

EVALUATION GUIDE

Traverse™

5.1



zyrion
Business Service Assurance

© 2009 Zyrion, Inc. (www.zyrion.com) All rights reserved. Zyrion, Traverse and the Zyrion logo are registered trademarks of Zyrion, Inc. and/or its affiliates in the United States and/or other countries. All other registered and unregistered trademarks herein are the sole property of their respective owners. Zyrion, Inc. reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs.

About Traverse

Zyrion's Traverse is a breakthrough Business Service Management application that provides real-time visibility into the performance of IT services. Traverse's innovative Service Container technology enables IT and business personnel to create unique virtual views of discrete business services. Traverse facilitates decentralized remote infrastructure management that is pro-active and preventive rather than reactive, giving all employee levels the control and information they require based on their specific responsibilities and permissions. Traverse provides an easy-to-use Web-based user interface and is a distributed, scalable, real-time, and easy-to-manage platform.

Contacting Zyrion

Customer Support

You can reach Zyrion technical support online:

<http://www.zyrion.com/support>

Telephone

In the US: **877-7-ZYRION (877-799-7644)**

Outside the US: **+1 408-524-7424**

Email

support@zyrion.com

User Forum

To join a customer-driven user group connecting the worldwide community of Zyrion users, visit our online forum:

<http://community.zyrion.com/>

Contents

About Traverse	ii
Contacting Zyrion	ii
Overview and Installation	3
About This Guide	3
Traverse Architecture	3
System Operation	3
Traverse Installation	3
Installation Checklist	3
Supported Platforms	4
Minimum Hardware Requirements	4
Installing Traverse	4
Basic Configuration	7
First-time Startup	7
Logging in to the Traverse Web Application	7
Manually Adding New Devices	8
Running Network Discovery	9
Creating Actions and Schedules	9
Adjusting Thresholds	12
Generating Reports	12
Ad Hoc Reports (My Reports)	14
Scheduling Automatic Reports	14
Advanced Topics	15
Service Containers	15
Creating a Service Container that Contains Devices	15
Creating a Service Container that Contains Tests (Virtual Device)	16
Nesting Service Containers	18
Examining Service Container Status	18
Creating Dashboards	18
Panorama Topology Display	21
Creating an SLA Measurement	22
Event Manager & Message Handler	23
Federated Security Model	23
Configuring Network Flow Analysis	24
Enabling the Traverse Integrated NetFlow Collector	24
Enabling NetFlow on a Cisco Router (or switch running IOS)	24
Using the Network Flow Analysis Console	25
Extensible APIs	28
BVE FlexAPI	28
Plugin Monitors & Plugin Actions	28

1. Overview and Installation

1.1 About This Guide

This guide is intended for users who are doing an evaluation of Zyrion Traverse. It gives a quick overview of installing the software in your environment and all of its key features.

NOTE: Managed Service Providers (MSPs) should review the "*MSP User Guide*" available from Zyrion's support web site.

1.2 Traverse Architecture

The Traverse system comprises the following three components:

- **Business Visibility Engine (BVE):** An embedded object-oriented database that stores all configuration information, including metadata related to user authentication, devices, tests, thresholds for test results, action profiles and other key information. The BVE FlexAPI, which allows access to the BVE for provisioning and results, also operates on this server.
- **BVE WebApp:** Provides the Web-based user interface into Traverse. It correlates the data from multiple DGEs, and allows end users to look at the real-time status of their devices, add new devices and actions, and execute reports, using a simple Web browser. It manages the distributed databases and distributed processing while generating the real-time reports and graphs. You can have more than one BVE Web application for load sharing.
- **Data Gathering Engines (DGE):** Performs the actual polling of data, receives SNMP traps, generates alarms based on thresholds, and does the aggregation of data in real time. DGEs should be located as close as possible to the devices being monitored to reduce wide area network traffic. The DGEs can be geographically dispersed or you can have multiple DGEs in the same location to distribute the load across different physical servers. When you have multiple DGEs in the same location, the system automatically provisions new devices onto the DGE with a lower number of devices.

In a large environment, Zyrion recommends that each component reside on its own physical host server, but for a small trial with up to 500 devices, you can install all components on a single host.

1.3 System Operation

Each component of Traverse operates independently to provide a high level of scalability and fault tolerance. When you start a DGE, it connects to the BVE and downloads the entire configuration associated with its unique name, including tests, thresholds and actions.

After this process completes, the DGE performs tests, generates events when thresholds are crossed, and triggers the corresponding notifications. The data collected by each DGE is stored in a local SQL database on the DGE itself.

When a user logs into the Web application, the system searches the configuration database for the list of devices that the user has permission to view. The Web application then connects directly to the distributed DGEs and gets the real-time status of the services or devices. When the user needs a report, the Web application fetches the data using parallel queries from the distributed DGEs and generates the reports in real time.

1.4 Traverse Installation

Installation Checklist

Prior to installing Traverse, you will need the following:

- 1 a dedicated hardware platform to install the Traverse software (see specifications and Supported Platforms below)
- 2 the read-only SNMP community ID (password) for your routers, switches and other SNMP enabled equipment (including UPS, SAN or NAS devices, etc.). This is also important for proper topology discovery.
- 3 The administrator password for your Windows servers so that they can be queried using WMI
- 4 ensure that the firewall ports have been opened in order for your Traverse server to query your IT infrastructure (see list of ports in the Traverse User Guide).

Supported Platforms

Windows

- Windows XP Professional with Service Pack 3
- Windows Server 2003 Standard and Enterprise x64 Edition
- Windows Vista

UNIX

- RedHat Enterprise Linux ES/AS 4 and 5 on x86 platforms
- CentOS 4 and 5 on x86 platforms
- Solaris 9 and 10 on UltraSparc platforms

Minimum Hardware Requirements

- 2GHz+ CPU on x86 platform (Windows and UNIX versions)
- 1.5GHz+ UltraSPARC III CPU on Sun Sparc platform (Solaris version)
- 4GB RAM (2GB if running DGE only)
- 18GB free disk space (SCSI or fast IDE)

NOTE: It is not recommended to install Traverse on a laptop, since laptop disk drives are generally not fast enough.

Installing Traverse

- 1 Download the latest version of the Traverse software from the Zyrion website at www.zyrion.com.
- 2 Make sure you are not running any other Web server on TCP port 80 on the Traverse host.
- 3 Make sure the Traverse host has a static IP address.
- 4 Make sure the Traverse host has access to an email relay for sending notifications.
- 5 Execute the installation file.
 - Windows:
Double-click **traverse-x.y.z-windows.exe**, and then follow the instructions.
 - UNIX:
You should be logged in as root.
Extract the installation package as follows (you must use GNU tar on Solaris):

```
gunzip -c traverse-x.y.z-platform.tar.gz | tar xpf -
```

Change to the directory containing the extracted files, execute the install script, and then follow the instructions:

```
cd traverse-x.y
./install.sh
```

- 6 If you are installing Traverse on Windows, you **must** reboot after the installation.

2. Basic Configuration

2.1 First-time Startup

- 1 Start Traverse and verify that all of the components started and are operating correctly.
 - Windows:
Start > Programs > Zyrion Traverse > Start Zyrion Traverse
The Traverse Service Controller reports the status of all the components.
 - UNIX:

```
cd /usr/local/traverse/etc  
./traverse.init start  
./traverse.init status
```
- 2 If some components do not start, check for the following common start-up problems:
 - Expired license key (send email to eval@zyrion.com to get a new key)
 - Another Web server using TCP port 80
 - Failure to reboot after Windows installation

You can also look for errors in the logs/error.log file in the Traverse directory.

NOTE: After identifying and fixing any problems related to component start-up, restart Traverse.

2.2 Logging in to the Traverse Web Application

- 1 Use your web browser to connect to http://your_host/ where your_host is the fully qualified host name or IP address of the server that the Traverse Web application is running on.



- 2 Log in using the default end-user name *zyrion* with password *zyrion*.
- 3 Set your time zone and other user preferences by navigating to Administration > Preferences.

2.3 Manually Adding New Devices

- 1 Navigate to Administration > Devices > Create a Device.

CREATE DEVICE
Select or complete the required fields below. Click 'Create Device' to confirm.
* - indicates a required field

* Type of Device: Select Device Type

* Device Name:

* Fully Qualified Host Name/IP Address:

Do Not Validate/Resolve Device Address

Comments/Description (optional):

Tag 1:

Tag 2:

Tag 3:

Tag 4:

Tag 5:

Automatically Clear Comment When In OK State:

Display Comment In Summary Screen:

* Create In Location: Default Location

Enable Smart Notification:

Enable Test Parameter Rediscovery:

Create New Tests After Creating This Device:

Create Device Dependency After Creating This Device:

Create Device Reset Cancel

- 2 Select the device type and provide the device name and IP address or fully qualified host name.
- 3 The tag fields can be used to give devices arbitrary tags that can be used to search for them later. For example, you might use a tag to record the location of the device (HQ or CHICAGO), or the function of the device (ROUTER or SWITCH). Add a device with a value for Tag 1 of "ROUTER" for use later in this evaluation.
- 4 Leave the "Create New Tests After Creating This Device" box checked and click **Create Device**.
- 5 To create tests for the new device, first select the type of tests. You can use built-in or user-defined Application Profiles (which auto-discover a filtered list of tests) or user-defined Monitoring Profiles (which define a specific list of tests), or you can manually choose which monitors and tests to add, in which case Traverse automatically discovers all monitors and tests for the device.
- 6 If you want to use SNMP (Simple Network Management Protocol) or WMI (Windows Management Instrumentation) monitors, you must enter the SNMP community string and port number or WMI domain username and password.
- 7 Once the device is added, it appears on the Administration > Devices page. Click **Tests** under the Modify column to manage all tests for that device. Then, click the icon under the Modify column next to a test to update the test parameters, such as the polling interval and the values for warning and critical thresholds.

- 8 Navigate to Status > Devices to view a status summary for all devices. From here click on a device name to drill down and see the status of the tests for that device, and then click on a test name to see details and graphs of short- and long- term history.

2.4 Running Network Discovery

You can also have Traverse search your network to automatically discover any devices, or just specific types of devices. You should also limit the subnets to be included in the discovery to class-C networks instead of class-B or larger.

- 1 Navigate to Administration > Other > Device Discovery & Import > New Network Discovery Session.
- 2 Enter the IP and netmask for each subnet you want to discover devices in. If you want to discover SNMP devices, enter the SNMP community string(s). If you check the "Discover physical connectivity (topology) between devices" box, Traverse will automatically map the relationships between devices.
- 3 Once discovery is complete, select and confirm the devices you want to provision, and then discover and select tests.

For information about displaying the discovered network topology, see [Panorama Topology Display on page 21](#).


2.5 Creating Actions and Schedules

When a test result crosses a threshold, Traverse takes action based on rules defined in Action Profiles. Some possible actions include sending email, sending SNMP traps, opening trouble tickets, or running an external script.


- 1 Navigate to Administration > Actions > Create an Action Profile.

- 2 Create an action profile with two levels of escalation. In this example, email is sent immediately to the admin when a test goes into warning, critical, or unknown state, and to the manager after a test is critical for 15 minutes during peak hours.

STATUS
DASHBOARD
REPORTS
ADMINISTRATION



DEVICES
CONTAINERS
SLA
ACTIONS
OTHER
PREFERENCES

Logged in: | [LOGOUT](#) | [ABOUT](#) | [USER GUIDE](#) | 

CREATE ACTION PROFILE

Enter the action profile name and then fill in information for the individual actions below. Click 'Create Action Profile' to confirm. *Note:* If your notification method is email, you can specify multiple recipients by separating their addresses with commas.

* - indicates a required field

* Action Profile Name:

Action Profile Description:

?

Action #1

Notify Using:

* Message Recipient: ?

Notify when test is in state: Ok: Warning: Critical: Unknown:

Notification should happen after: cycles

If this test stays in the trigger state, repeat this action: cycles

Schedule: [Manage Schedules](#)

Select DGE to test this action:

Action #2

Notify Using:

* Message Recipient: ?

Notify when test is in state: Ok: Warning: Critical: Unknown:

Notification should happen after: minutes

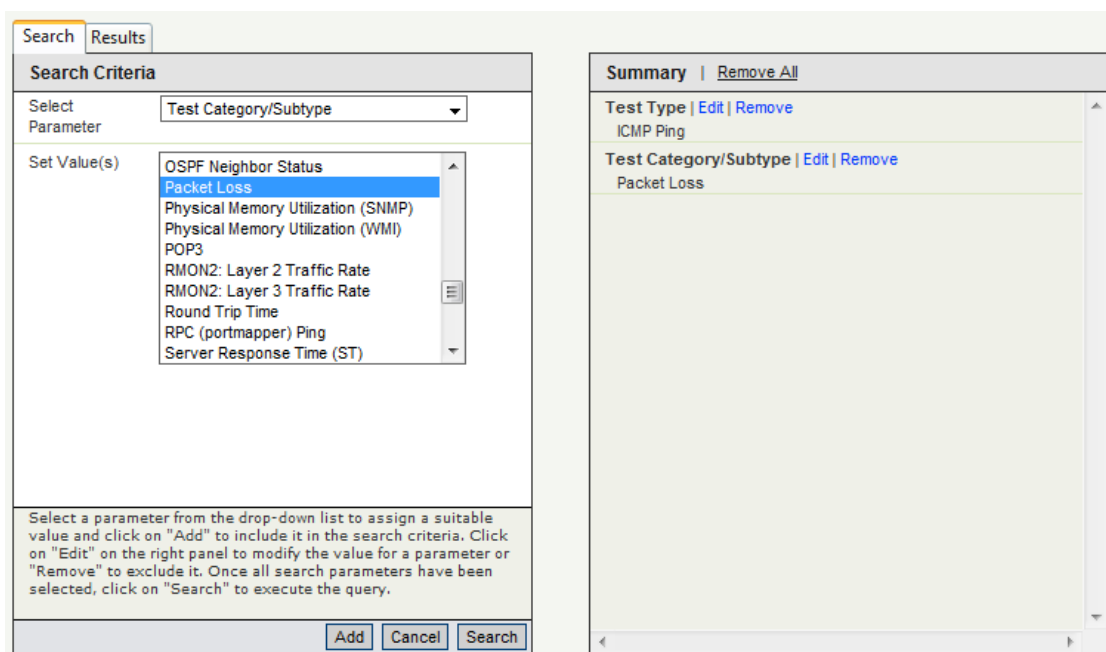
If this test stays in the trigger state, repeat this action: cycles

Schedule: [Manage Schedules](#)

Select DGE to test this action:

- 3 Click **Create Action Profile** to create the profile.
- 4 To assign this profile to tests, click **Assign to Tests** in the row where the new action profile now appears on the Manage Action Profiles page, and then click **Add**.

- Choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you like, and then click **Search**. In this example, you are assigning the new Notify Admin and Manager action profile to all ICMP Ping and Packet Loss tests.



- In the Results pane, select the devices whose tests you want to use the action profile, and then click **Assign Action Profile**.
- The Assign Action Profile page now lists all of the devices with tests to which this action profile is assigned, and if you click on a device, you can see the specific tests on that device that are using the profile.

By default, tests and actions run all the time, but you can control when they run by creating and assigning Schedules to them. For instance, you might want some tests and actions to run only during business hours.

- Navigate to Administration > Other > Custom Schedules > Create a Schedule.
- Enter "business hours" in the Schedule Name field, uncheck all the boxes for days and times that fall outside of business hours, and then click **Create Schedule**.
- To assign this schedule to a device, click **Select Devices For Schedule** in the row where the new schedule appears, and then click **Add**.
- Choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you like, and then click **Search**.
- In the Results pane, select the device you want to add, and then click **Assign Schedule**. The new schedule is assigned to all tests for that device.

You can also assign a schedule to specific tests through device administration.

- Navigate to Administration > Devices and click Tests in the row for the device whose tests you want to schedule.
- Click the Modify icon in the row for the test you want to schedule, and then use the drop-down Schedule menu to assign a schedule.

You can assign the new business hours schedule to the actions in your Action Profiles as well.

- Navigate to Administration > Actions and click **Update** in the row for the Action Profile you created.

- 2 For each action, use the drop-down Schedule menu to assign a schedule.

2.6 Adjusting Thresholds

Traverse comes with pre-defined thresholds for most metrics, but these warning & critical thresholds might be too low for your environment and require adjustments. If you have a small number of devices, and if you are seeing some devices in warning or critical state for long periods of time, you should click on the devices and increase the thresholds as needed.

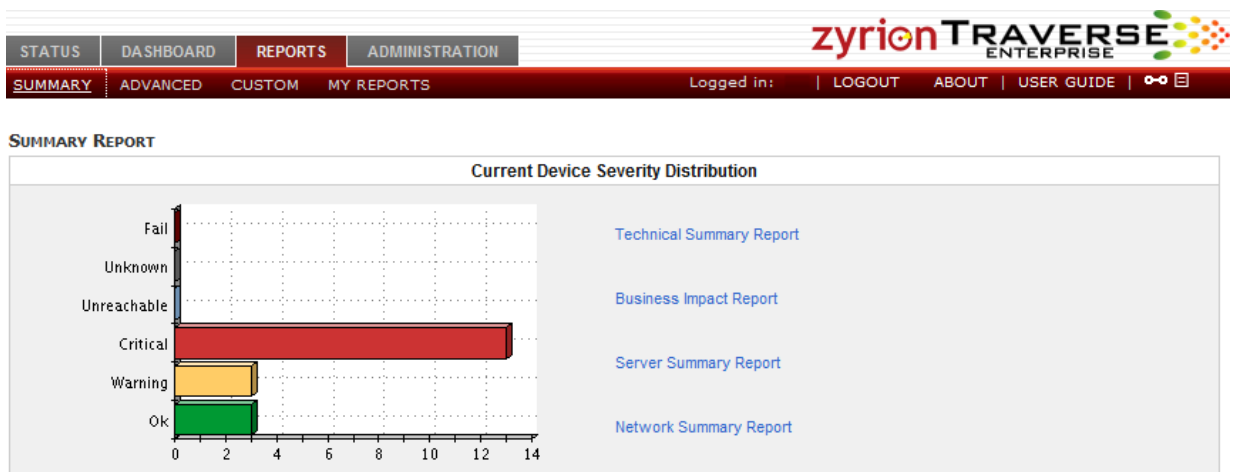
- 1 Click on *Status* > *Tests* from the main menu
- 2 Click once on the test name which is in red or yellow state to select that row. Note the current result, and then click on the "edit" icon on the top right menu.
- 3 On the *Update Test* page, change the warning threshold to be a little higher than the current value for the test that you noted earlier and a matching critical threshold (slightly higher than warning).
- 4 Click on the *Submit* button.
- 5 Repeat these steps for the remaining tests which are in warning or critical state.

If you have a large number of devices, you can use the "baselining" feature in Traverse to automatically adjust the thresholds based on the historical data collected (this is described in the *Traverse User Guide*). This option is under *Administration* > *Devices* > *Test Baseline Management*

2.7 Generating Reports

Traverse has extensive and flexible reporting generated in real time from data collected by the DGEs and then processed by the BVE reporting engine.

- 1 Navigate to *Reports* > *Summary* to view the built-in Technical Summary, Business Impact, Server Summary, Network Summary reports, which provide a quick snapshot for the past week.



- 2 Click **Advanced Reports** for specific operational reports on devices or containers. Select the type of report (Server, Network, Application, or SLA), and then specify the duration and devices and/or containers to include.

- 3 Click **Custom** for customizable Fault, Performance, Threshold Violation, and Messages reports.

CREATE CUSTOM REPORTS
Choose a report type

1) Fault Reports	: top 10 by number or duration of events (downtime), correlation histogram.
2) Performance Reports	: composite graphs, statistics from historical data, trend analysis.
3) Threshold Violation History	: display events for devices and test types between specified time interval.
4) Messages Report	: display messages for devices and message types between specified time interval.
5) Inventory Report	: statistics for device types and vendors

- 4 To create a custom performance report, click **Performance Reports**. In this example, you are creating a report that shows statistics and a composite line graph for CPU utilization.

CREATE PERFORMANCE REPORT
Select options to generate a performance report.

Duration:

Device Name/Regexp:

Container:
 All
 All ICMP Tests
 Application Performance
 CPU Fans
 Critical Services
 Custom Applications
 Email Service

Device:
 All
 Cisco Call Manager (Secondary)
 Cisco Call Manager - Primary
 Cisco Meeting Place
 Cisco Router
 Demo Reporting Engine
 Demo Server

Test Name:

Test Type:
 CISCO Memory Pool Utilization
 Compaq Array Controller Board Health
 Compaq Standard Equipment Status
 CPU Idle Time (SNMP)
 CPU Utilization (SNMP)
 CPU Utilization (WMI)
 Disk Space Utilization (SNMP)
 Disk Space Utilization (WMI)
 Fast To Fast Response Time (FTF)

Number of items:

Customize Report:

graphs

plot tests of same type on single graph

shown as individual lines

Reverse Counterpart (Allows you to plot the matching pair of "in" and "out", or "sent" and "received" tests (for example, network traffic or disk I/O tests) on opposite axis)

shown as sum

shown as average

use same scale for tests of same type


statistics table

trend analysis

- 5 Click **Run** to create the report.
- 6 You can save any report by clicking **Save Report Parameters**, and the saved query can be accessed from Administration > Other > Custom Report Queries.

Ad Hoc Reports (My Reports)

You can create and save your own Ad Hoc reports that combine components from different reports and make them easy to access.

- 1 Run a report, and then click on the  icon next to a component title to bring up the Add To My Reports dialog.
- 2 Name your Ad Hoc report in the Create A New Report field, and then click **Submit**.
- 3 Your saved report now shows up when you navigate to Reports > My Reports, where you can click the name of the report to run it.

Scheduling Automatic Reports

You can also schedule any saved report (saved query parameters or ad hoc reports) to execute automatically and email the results to a list of recipients.

- 1 Navigate to Administration > Other > Scheduled Reports For Email Delivery > Create A Scheduled Report.
- 2 Name your scheduled report in the Scheduled Report Name field, use the drop-down Generate Using Saved Query menu to select a saved report, and then enter the recipient(s) and define the schedule.

3. Advanced Topics

3.1 Service Containers

Service containers allow you to group tests and devices to create logical, business-oriented views of your network in addition to your hardware-oriented views. A service container can hold virtual devices (special types of containers that hold only tests), real devices, or other service containers.

Creating a Service Container that Contains Devices

- 1 Navigate to Administration > Containers > Create a Service Container.
- 2 In this example, you are creating a service container named Routers. Fill in the Service Container name, and then click **Next**.
- 3 Select **Devices & Containers** in the Container Will Include field.
- 4 You can assign devices to a container either by performing a search and manually selecting the devices to include, or by specifying rules and having the results automatically assigned to the container.

For this example, select **Automatically Based On Specified Rule** in the For Device Containers, Assign Devices field.

Choose Tag 1 in the selection_criteria drop-down menu, type "ROUTER" in the text field, click **Test This Rule** to see which devices will match the rule, and then click **Next Step**.

CREATE A SERVICE CONTAINER

Container: Routers

Click on 'Add' to search for suitable members for this container. If this is a test container, the search workflow can be used to select specific tests. Otherwise uncheck the 'All Tests' checkbox next to device name to remove individual tests. Click 'Next Step' to confirm.

* - indicates a required field

The screenshot shows a web form for creating a service container. The form is titled "CREATE A SERVICE CONTAINER" and has a sub-header "Container: Routers". Below the title, there is a paragraph of instructions: "Click on 'Add' to search for suitable members for this container. If this is a test container, the search workflow can be used to select specific tests. Otherwise uncheck the 'All Tests' checkbox next to device name to remove individual tests. Click 'Next Step' to confirm." Below this, there is a small asterisk and a note: "* - indicates a required field".

The form itself is divided into several sections:

- Service Container Name:** A text field containing "Routers".
- Container Will Include:** A radio button selection with three options: "Devices & Containers" (selected), "Tests (Virtual Device)", and "Manually By Selecting Items From List Below".
- For Device Containers, Assign Devices:** A radio button selection with two options: "Automatically Based On Specified Rule" (selected) and "Manually By Selecting Items From List Below".
- Devices matching following rules should be added to container automatically (applicable only for device containers):** This section contains a dropdown menu with "Tag 1" selected, a text field with "* ROUTER", and a "--remove--" button.
- Buttons:** "Add Another Rule" and "Test This Rule" (highlighted with a blue border).
- Rule Results:** A scrollable list box containing the following items: "Distributed Sniffer Probe", "Plano Corp Router", and "WAN Router".
- Bottom Buttons:** "Next Step", "Reset", and "Cancel".

- 5 Assign an action profile if desired, decide the criteria for determining the severity status of the container, and then click **Create Container**.

CREATE A SERVICE CONTAINER

Select the severity options for the container. Click 'Create Container' to create the container.

* - indicates a required field

Creating a Service Container that Contains Tests (Virtual Device)

- 1 Navigate to Administration > Containers > Create a Service Container.
- 2 In this example, you are creating a service container named All ICMP Tests. Fill in the Service Container name, and then click **Next**.
- 3 Select **Tests (Virtual Device)** in the Container Will Include field.

CREATE A SERVICE CONTAINER

Container: All ICMP Tests

Click on 'Add' to search for suitable members for this container. If this is a test container, the search workflow can be used to select specific tests. Otherwise uncheck the 'All Tests' checkbox next to device name to remove individual tests. Click 'Next Step' to confirm.

* - indicates a required field

- 4 You must manually select tests for a virtual device container. Click **Add** in the Selected Device box, and then build a filter that matches the devices or tests you want to find; choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you like, and then click **Search**. In this example, you are adding all ICMP Ping type tests.

The screenshot shows two panels. The left panel, titled 'Search Criteria', has a 'Select Parameter' dropdown set to 'Test Type'. Below it, a 'Set Value(s)' list contains various test types, with 'ICMP Ping' selected. A note at the bottom of this panel explains the search workflow. The right panel, titled 'Summary | Remove All', shows 'Test Type | Edit | Remove' and 'ICMP Ping' listed.

- 5 In the Results pane, select the devices whose tests you want to add, and then click **Add**. The Create a Service Container page now lists all of the devices with tests to be added to the new container, and if you click on a device, you can see the specific tests on that device that are included.

CREATE A SERVICE CONTAINER

Container: All ICMP Tests

Click on 'Add' to search for suitable members for this container. If this is a test container, the search workflow can be used to select specific tests.

Otherwise uncheck the 'All Tests' checkbox next to device name to remove individual tests. Click 'Next Step' to confirm.

* - indicates a required field

The screenshot shows the 'CREATE A SERVICE CONTAINER' page. The 'Service Container Name' is 'All ICMP Tests'. The 'Container Will Include' section has 'Tests (Virtual Device)' selected. The 'For Device Containers, Assign Devices' section has 'Manually By Selecting Items From List Below' selected. A list of devices is shown, with 'Cisco Call Manager - Primary' selected. A list of tests is shown, with 'Packet Loss' and 'Round Trip Time' selected.

- 6 Click **Next Step**, assign an action profile if desired, decide the criteria for determining the severity status of the container, and then click **Create Container**.

Nesting Service Containers

You can nest service containers to build a logical hierarchy of your environment. For example, you might have Routers, Switches, and Firewalls containers, all contained within a Network Devices container.

MANAGE SERVICE CONTAINERS
Create A Service Container

page 1 of 1 GO
name or perIpse SEARCH

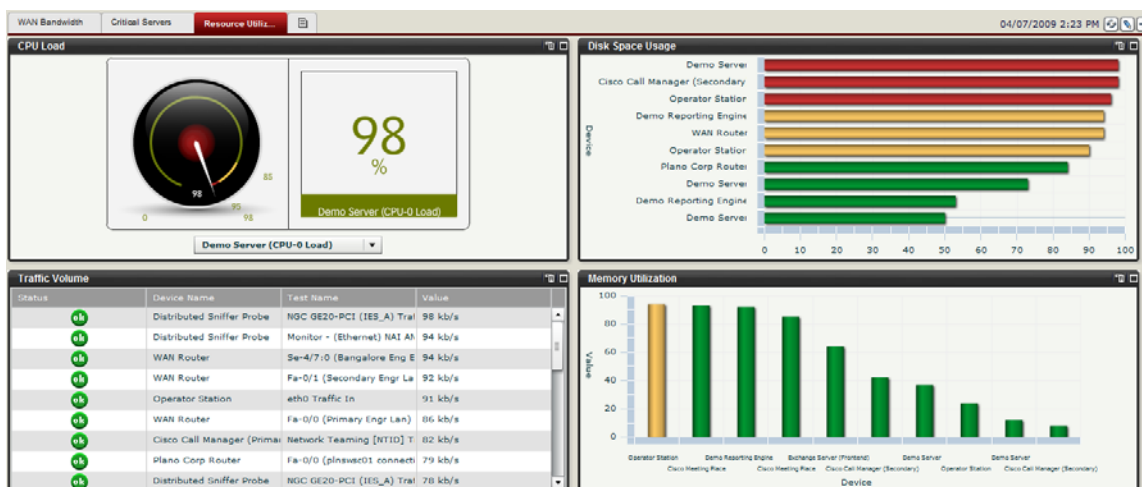
SERVICE CONTAINER	MODIFY
All ICMP Tests	Update Members Actions Delete
Critical Services	Update Members Actions Delete
Custom Applications	Update Members Actions Delete
Email Service	Update Members Actions Delete
Network Infrastructure	Update Members Actions Delete
Network Devices	Update Members Actions Delete
Firewalls	Update Members Actions Delete
Routers	Update Members Actions Delete
Switches	Update Members Actions Delete
Traverse Performance	Update Members Actions Delete
VoIP Infrastructure	Update Members Actions Delete

Examining Service Container Status

- 1 Navigate to Status > Containers to view a status summary for all containers.
- 2 Click on a container name to list its contents.
- 3 Drill down into the container hierarchy to reach a test container, and then click on the Run Reports menu to generate reports of Recent Events and Correlation.
- 4 Click on a test name to see its status page and access Long-Term History, Trend Analysis, and Raw Data reports.

3.2 Creating Dashboards

The RealView dashboard feature lets you create custom dashboards to view the performance of services and infrastructure. You can create multiple dashboards, each containing dashboard components related to a particular area of service you want to monitor.



- 1 Navigate to Dashboard > Create New Dashboard.

- 2 Enter a name for your dashboard and choose whether you want it to be visible to other users or private, and then click **OK**.
- 3 Click **Create New Chart/Table** in your new empty dashboard to open the Create Dashboard Component dialog.
- 4 In this example, you are creating a line chart component for traffic tests. Select the line chart component type icon, fill in the Title field, select the refresh interval, and then click **Apply**.

Create Dashboard Component

Component Type :

Title :
Traffic Test

Refresh :
0 5m 10m 15m 20m 25m 30m

Apply **Cancel**

- 5 Now specify the data source for the component. Select the devices and test types, and then click **Search** to find the matching tests. Select the tests you want the component to use by dragging and dropping them from the Matching Tests list to the Selected Tests list, and then click **Apply**.

Component Data Source

Object Type:
 Test Device Container

Selection Method:
 Manual Top 10

Device:
LAN Switch (1-6 Net)
LAN Switch (21-10 Net)
Operator Station
Oracle 10g Database
Plano Corp Router
WAN Router
Web/Application Server
Wireless Gateway

Test Type:
port
rpc
snmp
wmi


Test SubType:
Network Interface: Packets Discarded (SNMP)
Network Interface: Packets Transmitted (S
Network Interface: Traffic Volume (SNMP)
Number of Processes (SNMP)

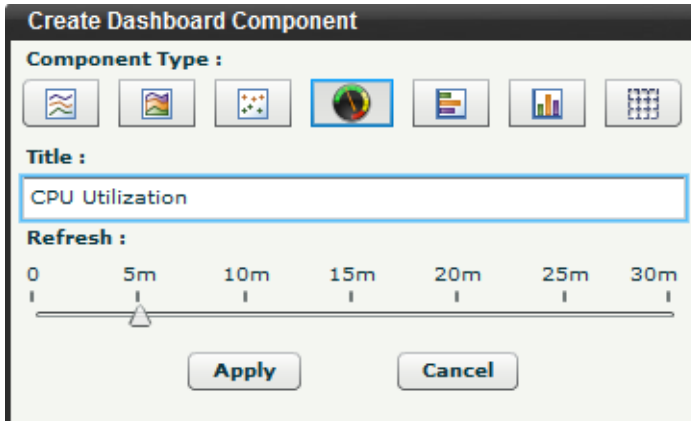
Matching Tests:
Plano Corp Router - Fa-0/0 (plnswsc01 conne
Plano Corp Router - Fa-0/0 (plnswsc01 conne

Selected Tests:

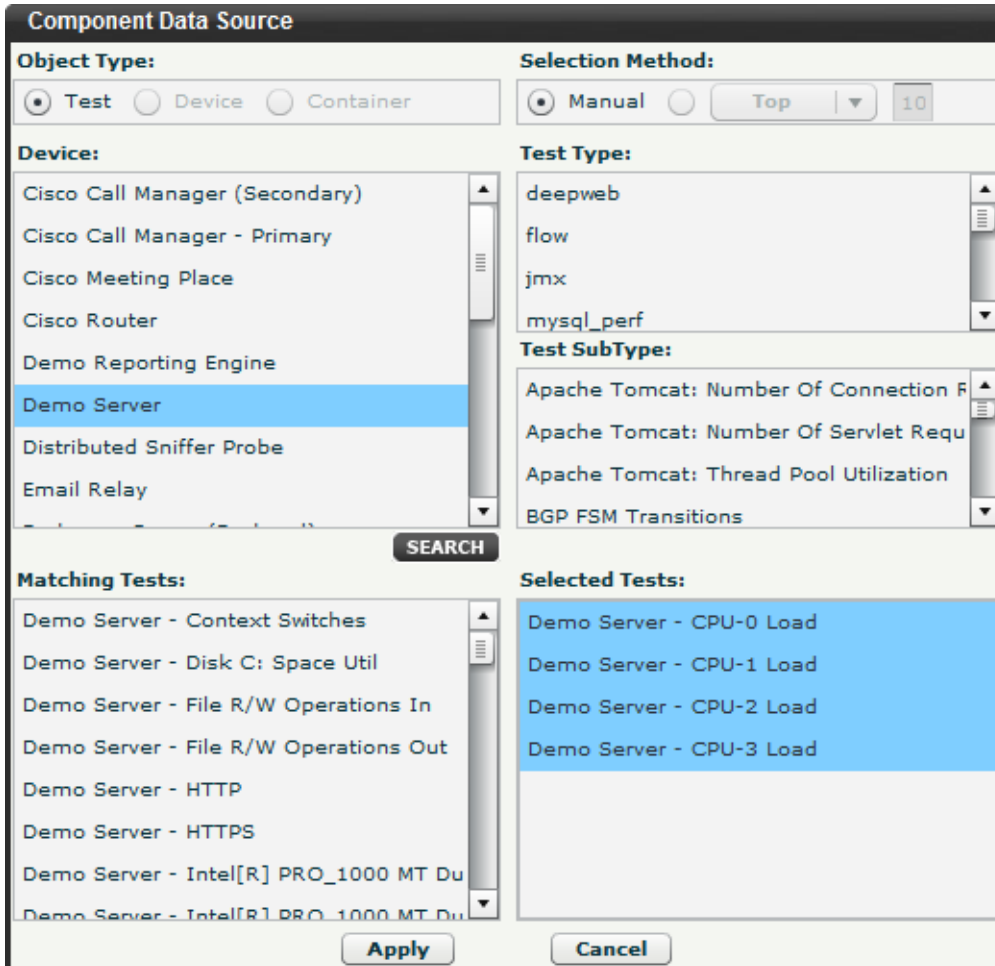
SEARCH

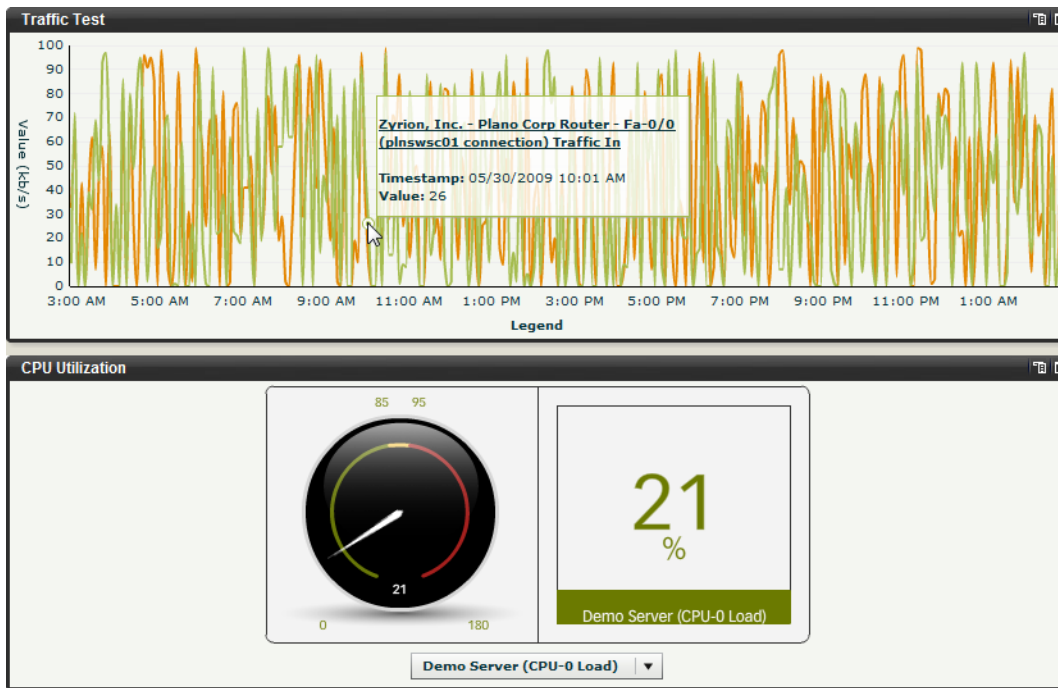
Apply **Cancel**

- 6 Now add a gauge component for a CPU utilization test. Click the  Add Dashboard Component icon in the upper right corner of the dashboard, select the gauge component type icon, fill in the Title field, select the refresh interval, and then click **Apply**.



- 7 Now specify the data source for the component. Select a device, and then click **Search** to find the matching tests. Drag and drop the CPU load tests to the Selected Tests list, and then click **Apply**.

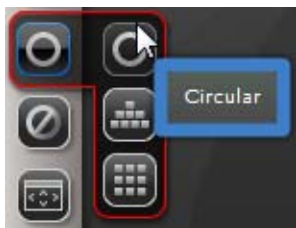




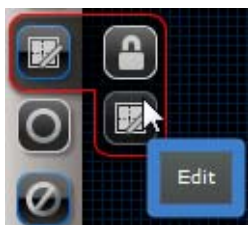
3.3 Panorama Topology Display

The Panorama feature offers an interactive graphical representation of the devices in your network that are being monitored, including the status of the devices and the dependency relationships between them. Panorama offers three different topology layouts, flexible display filters, pan and zoom functionality, the ability to configure and save custom views, and the ability to add or remove device dependencies.

- 1 Navigate to Status > Panorama.
- 2 Choose between hierarchical (the default), circular, or grid layout algorithms:.



- 3 In edit mode, you can move the position of the nodes on the canvas.



You can also add or remove device dependencies. When you click on a device node, a plus sign appears on the icon; click this plus sign and drag to another device to create a new parent/child dependency relationship. When you click on the line connecting two devices, a red X icon appears; click this X to remove the device dependency.

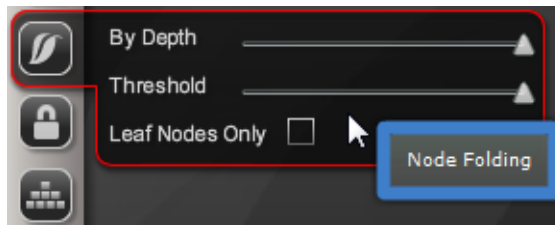
- 4 You can filter the devices shown in the topology view by type or status.



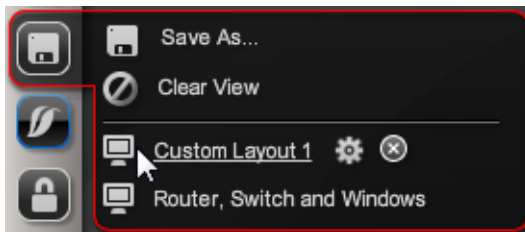
By default, the Filter By Device Type & Status frame opens with the Device Types pane expanded. If you click on the Status bar, the Status pane expands instead.

You can also click on the highlight option for each device or state, and device nodes of that type or state will appear highlighted in the topology view.

5 You can choose to collapse nodes based on depth in the hierarchy or threshold number of child nodes. If you select the Leaf Nodes Only check box, only the leaf nodes will be collapsed.



6 After customizing the topology view, you can save it as a custom layout:

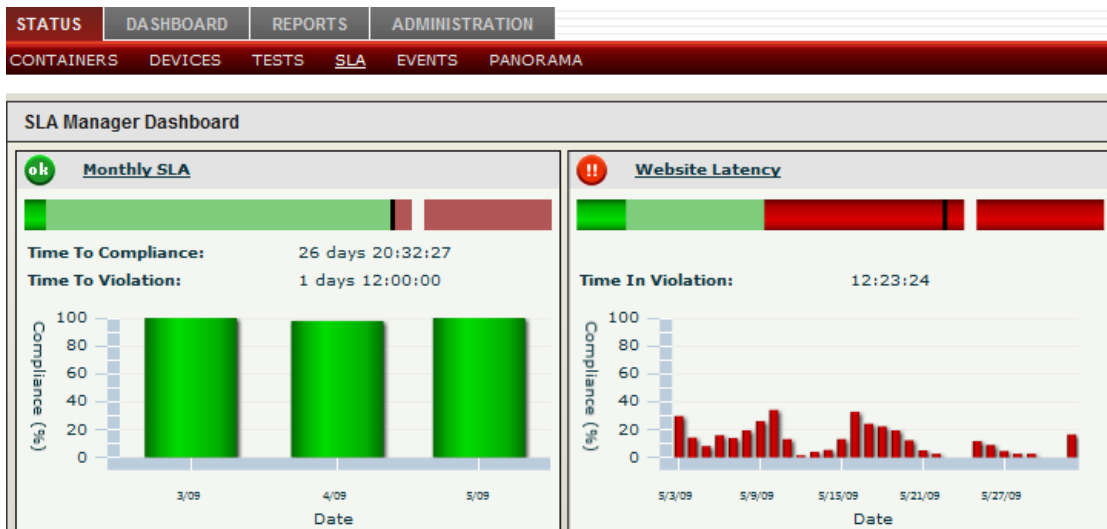


3.4 Creating an SLA Measurement

The SLA Manager lets you track compliance against user-defined Service Level Agreement metrics. These SLA metrics are calculated and displayed on a real-time dashboard that displays the amount of time that the metric is within the SLA threshold and also displays how close the metric is to violating the SLA requirement.

- 1 Navigate to Administration > SLA in the Traverse Web application.
- 2 On the Configure SLA Manager page, click **Create an SLA Measurement**.
- 3 Fill out the fields in the Create an SLA Measurement form, where Threshold is the percentage of the Calculation Period that the metric must be in the OK state.
- 4 Click **Submit** to go to the page for selecting the underlying device tests for this SLA metric, and then click **Add**.
- 5 Choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you need, and then click **Apply** to run the search.
- 6 In the Search Results pane, select the tests that you want to be a part of the SLA metric for each device, and then click **Assign to SLA Measurement**.

- 7 You can now click on the devices you've added in the Assigned Devices list, and the tests you selected will appear under Assigned Tests. Use the Add, Edit, and Remove buttons to make any further changes to the devices and tests you want to include, and then click **Done** to finish creating the SLA measurement.
- 8 Navigate to Status > SLA to view real-time data for your SLA metrics on the SLA Manager dashboard.



3.5 Event Manager & Message Handler

The Traverse Event Manager Console displays messages (traps, logs, windows events) forwarded from the Message Handler, as well as threshold violations.

- 1 Navigate to Status > Events.
- 2 From the Event Manager Console you can acknowledge, suppress, and delete events. Events can be suppressed until a particular date and time, or until the state changes. The screen refreshes automatically every few minutes (this interval can be changed on the Administration > Preferences page).

The Message Handler is a distributed component of Traverse which accepts syslogs, SNMP traps, Windows events or any other text messages and then searches for specified patterns in these messages. When a pattern match is found, the message string is transformed and a severity assigned to it, and then it is forwarded to the DGE. The processed messages from the Message Handler are displayed on the Traverse Event Manager Console and can trigger actions & notifications setup on the DGE.

For more information on configuring the Message Handler, see the *Traverse User Guide*.

3.6 Federated Security Model

Traverse has a multi-tier user model, which allows you to create accounts for different departments such that users in one department cannot see the devices in another department. You can also create administrator accounts for users who need to view multiple departments across the enterprise. For more information, see the *Traverse User Guide*.

3.7 Configuring Network Flow Analysis

Traverse integrates with network flow and packet level data collection tools to provide a seamless drilldown from system and device level monitoring to troubleshooting and analysis using flow and packet data. This data provides details about the network traffic between hosts, enabling quick identification of impacted services, trouble areas, and problem sources.

Enabling the Traverse Integrated NetFlow Collector

Traverse has an integrated NetFlow collector which can be used for smaller environments. The integrated network flow collector is pre-installed with the DGE, but disabled by default.

- 1 On UNIX, execute the following command as root:

```
touch /usr/local/traverse/plugin/monitors/flow.enable
```

On Windows, open a command window and execute the following commands:

```
sc config tvFlowQD start= auto
```

```
sc config tvSiLK start= auto
```

NOTE: The space after "start=" is required.

- 2 Edit <TRAVERSE_HOME>/apps/silk/data/sensor.conf and locate the following line:

```
internal-ipblock 192.168.10.0/24
```

Update the network segment (192.168.10.0/24) to match your local IP subnet in n.n.n.n/mask format.

For more information about the options in this configuration file, see <http://tools.netsa.cert.org/silk/sensor.conf.html>.

- 3 On UNIX, start the NetFlow collector by executing the following command as root:

```
<TRAVERSE_HOME>/etc/traverse.init start
```

On Windows, start the NetFlow collector by navigating to Start > Programs > Zyrion Traverse > Traverse Service Controller and clicking **Start All** to start the NetFlow collector components.

Enabling NetFlow on a Cisco Router (or switch running IOS)

The network flow analysis feature in Traverse relies on collecting network flow data exported by a router or switch, so you need to enable your network equipment to export flow records. Network flow records are exported from the routers to the default TCP port of 9996.

- 1 Telnet or SSH into the router and enter enable mode.
- 2 Enable Cisco Express Forwarding:

```
router(config)# ip cef
```

- 3 Enable NetFlow on all physical interfaces that will take part in routing traffic between devices of interest:

```
router(config)# interface <interface>
```

```
router(config-if)# ip route-cache flow
```

NOTE: Routers may by default export flow data only for traffic entering the router, so make sure you enable NetFlow on all interfaces for accurate analysis of traffic both into and out of

the router.

4 Enable export of NetFlow records:

```
router(config)# ip flow-export version 5
router(config)# ip flow-export destination <dge_address> 2055
router(config)# ip flow-export source FastEthernet0
router(config)# ip flow-cache timeout active 1
router(config)# ip flow-cache timeout inactive 15
```

NOTE: The 'ip flow-export source' can be any interface that stays active; a stable or Loopback interface is preferred.

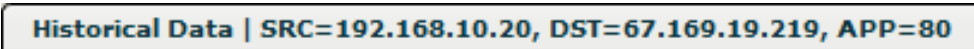
5 Save the configuration:

```
router(config)# end
router# write mem
```

Using the Network Flow Analysis Console

You can access the Network Flow Analysis console from the Traverse Web application from a device Test Summary page or from a Test Details page.

Each chart in the network flow analysis console has a title bar that states which device(s) (and optionally, which application) are being examined, as well as their roles.



Historical Data | SRC=192.168.10.20, DST=67.169.19.219, APP=80

Figure 3-1. Network Flow Analysis Chart Title Bar

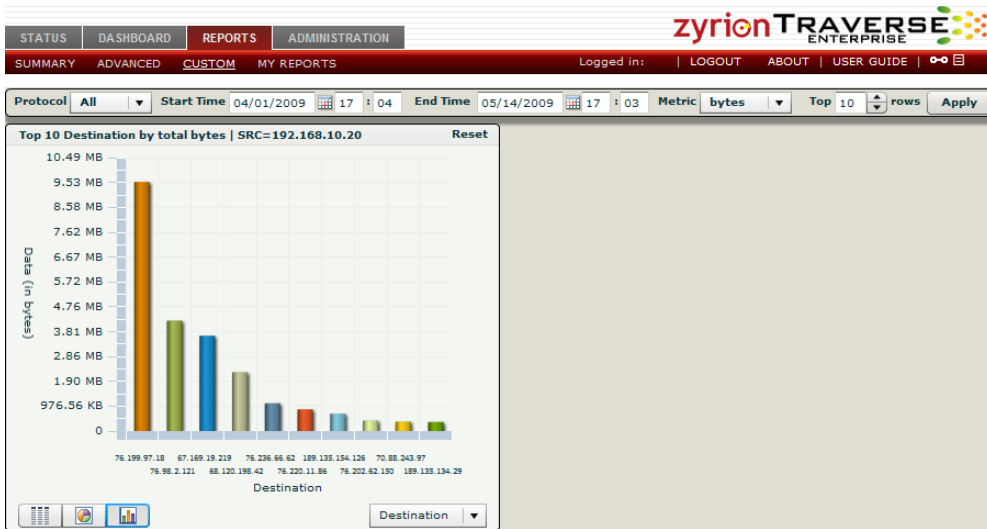
SRC = Source (represented by an IP address)

DST = Destination (represented by an IP address)

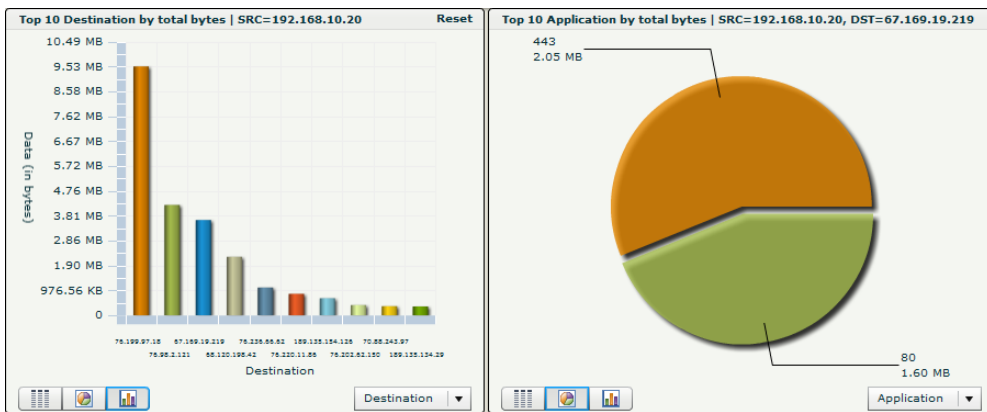
APP = Application (represented by a port number)

- 1 Navigate to Status > Devices and click on a device name.
- 2 On the Test Summary page, open the Run Reports drop-down menu and click on **Flow Analysis**.

- By default, network flow data for the past 24 hours is analyzed to determine the top 10 destinations communicating with the selected device (source), and the results are presented in bar chart format.

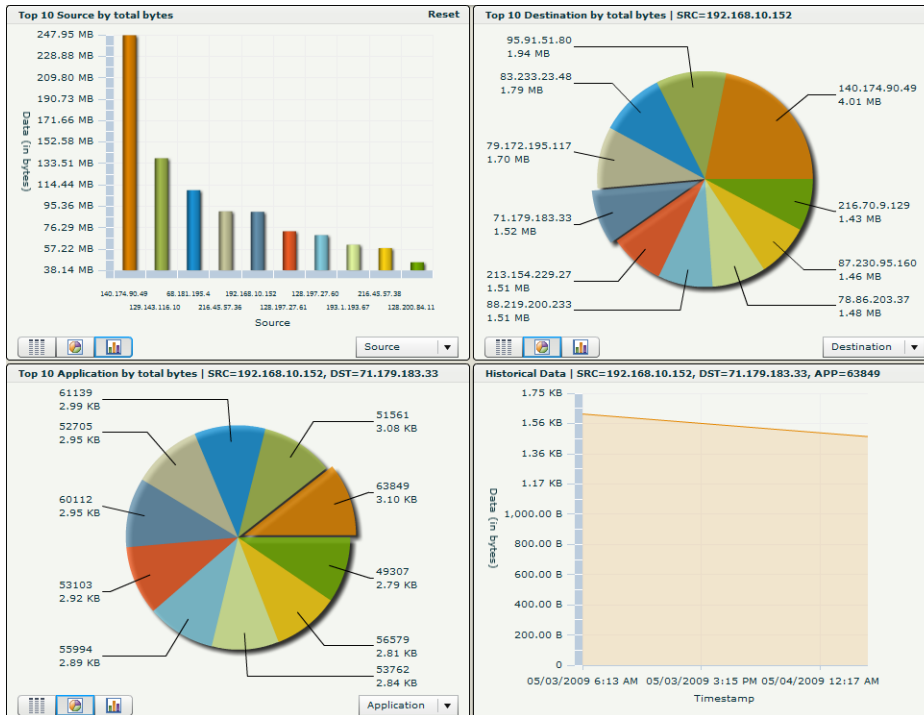


- Click on the results for an IP address on the Destination chart to display the top 10 applications for that destination of that source alongside in pie chart format.



- Click on the results for an application on the Applications chart to display historical data for network traffic for that application for the selected destination-source pair.
- Normally data is displayed for a single source or destination device, but you can click on **Reset** in the upper right corner of the first chart in the network flow analysis console to expand the scope of data to the entire network, providing a network-wide view of the top-N sources, destinations, or applications.

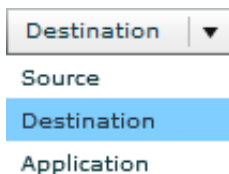
- 7 Click through as described above to get detailed device data.



- 8 Each network flow analysis chart can be displayed as a table, a pie chart, or a bar chart. Click on the corresponding button in the lower left corner of the chart to change how the data is displayed.



- 9 You can change the network flow analysis workflow by looking at a device first from any of the three different roles: source, destination, or application. Choose the role from the drop-down menu in the lower right corner of the chart.



- 10 Use the options in the menu bar at the top of the network flow analysis console to customize the data shown:
- The Protocol drop-down menu lets you choose whether to show just tcp or udp traffic, or all traffic.
 - You can specify the Start Time and End Time to see network flow data for a particular time period.
 - The Metric drop-down menu lets you choose whether to show data in bytes or packets.
 - The Top field lets you choose how many clients or servers to show.

NOTE: You must click **Apply** to show the new data after making any changes to these options.

3.8 Extensible APIs

Traverse has very powerful APIs which allow access to all components of the software. Users familiar with Perl or C can start using the API very quickly due to its familiar commands and interface. These APIs allow you to configure connections to other legacy products or custom applications.

BVE FlexAPI

You can use the BVE API to perform bulk changes to tests or devices. The BVE API can be accessed via a direct telnet connection or through the perl API. Any Traverse end user can log in to the API and will get access to the same privileges and devices as when logging in via the Web interface.

- 1 To log in, ensure that the BVE API is running on the Traverse host. Then, from a Windows command prompt, UNIX shell, or alternate telnet client, telnet to port 7661 and enter the following command:

```
telnet localhost 7661  
  
LOGIN <login_id>/<password>
```

- 2 The basic commands are *list*, *add*, *delete*, and *suspend*, which can be applied to contexts such as *device*, *test*, and *user*. The general syntax is "context.command <parameters>", as in the following examples.

- List all devices:

```
device.list "deviceName=*" 
```

- List all tests for a device:

```
test.list "deviceName=xyz", "testName=*" 
```

- Set the warning threshold for all line utilization tests to 80% (you can also set this threshold using the Web application):

```
test.update "testName=Line Utilization", "deviceName=*",  
warningThreshold="80"
```

Plugin Monitors & Plugin Actions

The plugin monitor functionality in Traverse allows creating new monitors in Java or any other programming language such as C, perl, shell, etc. The system treats such plugin monitors as an integrated component of Traverse and provides a similar multi-threaded framework as it uses internally for its own monitors.

Plugin Actions allow you to run any custom script when a threshold is crossed or a new event is generated.

For more information, see the *Traverse Developer Guide & API Reference*.