply view the screens provided in this user's guide to follow along with the procedure.

- 5 Choose Scenario > Switch to Scenario and select scenario Lab_2.
- 6 Duplicate the scenario:
 - 6.1 Choose Scenario > Duplicate Scenario.
 - 6.2 Name the new scenario *Lab_3* and click **OK**.
- 7 Detect configuration errors:
 - 7.1 Choose NetDoctor > Configure/Run NetDoctor.
 - 7.2 Select all the rules in the Rule Suites > IP Addressing.
 - 7.3 Expand the rule suite IP Routing, and select Inconsistent Metric Components rule.

7.4 Click Run.

Configure/Run NetDoctor	
Template: Default NetDoctor Report	-
Report title: NetDoctor Report	
Rules Settings Notification	
IGRP	
P Addressing	
- Classless Subnet Mask for Classful Routing Protocol	
- Duplicate Address	
Invalid Interface IP Address	
Invalid Subnet Mask	
Uverlapping Subnets	
Peers In Different Subnets	
P Multicast	_
P IP Routing	
Inconsistent Metric Components	
Inconsistent Routing Protocols	
Interface Not Advertised by Router	
Mismatched Interface MTU	
H Multiple Next Hops to Destination (Requires Simulation Output)	-21
<u> </u>	

Figure 3-29 Configure/Run NetDoctor

NetDoctor shows one configuration error and one warning.



Figure 3-30 NetDoctor Report's Rules Section

7.5 Click on each of them to see more details about the error/warning.

7.6 Error: IP Addressing: Duplicate Address: - two interfaces in the network are using the same IP address 10.2.1.3.

IP Addressing: Duplicate Address			
All active interfaces should have unique addresses. Having duplicate addresses in a network may cause incorrect routing.			
NOTE: This rule will report problems in a network even if there is a valid reuse of addresses e.g., a network using NAT.			
Tested: Addresses of all interfaces in the network			
ERROR Configuration	The following 2 interfaces have the same address "10.2.1.3/32": • LA[Loopback0] • SF[Loopback0] Both interfaces are active.		

Figure 3-31 IP Addressing Error

7.7 h. Warning: IP Routing: Inconsistent Metric Components: - two peer interfaces are having inconsistent bandwidth or delay metrics.

IP Routing: Inconsistent I	Metric Components
----------------------------	-------------------

When using EIGRP, IGRP, or OSPF, peer interfaces should have consistent bandwidth and delay metrics. Inconsistent metrics may cause asymmetric routing.



Figure 3-32 IP Routing Error

7.8 Close the browser window that shows the NetDoctor report.

We will first fix the Duplicate Address error by modifying the configuration file and then work on the inconsistent metric warning using the Virtual Command Line Interface (Virtual CLI).

End of Procedure 3-10

Procedure 3-11 Clear Configuration Errors

- 1 Locate problem devices:
 - 1.1 Choose Protocols > IP > Addressing > Select Node with a Specified IP Address.
 - **1.2** Enter **10.2.1.3**, and click **Find**.

Two nodes *LA* and *SF* are shown to have duplicate IP addresses on their loopback interfaces.

Node Name	Interface
DCI Network.LA	Loopback0
DCI Network.SF	Loopback0

Figure 3-33 Nodes with Duplicate IP Addresses

Click **OK** to close the dialog box that shows the nodes having duplicate IP addresses.

- 1.3 Click Cancel to close the IP Address-based Node Selection dialog box.
- 2 Right-click on router SF and select View Device Configuration Source Data.
- **3** Scroll down to line number 48 in the file.
- 4 Change the IP address of interface **Loopback0** from 10.2.1.3 to 10.2.1.1.

46	!
47	interface Loopback0
4.8	ip address 10.2.1.1 255.255.255.255
49	no ip directed-broadcast
50	1
51	interface EthernetO
52	ip address 10.2.4.1 255.255.255.0
53	no ip directed-broadcast
54	1
55	interface SerialO
56	no ip address
57	no ip directed-broadcast
58	encapsulation frame-relay
59	no ip mroute-cache
60	bandwidth 2015
61	1

Figure 3-34 Device Configuration Source Data

5 Choose File > Save Project, and close Edit Pad.

End of Procedure 3-11

45

Procedure 3-12 Re-import Modified Configuration Files

- 1 Select Topology > Import > Device Configuration files...
- 2 Select the Reimport configurations for modified devices import mode.
- 3 Deselect model assistant files, if any are selected, by unchecking the checkbox Use the following model assistant files.

4 Make sure your settings display as shown below:

🛞 Import Device Configurations	×	
- Import Mode		
C Replace entire model		
C Merge with existing model		
C Reimport configurations for selected devices		
Reimport configurations for modified devices		
Specify Directories Containing Device Configuration Files		
Cisco (IOS, CatOS, PIX) C:\Netwars\User_Data\Projects\S	Session_1617\Lab_2\Cisco_Routers Browse	
✓ Juniper (JUNOS) C:\Netwars\User_Data\Projects\S	Session_1617\Lab_2\Juniper_Routers Browse	
Import Options	Model Assistant Files	
Create nodes to represent external ASes	Use the following model assistant files:	
Create nodes to represent edge LANs	<click add="" to=""></click>	
Create PVCs		
C Generate import log		
	Import Cancel Help	

Figure 3-35 Import Device Configuration dialog box

- 5 Click Import.
- 6 The Import Summary (Concise) displays. Click Close.

Procedure 3-13 Verify that Configuration Errors are Cleared

- 1 Run NetDoctor:
 - 1.1 Choose NetDoctor > Configure/Run NetDoctor.
 - 1.2 Make sure all the rules in the Rule Suites > IP Addressing are selected.
 - **1.3** Make sure the **Inconsistent Metric Components rule** under rule suite **IP Routing** is also selected.
 - 1.4 Click Run.
- 2 Verify that NetDoctor reports zero errors and one warning message in the web report. We will fix this warning using the Virtual Command Line Interface (Virtual CLI).
- 3 Close the browser window that shows the NetDoctor report.

End of Procedure 3-13

Virtual Command Line Interface

Virtual CLI emulates Cisco's CLI so that Cisco configuration commands can be entered for NETWARS models. This interface is only available for NETWARS node models created from Cisco IOS and CatOS configurations.

Procedure 3-14 Use Virtual CLI

- 1 Verify the correctness of the NetDoctor warning message, by observing the following attribute at the nodes Atlanta, interface Serial0/1 and US_Partner, interface Serial0/0.
 - **1.1** Go under the **IP** attributes group: IP Routing Parameters > Interface Information > Metric Information > Bandwidth.

To fix this warning message, the bandwidth metric of one of the peer interfaces has to be changed. We will fix the problem at the interface Serial0/1 at Atlanta.

- 2 The command that you enter on a router to change the bandwidth is "*bandwidth values*" in the interface configuration mode.
- 3 Right-click on the router Atlanta and select Open Virtual CLI...

The dialog box that appears is the virtual command line interface and Cisco commands can be entered as you enter them on the real Cisco device.

- 4 At any point you can also make use of the auto-fill and list supported commands feature by pressing Tab or typing a ?.
- 5 Press Enter, and type en to enter the enable mode.
- 6 Type show running-config, and press Enter.
- 7 Press Enter or <space bar> to scroll down to the interface configuration for *Serial0/1*.
- 8 Note that the bandwidth command has a value of 200000 which is not same as its peer's value (2048).

🛨 Yirtual Command Line Interface: Atlanta	×
! interface Serial0/1	-
description to US_Partner serial 0/0 bandwidth 2000000	
ip address 10.3.4.1 255.255.255.252	
ip policy route-map from_us_partner	
ip access-group 100 out	

Figure 3-36 Virtual Command Line interface

- 9 Enter q or any character to exit the show running config output.
- 10 Type config t and press Enter to enter configuration commands from the terminal.

- 11 The interface of interest to us is *Serial 0/1*, so type in *interface Serial0/1* and press Enter to enter the interface configuration mode.
- 12 Type bandwidth 2048, and press Enter.
- **13** Type **Exit** to leave the interface configuration mode.
- 14 Type Exit to leave of the configuration mode and save the changes.
- 15 Click Close to leave the Virtual Command line interface.

Atlanta#config t Enter configuration commands, one per line. End with CNTL/Z. Rerun simulation if changes are made to the router's configuration. Atlanta(config)#interface Serial 0/1 Atlanta(config-if)#bandwidth ? <1-10000000> Bandwidth in kilobits Atlanta(config-if)#bandwidth 2048 Atlanta(config-if)#exit Atlanta(config)#exit Atlanta#
Copy Paste Close Help

Figure 3-37 Virtual Command Line interface

16 Verify that the bandwidth attribute was indeed changed by observing the attribute "IP.IP Routing Parameters. Interface Information. Metric Information. Bandwidth" at the router Atlanta for the interface Serial0/1.

End of Procedure 3-14

Procedure 3-15 Verify that Warnings are Cleared

- 1 Run NetDoctor:
 - 1.1 Choose NetDoctor > Configure/Run NetDoctor.
 - **1.2** Make sure all the rules in the **Rule Suites > IP Addressing** are selected.
 - **1.3** Make sure the **Inconsistent Metric Components rule** under rule suite **IP Routing** is selected.
 - 1.4 Click Run.
- 2 Verify that NetDoctor reports zero errors and zero warning messages in the web report.

End of Procedure 3-15

Conclusions

The NetDoctor module can be used to detect configuration errors in a network model. You cleared configuration errors reported by NetDoctor by editing a device configuration file and using virtual command line interface

DCI's import mode **Reimport configurations for modified devices** is useful when configurations change for some select devices in the network. You used this mode to reimport the modified configuration for a single node that had a configuration error. This mode results in considerable savings in time when only a small part of a large network is changed.

Troubleshooting the Imported Network

A configuration file set is given which might have some missing information that is leading to unconnected islands in your network. Your job is to detect such issues and fix them.

Find Configuration Errors

Procedure 3-16 Find Configuration Errors

- 1 Launch NETWARS, if not already opened.
- 2 From the System Editor's File menu, choose Open Editor.
- From the Open Editor drop-down menu, choose Scenario Builder, and then click OK.
- 4 Select File > Open Project. The Open Project dialog box displays.
- 5 In the Open Project dialog box, select the project file named Session_1617, and then click Open.

Note—If you do not have access to this file, simply view the screens provided in this user's guide to follow along with the procedure.

- 6 Choose Scenario > New Scenario, name the scenario Lab_4, and click OK.
- 7 Choose Topology > Import> Device Configuration Files... The Import Device Configurations dialog box opens.
- 8 Specify import settings:
 - 8.1 Keep the checkbox for Cisco (IOS, CatOS, PIX) checked.
 - 8.2 Click the **Browse** button for Cisco Router IOS and select the folder:

C:\Netwars\User_Data\Projects\Session_1617\Lab_4\Origina l_Configs

8.3 Uncheck the Juniper (JunOS) checkbox.

- **8.4** Make sure the import option **Create PVCs** is checked.
- **8.5** Toggle off the import option **Generate Import Log**.
- 9 Import:
 - 9.1 Click the Import button.

Import Summary (Concise) displays. The summary says there are 2 devices with missing CDP Information and 1 device with missing the show version information.

Also, observe in the background that there are 3 unconnected islands in the network.

🛞 Import Summary (Concise)		<u>_ ×</u>
Device Information		-
Number of Devices Successfully Imported	8	
Number of Files Skipped	0	
Missing Information		
Missing CDP information	2 devices	
Missing version information	1 device	-
View Details	<u> </u>	

Figure 3-38 Import Summary (Concise) dialog box

9.2 Click View Details...

Detailed summary shows us a number of useful information in determining the status of the import and, for troubleshooting.

- 9.3 Notice that the log says, devices *c5500_DC_switch1* and *c5500_DC_switch3* have no CDP information and device *c6500_DC_gw1* does not have version info.
- 9.4 Close the summary log.

The imported network looks like.



Figure 3-39 Sample Network

9.5 Right-click on the device *c6500_DC_gw1* and select Edit Attributes. Notice the make of the device.

Kc6500_DC_gw1) Attributes	Ş	<u>_ </u>
Type: router switch	Make: Cisco Systems Generic	
Attribute	Value	<u> </u>
🕐 _ name	c6500_DC_gw1	
(?) - model	layer3_switch_e2_fe12_fr_dc	

Figure 3-40 Attributes dialog box

9.6 Close the dialog box.

10 Examine the topology diagram below, provided to us by the network admin for the above network.



Figure 3-41 Sample Network Topology Diagram

Comparing it with our imported network, we see that there are 3 discrepancies in our import.

- The device c5500_DC_switch1_RSFC is the routing module for the c5500_DC_switch1 and should appear in the network as one device.
- Device *c5500_DC_switch3* and *c5500_DC_switch1* should have been connected to *c6500_DC_gw1*.
- Device c6500_DC_gw1 should have been brought in as Cisco 6500 model.
- 11 Identify the cause for the problems above.
 - Why is the routing module not connected to its switch?

DCI identifies the router (MSFC) and switch coupling based on the CDP neighbor information available on the switch or the MSFC card.

CAUSE: From the import summary, we know that device *c5500_DC_switch1* is missing the output from "show cdp" command.

Right click on the device *c5500_DC_switch1* and choose View Device Configuration Source Data and note that there is no "show cdp" information . • Why is the layer two connectivity between three devices missing? Or how can DCI infer layer 2 connectivity?

DCI can infer layer 2 connectivity only based on the CDP neighbor information.

CAUSE: From the import summary, we know that device *c5500_DC_switch3* is also missing the "show cdp neigh" information.

Right-click on the device *c5500_DC_switch3* and choose View Device Configuration Source Data, and note that there is no "show cdp" information.

• How can DCI identify the device type and make? Or what information is needed for DCI to identify the device type and make?

DCI identifies the device type based on the "show version" information.

CAUSE: Again, from the import summary, we know that the device *c6500_DC_gw1* is missing "show version" information.

Right click on the device *c6500_DC_gw1* and choose View Device Configuration Source Data and note that there is no "show version" information.

End of Procedure 3-16

Procedure 3-17 Providing the Missing Information

- **1** To fix the problems, we must include the missing information in the config files:
 - 1.1 Add "show cdp neighbors" output to both *c5500_DC_switch1* and *c5500_DC_switch2*.
 - 1.2 Add "show version" output to *c6500_DC_gw1*.

Note—For this example, we have added the outputs of these commands to the configuration files and have provided the modified config files.

- 2 Import the modified configurations:
 - 2.1 Choose Scenario > New Scenario, name the scenario Lab_4b, and click OK.
 - 2.2 Choose Topology > Import> Device Configuration Files... The Import Device Configurations dialog box opens.
 - 2.3 Specify import settings:
 - Keep the checkbox for Cisco (IOS, CatOS, PIX) checked.
 - Click the **Browse** button for Cisco Router IOS and select the folder:

C:\Netwars\User_Data\Projects\Session_1617\Lab_4\Modif ied_Configs

- 2.4 Click Import.
- 3 Import Summary (Concise) displays. Note that there is no missing information.



Also, observe that we now have a completely connected network.



End of Procedure 3-17

Conclusions

The concise import summary provides us a brief summary and lets us evaluate the status of the configuration import. The detailed summary provides more specifics about the devices with missing information. You used this information to troubleshoot an unconnected network, by providing the missing information.

4 Importing Network Traffic Data with MVI

Introduction

The Multi-Vendor Import (MVI) module enables users to leverage real-world traffic data and build accurate and efficient models by importing time-varying link and PVC load data as well as end-to-end flow data from various data sources.

This chapter covers the different types of traffic data that can be imported using MVI: link and pvc baseline loads and end-to-end traffic flow data. Users will perform traffic flow and link/pvc baseline load imports and learn about the workflow options available when performing network analyses using data from various sources, such as:

- Concord eHealth (link/pvc loads)
- HP Openview Performance Insight (link/pvc loads)
- MRTG (link/pvc loads)
- InfoVista (link/pvc loads)
- Cisco Netflow (traffic flows)
- NetScout Manager/nGenius (traffic flows)
- Cflowd (traffic flows)
- Distributed Sniffer (traffic flows)
- Fluke Networks OptiView
- ASCII Text Files (link/pvc loads or traffic flows)

Note—The following examples were presented at OPNETWORK 2004 in Session 1619, Importing Network Traffic Data with MVI. If you do not have access to the files that these procedures use, you can still follow along using the sample screens provided in this user's guide.

Examining Loads and Flows

The following procedure shows you how to examine background load and flow data in an existing network. Specifically, you will examine background load on a link and a PVC, visualize link loads gain, and examine a traffic flow using the Flows Browser.

Procedure 4-1 Examine Loads and Flows

- 1 Launch NETWARS, if not already opened.
- 2 From the System Editor's File menu, choose Open Editor.
- From the Open Editor drop-down menu, choose Scenario Builder, and then click OK.
- 4 Select File > Open Project. The Open Project dialog box displays.
- 5 In the Open Project dialog box, select the project file named 1619, and then click Open.

Note—If you do not have access to this file, simply view the screens provided in this user's guide to follow along with the procedure.

5.1 If the scenario is not set to Lab1, choose Scenario > Switch to Scenario and select Lab1.



Figure 4-1 Sample Network

- 6 Right-click on the link going to the **pixfirewall** node.
- 7 Select Edit Attributes.
- 8 Double click on the **Background Load** attribute value (...).

9 Double click on Atlanta-pixfirewall (Atlanta --> pixfirewall). Note the following profile editor:

\star Profil	e: Atlanta	-> pixfirewall_60					×
Profile na	me: Atlanta	> pixfirewall_60					
<u> </u>	m X intervals						seconds/step
🔽 Use s	tart time	10:55:42.000 Jul 16 2	004				
seconds	bits/second			bits/s	econd		[
0.0	89.64864864	486		200			
3,605	75.04244105	541					
7,213	75.98447893	357		100 🕁	may me	_	<u> </u>
10,813	95.53555555	556					
14,413	101.8755555	556		0			
17,999	101.8605688	379		Auto.			
21,601	103.8956135	548		620.22			
25,213	107.8870431	189		74 F	4		
28,812	99.06751875	552					
32,413	109.8961399	961		E Channada			
00.040	1400 100000		Ľ	J▼ Show cale	noar (me		
<u>E</u> xpo	t <u>I</u> m	port				<u>o</u> k	<u>C</u> ancel

Figure 4-2 Profile Editor for Atlanta-pixfirewall

- 10 Click Cancel (three times) to close all the object editor dialog boxes.
- 11 Select View > Visualize Link Loads > Color by Link Load... The Color Links by Load dialog box displays.

🛨 Color Links by Load		×
Color links based on data from Baseline Link Utilization	using the peak utilization for each link	
Each link will be colored according to its individual peal links will not necessarily coincide to the same network	k baseline link load. Note that the peak values for all time.	- -
	DK Cancel Apply Cjear	

Figure 4-3 Color Links by Load dialog box

12 Set the drop-down list boxes to **Baseline Link Utilization** and **peak utilization for** each link, and then click OK.



Figure 4-4 Sample Network with Colored Links

Links are colored based on static background utilization.

13 Place the mouse cursor over the red link.

13.1 Note the utilization in the 10_10_12_0/30(+) --> NY_Pri_IDC is at 87.39%

- 14 Select View > Visualize Link Loads > Clear Visualization.
- **15** Right-click on any flow going from DC to PE2 and choose **Hide Similar Demands**. This hides the flows, so we can more easily see the PVC demands.

You should now see the following network:



Figure 4-5 Sample Network with Hidden Flows

- 16 Right-click on Boston_Bkup_IDC/ATM1/0 <-> DC/at-0/1/0 and choose Edit Attribute.
- 17 Double click on Traffic Information (...).
- 18 Double click on Boston_Bkup_IDC --> DC (Boston_Bkup_IDC --> DC).
- **19** Observe the PVC background load profile:

Horofile: Boston_Bkup_IDC> DC_62					
Profile name: Boston_Bkup_IDC> DC_62					
Uniform X intervals	seconds/step				
☑ Use start time 10:55:39.000 Jul 16 2	2004				
seconds bits/second	bits/second				
0.0 65,521.8855219	- 80,000 AD - 41				
3,605 60,172.5381415					
7,213 60,574.556541	40,000				
10,813 67,262.222222					
14,413 70,553.8888889					
17,999 68,368.9347462	4.6.				
21,601 71,167.4069961	i de la companya de				
25,213 73,313.3997785	The Alt				
28,813 73,287.2222222					
32,413 70,059.444444	T Cham calandar line				
Export Import	<u> </u>				

Figure 4-6 Profile Editor for Boston_Bkup_IDC-DC

- 20 Click Cancel to close the profile editor and attribute editor dialog boxes.
- 21 Press Ctrl+M to show all demands and flows. You should see the following network:



Figure 4-7 Sample Network Showing All Demands and Flows

- 22 Right-click on Core (172_20_1_5)-->DC (192_168_50_10), and choose Edit Attributes from the first flow on the popup list.
- 23 Double-click on Traffic (bits/second), and observe the following profile:



Figure 4-8 Profile Editor for Core (172_20_1_5)-->DC (192_168_50_10)

- 24 Click Cancel.
- 25 Double-click on Traffic (packets/second), and observe the following profile:

Uniform X intervals					
seconds	packets/second		nd		
0.0	0.0069444444444	0.06			
10	0.0414272030651				
68	0.0069444444444	0.03			
189	0.0208333333333				
549	0.0069444444444	0.00			
608	0.023611111111	2 73	7.		
720	0.0166666666667	1200	30		
788	3.46944695195E-018	12 W	14		



- 26 Click Cancel twice.
- 27 Select Traffic > Visualize > Open Flows Browser. The Flows Browser dialog box displays.
- 28 Select Flows in the Arrange by drop-down list box.
- 29 Click on Atlanta (10_10_6_1)-->DC (192_168_50_10).



Figure 4-10 Sample Network in Flows Browser

The flow is rendered in the network window and the profiles are displayed.

30 Select Connections in the Demand Type drop-down list box.

	×
Model: All	Technology: All
Adlaria Housian ISanchia SF LA Botton, Bkup, Joc C5509 10,10,13,008(+) PE1 20, DC	Parts
4,000 bits/second 60,000 2,000	bits/second
	Model All Carling and the second of the seco

31 Click on DC/at-0/1/0_2 <-> PE1/ATM1/0_1.

Figure 4-11 Sample Network in Flows Browser

The PVC is rendered in the network window and the profiles are displayed.

End of Procedure 4-1

Importing Link Loads

In the following procedure, imagine that you work for a small ISP and want to present a graphical representation of your network traffic to your supervisor. You have collected link load data during a period of heavy traffic using InfoVista. The following procedure shows you how to import link load data and visualize link loads.

Procedure 4-2 Import Link Loads

- 1 Launch NETWARS, if not already opened.
- 2 From the System Editor's File menu, choose Open Editor.
- From the Open Editor drop-down menu, choose Scenario Builder, and then click OK.
- 4 Select File > Open Project. The Open Project dialog box displays.

5 In the Open Project dialog box, select the project file named 1619, and then click Open.

Note—If you do not have access to this file, simply view the screens provided in this user's guide to follow along with the procedure.

5.1 If the scenario is not set to Lab2, choose Scenario > Switch to Scenario and select Lab2.



Figure 4-12 Sample Network

- 6 Verify that links are not currently loaded.
 - 6.1 Hold cursor over link between Atlanta-Access and 192_168_50_64/29.
 - 6.2 Note that tooltip shows no utilization.
- 7 Import loads.
 - 7.1 Select Traffic > Import > Device/Link Baseline Loads > From InfoVista...
 - 7.2 Import the file.
 - If C:\Netwars\User_Data\Traffic_Data is not expanded, do so.
 - Choose the file infovista 20-jul-2002.txt.

• Click Import.

★ Import Baseline Loads from Info¥ista Reports	_ 🗆 ×
Select data source(s):	
□ □ □ C:\Netwars\User_Data\Traffic_Data	A
infovista 20-jul-2002.txt	
1	
Add Directory Add Server Remove	
Time Range	
• All data	
C Data from past 24 hours	
C Data from past week	
C Data from past month	
C From time: Ceanliest in file>	
To time: < atest in file>	
Rollup	
Enable rollup	
Represent each 15 minute 🔽 interval by the maximum 🔟 among all values 💌 in the	hat interval.
☑ Overwrite existing data	
Save settings on importImportIoseSave Settings	Help

Figure 4-13 Import Link Baseline Loads from InfoVista Reports dialog box

- 8 Visualize Link Utilizations and Loads.
 - 8.1 Examine the import log.
 - When import statistics appear, click View Log.

🛞 Traffic Load Summary		
Traffic span imported	18:11:00.000 Aug 23 2001 to 18:30:00.000 Aug 23 200	1 🔺
Network Start Time	18:11:00.000 Aug 23 2001	
Total Number of Traffic Log Files	1	
Number of Traffic Files Imported with No Errors	0	
Number of Lines Skipped Due to Errors	40	
Total Number of Links in Network	34	
Number of Links Affected by Import	32	
	View Log	Close

Figure 4-14 Traffic Load Summary dialog box

The only skipped lines are Loopback interfaces.

- Close the log and statistics windows.
- **8.2** Use visualization to inspect the network.
 - Select View > Visualize Link Loads > Color by Link Load... The Color Links by Load dialog box displays.

• Set the drop-down list boxes to **Baseline Link Utilization** and **peak utilization for each link,** and then click **OK**.



Figure 4-15 Sample Network with Colored Links

- 9 Examine Load Attributes.
 - **9.1** Hold the cursor over the link between Atlanta-Access and 192_168_50_64/29. Note that the link has utilization.
 - **9.2** Right-click on this link, and choose **Edit Attributes**.

9.3 Expand the Background Load attribute.

*	(Atlanta-Access / Serial0/0 (192_168_50_65) <-> 192_16	8_50_64/29) Attributes
Γ	Attribute	Value 🔺
0	name	Atlanta-Access / Serial0/0 (192_168_50_65) <->
) - model	ppp_adv
0) 🖃 Background Load	()
0	Average Packet Size (bytes) [Atlanta-Access -> 192_168_5	Default
	Average Packet Size (bytes) [192_168_50_64/29 -> Atlant	Default
	Intensity (bps) [Atlanta-Access -> 192_168_50_64/29]	Atlanta-Access> 192_168_50_64/29
	Lintensity (bps) [192_168_50_64/29 -> Atlanta-Access]	192_168_50_64/29> Atlanta-Access
	Propagation Speed	Speed of Light
0) 🖵 data rate	4,632,000
		V
1		•
Γ	Apply changes to selected objects	☐ A <u>d</u> vanced
Γ	<u>Find Next</u>	<u> </u>

Figure 4-16 Background Load Attribute

- **9.4** View the profile of throughput vs. time.
 - Click on the Value column for the Intensity (bps) [Atlanta-Access 192_168_50_64/29] attribute and choose Edit...

★ Profile: Atlanta-Access> 192_168_50_64/29_30							
Profile na	Profile name: Atlanta-Access> 192_168_50_64/29_30						
☑ Iniform × intervals 60 seconds/step							
🔽 Use s	start time	18:11:00.000 Aug 23 2001					
second	s bits/second	bits/second					
0.0	893,013.702	2 1,200,000					
60	851,162.424	4					
120	834,519.184	48 800,000	-				
180	868,334.174	44					
240	843,627.086	64 400,000	-				
300	851,258.074	48					
360	884,946.610	08 🔟 0					
420	834,282.489	96 v a					
480	872,737.353	36 ⁶ -3 4					
540	878,486.128	88 70%					
600	873,337.197	76					
660	835,853.432	24					
720	024 404 070	ac 🔄 🗹 Show calendar time					
<u>E</u> xpo	rt <u>I</u> m	mport	<u>C</u> ancel				

Figure 4-17 Profile Editor for Atlanta-Access-192_168_50_64/29

- Also examine the throughput in the opposite direction. Notice that the load out of Atlanta-Access is about 850Kbps, but the load into Atlanta-Access is about 2.7Mbps.
- **9.5** Close the load profiles when you have finished examining them.
- 10 Examine Node Interface Aliases.
 - **10.1** Make sure the Edit Attributes dialog box is still open for the link between **Denver-Core** and **Other-ISP-2**.

10.2 Click the Advanced checkbox.

<mark>≭]</mark> (Denver-Core / FastEthernet3/0 (192_1	168_50_34) <-> Other-ISP-2 / FastEthernet0/ 💶 🗖 🗙			
Attribute	Value			
⑦ ⊢ name	Denver-Core / FastEthernet3/0 (192_168_50_34) <-> Other			
(?) - model	100BaseT			
(?) - creation source	Object Palette			
(?)	Unknown			
⑦ - creation data				
⑦ Background Load	[]			
Image: A standard stand Standard standard stand Standard standard stand Standard standard stand Standard standard stand Standard standard standard standard standard standard standard standa	head and tail			
① - color	black			
⑦ – delay	Distance Based			
⑦ – financial cost	0.00			
Ine style	solid			
Image: The second se				
③ – symbol	none			
⑦ └ thickness	1			
Bedefine Path Extended Attrs. Node A Interface Aliases Node B Interface Aliases				
Apply changes to selected objects 🔽 Advanced				
Eind Next				

Figure 4-18 Edit Attributes dialog box

10.3 Click on Node A Interface Aliases.

★ Denver-Core / FastEthernet3/0 (192_168_50_34) <-> Other-ISP-2 / FastEthernet0 🗴				
<u>File Edit Options</u>				
<u>りにおる。</u>				
1 [FP:192.168.50.34 2 IFName:FastEthernet3/0 3	4			
	× •			
	Line: 1			

Figure 4-19 Node A Interface Aliases

Notice aliases for IP address and interface name (SNMP ifDescr).

10.4 Close these dialog boxes when you are done.

End of Procedure 4-2

Summary

You have now imported and visualized link loads. You can report on certain links of interest, or visually show how heavily loaded the network is currently.

You could go on to convert these loads to flows to perform further studies. Alternatively, you could add explicit traffic or traffic flow data to perform studies.

Importing Traffic Flows and Running Flow Analysis

Using the following procedure, imagine that you work for SuperBroadCom, a service provider. Your company is looking to add AllFirstTrust National Bank of Iowa as a client. You have existing load data for your network, and AllFirstTrust has Netflow data representing their existing traffic during a busy hour. Your company wants to determine the total load on their network due to adding AllFirstTrust's traffic. Thus, you need to overlay AllFirstTrust's Netflow traffic on top of your already-loaded network and run Flow Analysis to determine the impact of this new traffic.

Procedure 4-3 Visualize and Inspect Link Loads

Before importing the traffic flows, you will want to examine the current load on the network to anticipate where problems might occur.

- 1 Launch NETWARS, if not already opened.
- 2 From the System Editor's File menu, choose Open Editor.
- 3 From the Open Editor drop-down menu, choose Scenario Builder, and then click OK.
- 4 Select File > Open Project. The Open Project dialog box displays.
- 5 In the Open Project dialog box, select the project file named 1619, and then click **Open**.

Note—If you do not have access to this file, simply view the screens provided in this user's guide to follow along with the procedure.

5.1 If the scenario is not set to Lab3, choose Scenario > Switch to Scenario and select Lab3.



Figure 4-20 Sample Network

Note the PVC demands (purple dashed lines for Frame Relay, dark green dashed lines for ATM) created by the topology import, in addition to the links.

6 Select View > Visualize Link Loads > Color by Link Load... The Color Links by Load dialog box displays.

6.1 Set the drop-down list boxes to **Baseline Link Utilization** and **peak utilization for each link**, and then click **OK**.



Figure 4-21 Sample Network with Colored Links

Note that the link between **NY_Pri_IDC** and **layer2_switch_32** is heavily loaded going toward **NY_Pri_IDC**.

7 Right-click on this link and choose Edit Attributes.

★ (NY_Pri_IDC / Serial2/1 <-> layer2_switch_32) Attributes				
Attribute	Value			
⑦ ⊢ name	NY_Pri_IDC / Serial2/1 <-> layer2_switch_32			
(?) - model	FR_link_adv			
⑦ Background Load	()			
Average Packet Size (bytes) [NY_Pri	Default			
Average Packet Size (bytes) [layer2	Default			
(?) Intensity (bps) [NY_Pri_IDC -> layer2	NY_Pri_IDC> layer2_switch_32			
Intensity (bps) [layer2_switch_32 -> N	NY_Pri_IDC			
⑦ – DLC Identifier	16			
Provide the second s	Enabled			
Propagation Speed	Speed of Light			
① L data rate	2,015,000			
	*			
Apply changes to selected objects	Advanced			
<u>Find Next</u>	<u> </u>			

Figure 4-22 Edit Attributes dialog box

Note the data rate of 2,015,000.

8 View the traffic profile from layer2_switch_32 NY_Pri_IDC.

米 Profi	ile: layer2_switch_32> NY_Pri_II	DC_1
Profile n	ame: [layer2_switch_32> NY_Pri_IDC_	1
🔲 <u>U</u> nife	orm×intervals	seconds/step
🔲 Use :	start time 17:42:18.000 Jul 27 2004	ļ
second	s bits/sec	bits/sec
0.0	1,603,154.15	2,000,000
301	1,599,958.36	1 500 000
601	1,603,522.895	1,300,000
900	1,605,554.015	1,000,000
1,201	1,589,141.84	
1,501	1,603,397.965	500,000
1,801	1,601,679.17	
2,101	1,602,894.215	
2,400	1,602,658.46	0h 8h 16h 24h
2,701	1,599,714.545	Show calendar time
0.004		
<u>E</u> xpo	ort Import	<u> </u>

Figure 4-23 Profile Editor for layer2_switch_32-NY_Pri_IDC

Note that the traffic is about 1,600,000 bps: about 80% utilization.

9 Close these dialogs and choose View > Visualize Link Loads > Clear Visualization.

End of Procedure 4-3

Procedure 4-4 Import Traffic Flows

- 1 Choose Traffic > Import Flows > From Cisco Netflow Traffic Data...
- 2 Expand the directory in the tree view to see all available files.

🛨 Traffic Flows Import	
Traffic archive directories:	Probe Information
□ lab3 flows	T Host:
↓ Iab3 flows\10.0.0.1.0945	Media:
	Device:
	Start:
	End:
	Interval:
ab3_flows\10.0.0.2.0959	Traffic Selection
lab3_flows\10.0.0.2.1015	From: j
	_models
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	flows
Iab3_flows\10.2.1.3.1030	100ws(10.0.0.2.1015
	Traffic Options
	Multiple archive alignment: Align based on time stamps
lab3_flows\10.3.1.1.1015	Anakin ananima ata Manimum
lab3_flows\10.3.1.1.1030	
L HM lab3 flows\10.3.1.2.0945	Traffic preprocessor: None
Selected archives:	Import threshold: 0.0 octets/sec
C:\op_models:lab3_flows\10.0.0.1.0945	Aggregation Options
C:\op_models:lab3_flows\10.0.0.1.0959	Aggregate by: IP Address
C:\op_models:lab3_flows\10.0.0.1.1015	Include Type of Service in Aggregation
C:\op_models:lab3_flows\10.0.0.1.1030	
C:\op_models:lab3_flows\10.0.0.2.0945	
C:\op_models:lab3_flows\10.0.0.2.0959	IV snow demands upon import
	Import Save Cancel

3 Double-click on the directory to choose all files.



4 Click Import.

5 Once the import completes, you should see the following import statistics.

Traffic span imported	04:01:00.000 D	ec 01 2002 to 05:30:00.000 Dec 01 2002	
Network Start Time	04:01:00.000 D	ec 01 2002	1
Total Number of Files	48		
Number of Files with Errors	2		
Number of Files Not Imported	0		
Total Number of Lines	10,968		
Number of Lines with Errors	0		
Number of Flows Imported	744		
Total Traffic Imported	37.16Gb		
Total Packets Imported	7,813,889.48		
Files Imported without Errors			
C:\op_models\lab3_flows\1	2.0.1.2.0945		
C:\op_models\lab3_flows\1	0.0.0.1.0945		
C:\op_models\lab3_flows\1	0.0.0.1.0959		
C:\op_models\lab3_flows\1	2.0.1.2.0959		
C:\op_models\lab3_flows\1	0.4.1.2.0959		
C:\op_models\lab3_flows\1	0.4.5.2.0959	-	
C:\op_models\lab3_flows\1	0.3.1.1.0959	Files Imported without Errors	
C:\op_models\lab3_flows\1	0.3.1.1.0945	C:\op_models\lab3_flows\10.4.1.2.0959	
C:\op_models\lab3_flows\1	0.3.1.3.0959		
C:\op_models\lab3_flows\1	0.4.1.1.0945		
C:\op_models\lab3_flows\1	0.3.1.2.0959		
C:\on_models\lab3_flows\1	0 0 0 2 0945		
J			

Figure 4-25 Traffic Flow Import Statistics

6 Click Close.

The traffic flow demands are visible in the network topology.



Figure 4-26 Sample Network with Traffic Flow Demands

End of Procedure 4-4

Procedure 4-5 View Flows Using the Flows Browser

The Flows Browser is a convenient way to view flows or connections in the network at a high level.

1 Choose Traffic > Visualize > Open Flows Browser.

By default, the Flows Browser opens showing nodes that are the source of at least one flow in the pane on the left.



2 Expand **DC** to see the flows originating at this node.

Figure 4-27 Sample Network in Flows Browser

3 Click on the flow *DC* (10_1_4_4) *ATT* (12_1_1_2). This is the fifth flow listed under DC. This shows the bits/second and packets/second profiles for this flow. Note that there is a constant level of traffic in this flow from about 1,500 seconds to about 5,000 seconds.
3.1 You can click on other flows to see that the traffic is not always constant, and sometimes the traffic-monitoring tool leaves small gaps in the measured traffic.



Figure 4-28 Sample Network in Flows Browser

- 4 You can also change how the network objects are displayed. Change the **Arrange by:** pull down menu so that the objects are arranged by flows.
- 5 Click on the first flow: *Atlanta (10_10_12_2) DC (192_168_50_10)*. Expand its item in the tree view to see its source and destination nodes.



Figure 4-29 Sample Network in Flows Browser

6 Click Close to close the flows browser.

End of Procedure 4-5

Procedure 4-6 Run DES

Now that the network has both the existing load data and the new flow data, you are ready to analyze the total traffic on your network to determine if it can handle the combined loads.

- 1 Choose DES > Configure/Run Discrete Event Simulation.
- 2 Change the **Duration** to **3600 seconds**.
- **3** Click **Run** to start DES.
 - **3.1** When prompted about unassigned IP addresses, you can click **Yes** or **No**. You will get the same results with either. This only changes whether IP addresses automatically assigned during flow analysis are set back on the nodes as attributes.
- **4** When viewing results, notice that there is now an over-utilized link with a maximum utilization of 147%.

End of Procedure 4-6

Procedure 4-7 Find the Over-Utilized Link

- 1 Choose DES > Results > Find Top Statistics...
- **2** Expand Link Statistics, then point-to-point, and select Utilization.

3 Click Find Top Statistics.

🛞 Top Objects: point-to-point.utilization					×	
All objects in 'DCI Network'						
Object Name	Minimum	Average /\	Maximu	Std Dev		
NY_Pri_IDC / Serial2/1 <-> layer2_switch_32 <	0	125.88	137.69	53.390		
ATT / Serial0/0 (12_0_1_2) <-> NY_Pri_IDC / Serial2/0 (12_0_1_1) <	0	82.86	87.26	37.780		
London / Serial0/0 <-> layer2_switch_32>	0	76.35	84.02	32.215		
London / Serial0/0 <-> layer2_switch_32 <	0	60.86	67.15	25.626		
Paris / Serial0/0 <-> layer2_switch_32>	0	60.74	67.03	25.572		
NY_Pri_IDC / Serial2/1 <-> layer2_switch_32>	0	53.06	58.80	22.272		
SanDiego / Serial0 <-> layer2_switch_32 <	0	52.76	58.49	22.139		
ATT / Serial0/0 (12_0_1_2) <-> NY_Pri_IDC / Serial2/0 (12_0_1_1)>	0	50.77	58.16	23.996		
Euro_Partner / Serial0/0 (10_4_5_2) <-> Paris / Serial0/1 (10_4_5_1)>	0	38.07	43.85	15.787		
SF / Serial0 <-> layer2_switch_32 <	0	30.84	38.65	13.589		
SF / Serial0 <-> layer2_switch_32>	0	30.83	38.64	13.587		
Boston_Bkup_IDC / Serial2/0 (4_0_2_1) <-> Genuity / Serial0/0 (4_0_2	0	21.90	23.66	10.094		
Atlanta / Serial0/0 <-> layer2_switch_32>	0	19.21	21.28	8.089		
Atlanta / Serial0/0 <-> laver2_switch_32 <	0	19.17	21.24	8.067	-	
Report on top 10 statistics whose Graphs 9	Graphs Stacked 💌 🗛 Is		▼ <u>G</u> raph			
Average				<u>I</u> ext Report		
☐ Ignore views				Eind Object		

Figure 4-30 Find Top Statistics

As you can see, the NY_Pri_IDC / Serial2/1 layer2_switch_32 link is overloaded. Also, ATT / Serial0/0 (12_0_1_2) NY_Pri_IDC / Serial2/0 (12_0_1_1) is nearly overloaded.

End of Procedure 4-7

Summary

You have found that your network will not be able to handle the additional traffic generated by AllFirstTrust. You have several possible solutions, assuming you still want to add this client. You can upgrade the links that will be at or near overloading. You could also attempt to change the routing on your network to redistribute some of the additional traffic to avoid overloads.