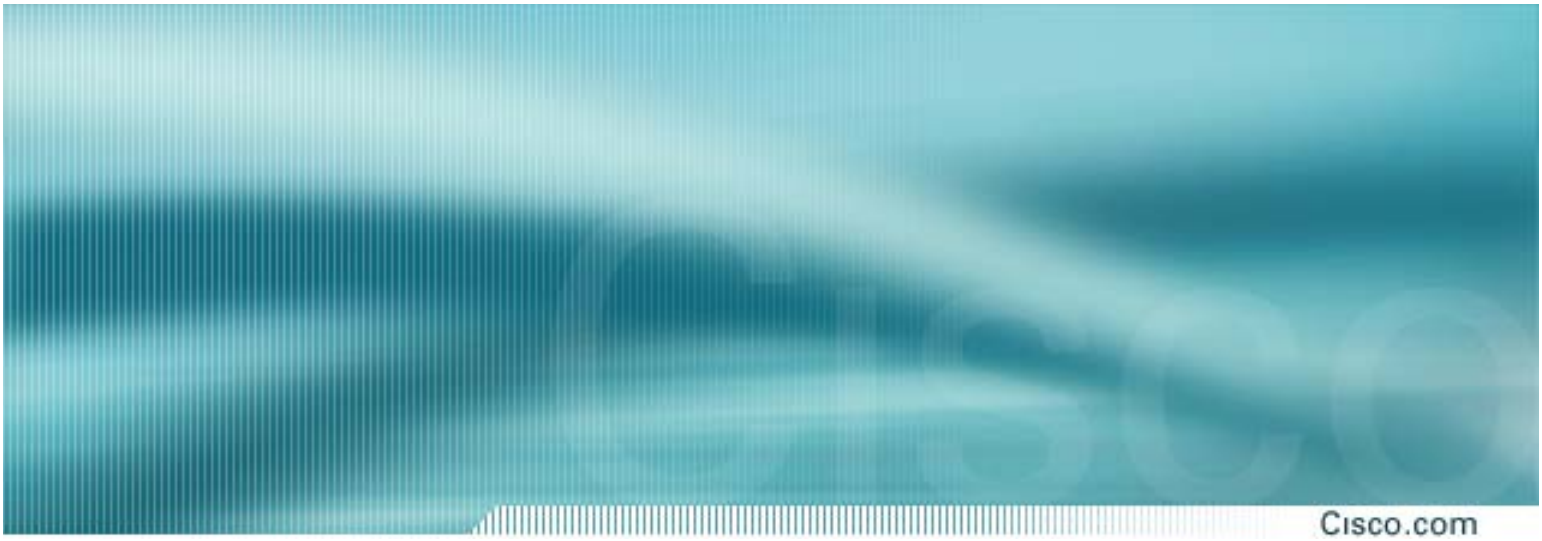


Cisco Performance Visibility Manager 1.0 Tutorial

The products and specifications, configurations, and other technical information regarding the products in this manual are subject to change without notice. All statements, technical information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. You must take full responsibility for their application of any products specified in this manual.

LICENSE

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THE MANUAL, DOCUMENTATION, AND/OR SOFTWARE ("MATERIALS"). BY USING THE MATERIALS YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE, PROMPTLY RETURN THE UNUSED MATERIALS (WITH PROOF OF PAYMENT) TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Cisco Systems, Inc. ("Cisco") and its suppliers grant to you ("You") a nonexclusive and nontransferable license to use the Cisco Materials solely for Your own personal use. If the Materials include Cisco software ("Software"), Cisco grants to You a nonexclusive and nontransferable license to use the Software in object code form solely on a single central processing unit owned or leased by You or otherwise embedded in equipment provided by Cisco. You may make one (1) archival copy of the Software provided You affix to such copy all copyright, confidentiality, and proprietary notices that appear on the original. EXCEPT AS EXPRESSLY AUTHORIZED ABOVE, YOU SHALL NOT: COPY, IN WHOLE OR IN PART, MATERIALS; MODIFY THE SOFTWARE; REVERSE COMPILE OR REVERSE ASSEMBLE ALL OR ANY PORTION OF THE SOFTWARE; OR RENT, LEASE, DISTRIBUTE, SELL, OR CREATE DERIVATIVE WORKS OF THE MATERIALS.

You agree that aspects of the licensed Materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Cisco. You agree not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Cisco. You agree to implement reasonable security measures to protect such trade secrets and copyrighted Material. Title to the Materials shall remain solely with Cisco.

This License is effective until terminated. You may terminate this License at any time by destroying all copies of the Materials. This License will terminate immediately without notice from Cisco if You fail to comply with any provision of this License. Upon termination, You must destroy all copies of the Materials.

Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. You agree to comply strictly with all such regulations and acknowledge that it has the responsibility to obtain licenses to export, re-export, or import Software.

This License shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this License shall remain in full force and effect. This License constitutes the entire License between the parties with respect to the use of the Materials

Restricted Rights - Cisco's software is provided to non-DOD agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the U.S. Government is subject to the restrictions as set forth in subparagraph "C" of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19. In the event the sale is to a DOD agency, the U.S. Government's rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202.

DISCLAIMER OF WARRANTY. ALL MATERIALS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event shall Cisco's or its suppliers' liability to You, whether in contract, tort (including negligence), or otherwise, exceed the price paid by You. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose.

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The following third-party software may be included with your product and will be subject to the software license agreement:

CiscoWorks software and documentation are based in part on HP OpenView under license from the Hewlett-Packard Company. HP OpenView is a trademark of the Hewlett-Packard Company. Copyright © 1992, 1993 Hewlett-Packard Company.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Network Time Protocol (NTP). Copyright © 1992, David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989, Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

The Cisco implementation of TN3270 is an adaptation of the TN3270, curses, and termcap programs developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981-1988, Regents of the University of California.

About This Tutorial

Cisco.com

- **Identify the need for traffic management**
- **Describe the industry standards and Cisco's implementation of traffic management**
- **Provide common traffic management scenarios**
- **Provide helpful guidelines on installation and troubleshooting PVM**
- **Provide links to helpful documentation**

About This Tutorial

The Cisco Performance Visibility Manager (PVM) tutorial provides self–paced training focused on using the PVM software to collect and view network traffic statistics from multiple NAMs and their associated switches and routers.

The Network Analysis Module (NAM) for Cisco Catalyst 6500 series switches and 7600 series internet routers is a network monitoring system that combines a rich set of embedded data collection and analysis capabilities with a Web–based management console. And all of this functionality resides on a single blade in a Cisco Catalyst switch. In addition, the NAM has dedicated resources for all management functions, thus eliminating any load it might impose on the host switch. The traffic data collected by the NAM is based on Remote Monitoring(RMON), RMON2, mini–RMON, Switch Monitoring(SMON), High–Capacity Monitoring(HCRMON) and DiffServ Monitoring (DSMON) standards.

While the NAM provides visibility into a wealth of traffic statistics at discrete points in the network, a typical enterprise will have deployed multiple NAMs at strategic locations to provide visibility into traffic on important segments of the network. A network administrator can glean valuable information about the network if there was a way to correlate and aggregate information from these strategically deployed NAMs. Cisco Performance Visibility Manager provides this ability, by aggregating and correlating information from multiple NAMs. It provides a wide range of reports and the ability to view select information from anywhere in the network.

The tutorial is structured as a series of self–paced modules, or chapters, that conclude with self–administered exercises. Also included is a helpful reference section containing links to technical documents on component products, concepts and terminology. The material is presented through text, helpful illustrations, hypertext links and common usage and troubleshooting scenarios.

Who Should Use This Tutorial

This tutorial was written as a technical resource for network administrators responsible for managing and troubleshooting their network and assumes that you have an understanding of networking principles and network management concepts.

Prerequisites

Users of the PVM should have at least the following prerequisites:

A basic understanding of the operation and configuration of their network, including the topology, device inventory, and security requirements

A basic understanding of switching; knowledge of how to configure and use the Cisco Catalyst® 6500 series switches or 7600 series internet routers

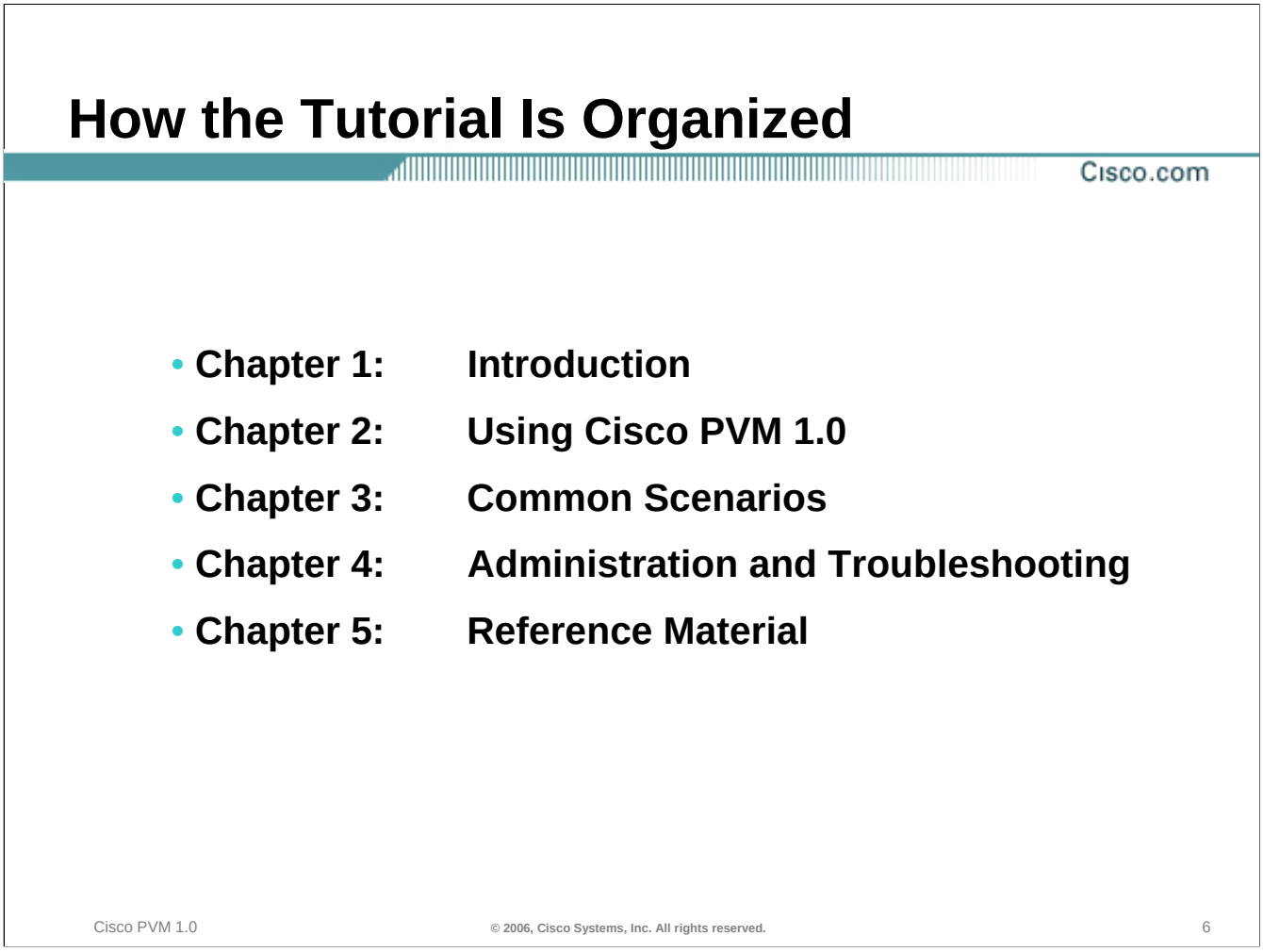
A basic understanding of spanning using an analyzer port on a Cisco Catalyst switch

A basic understanding of Simple Network Management Protocol (SNMP) and Management Information Bases (MIBs)

A thorough understanding of the Cisco Network Analysis Module (NAM), its various versions, concepts and configuration details

Estimated Completion Time

10 hours



How This Tutorial Is Organized

The tutorial is divided into five chapters. Each chapter begins with the learning objectives specific to that chapter and concludes with a series of self–assessment exercises based on the chapter objectives. Multiple–choice exercises are provided at the end of each chapter to enable you to assess your understanding of the material presented. A summary of each chapter is presented below.

Chapter 1 – Introduction

This chapter introduces the need for obtaining an aggregated view of traffic through your network. It briefly discusses the Cisco NAM and its integrated Cisco Traffic Analyzer software. An overview of Cisco's solution for gaining the aggregated view is presented by introducing Cisco PVM, before learning about the features and capabilities of Cisco PVM in Chapter 2 and applying them to common network management scenarios in Chapter 3.

Chapter 2 – Using Cisco PVM

This chapter discusses the key features of Cisco PVM to provide you with an understanding of the product as a whole, as well as each of the tasks necessary to configure Cisco PVM for monitoring and reporting. First, Cisco PVM architecture is outlined to identify how all the components work together. Second, an overview of the tasks necessary to configure Cisco PVM is provided. Third, to familiarize you with the various reporting views and capabilities of Cisco PVM, an overview of the monitoring and reporting suites available is provided. Fourth, a roadmap to using Cisco PVM is presented with a logical workflow depicting how to use Cisco PVM.

Chapter 3 – Common Scenarios

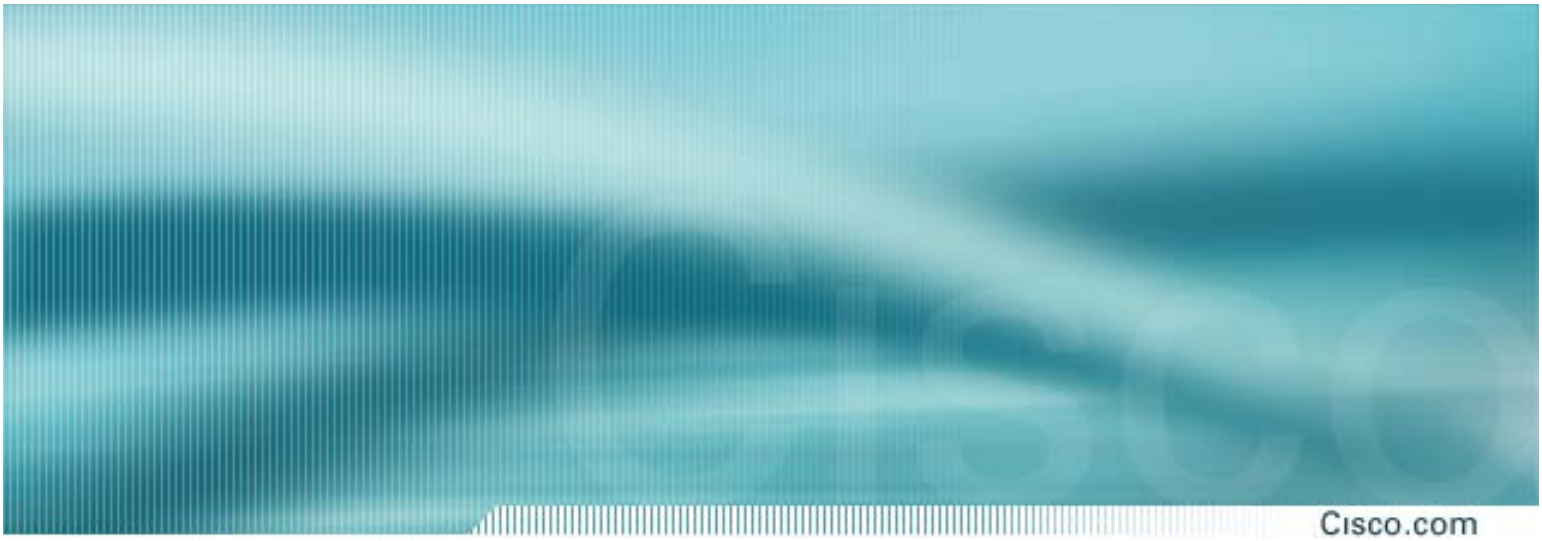
This chapter provides a walk–through of several common scenarios and how PVM can be used to help you in monitoring and assessing your network. These scenarios reinforce the concepts learned in Chapter 2 and enable to user to see how these concepts can be used practically to solve their network issues.

Chapter 4 – Administration & Troubleshooting

This chapter provides information on product requirements, general installation guidelines and tips for troubleshooting and avoiding common problems when using the PVM. For more detailed information on installation, please refer to the user guide. A link to the user guide can be found in the reference material section.

Chapter 5 – Reference Material

This chapter provides a comprehensive list of additional product information, such as links to white papers and documentation.



Chapter 1

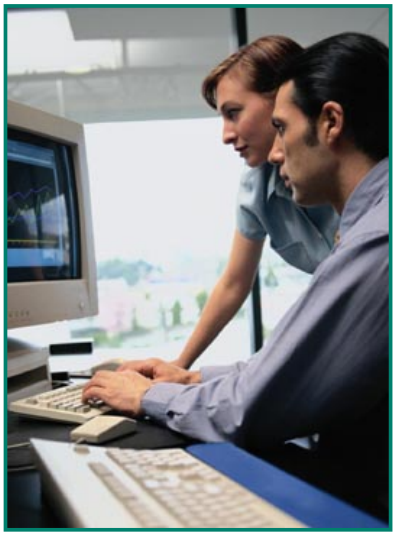
Introduction

Cisco Performance Visibility Manager 1.0

Chapter 1 Objectives

Cisco.com

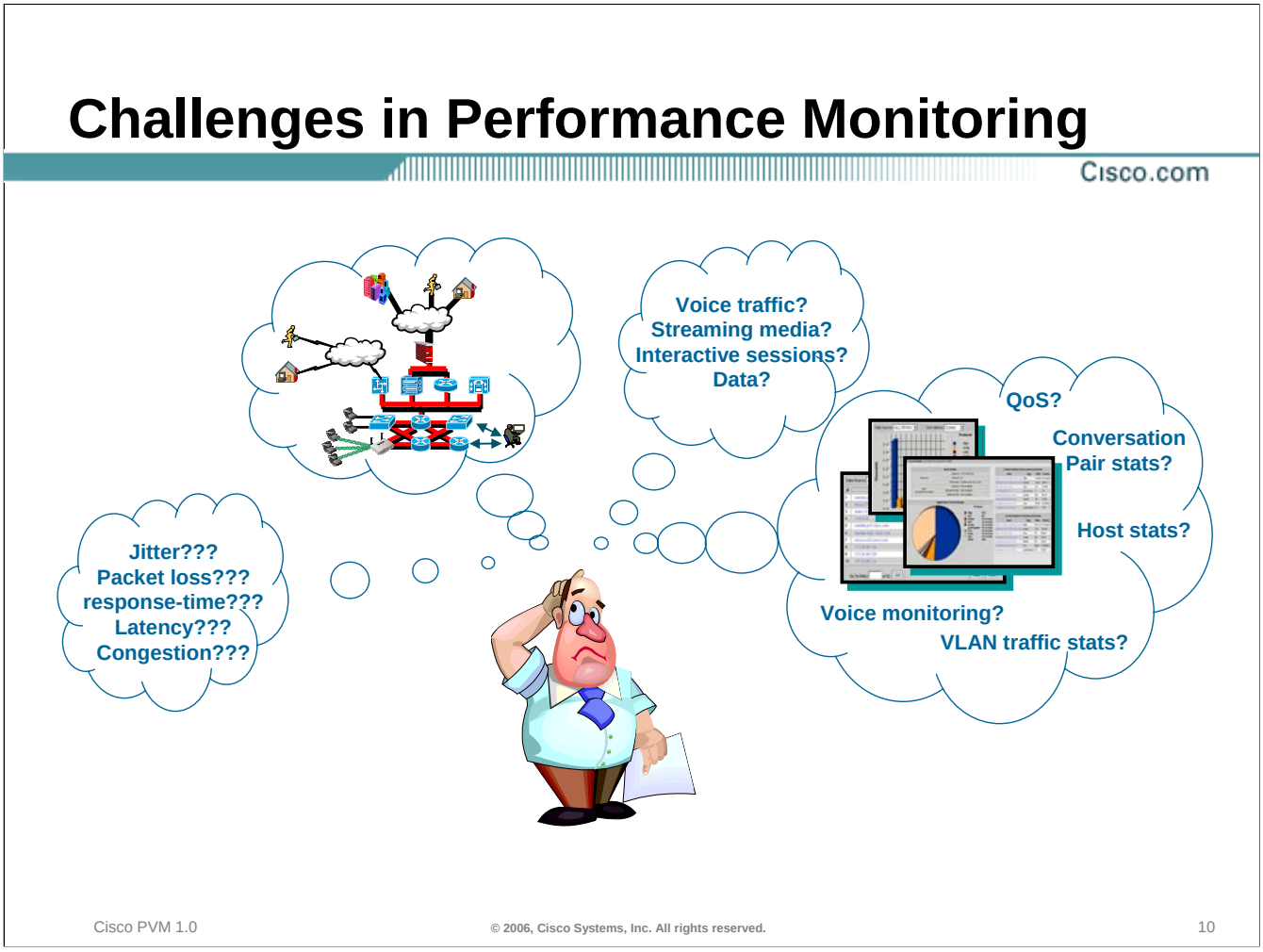
- **Challenges in performance monitoring**
- **Aggregated Traffic Data**
- **Cisco's solution – Performance Visibility Manager**



Chapter 1 Objectives

Today's networks are the foundation for the communications on which organizations depend for their day–to–day and mission–critical operations. Enterprise networks and their administrators these days are tasked with providing fast, secure, and reliable networking capabilities for the ever–expanding list of services that users and businesses demand. Today's network infrastructure has to support these varied and quickly changing services to deliver the same high quality voice, media, and data services that legacy systems have provided. These services are converging on the network infrastructure, whose complexity has grown immensely in the past few years.

As the complexity of the network and the need for network services increases, the task of the network managers and engineers grows correspondingly more complex. And under the pressure of increased productivity and budget reductions, network engineers are expected to do much more with much less. To work within these constraints, network engineers have to ensure that network resources are used efficiently and for the proper business reasons. Cisco believes that one key to your success is implementing effective performance monitoring tools that enable you to proactively manage your network. Let's look at how performance monitoring might be just what you need to manage your network and workload effectively and the answer Cisco has to the performance management issues that you face.

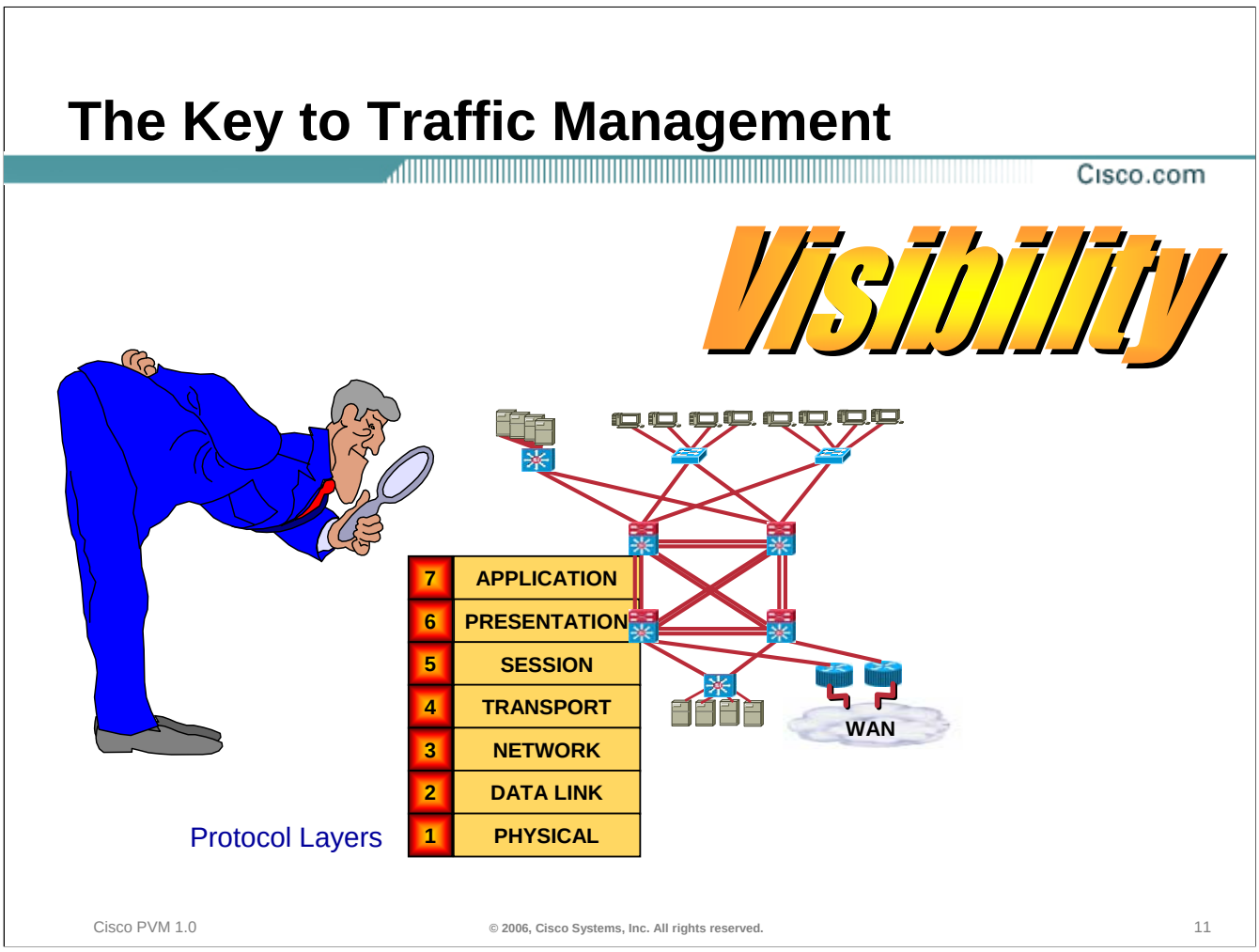


Challenges in Performance Monitoring

What are the challenges that network engineers and managers face when it comes to managing networks that support voice, streaming media, or data services? You face many issues. One that needs to be addressed is the existence of different types of traffic with differing performance requirements that run on the same network infrastructure. For example, voice and media traffic are very sensitive to the variations in delay of packet delivery, whereas data is not. Voice and media traffic are more tolerant of packet loss, whereas data is not. There are quality–of–service (QoS) solutions, such as Differentiated Services (DiffServ) and Multi-protocol Label Switching (MPLS), which allow you to prioritize traffic and reserve network resources to address these different requirements. But still, how do you know that these technologies have been implemented correctly to meet your service objectives? How do you measure the success of these technologies?

Another issue that you may face when running different services and applications on your network is that network management solutions often require different management services to collect the various types of data that give you meaningful performance information about each networked service. There are both standards–based and proprietary solutions for gathering data about applications, voice, DiffServ, virtual LANs (VLANs), and LANs, just to name a few. But if you run all these applications and services on your network, how do you find a monitoring system that collects and reports on all of them in a way that does not adversely impact your network, and yet gives you the information you need without being so complex that you need a development team to implement and integrate it?

Yet another issue that you may face when it comes to managing your network is identifying the complex patterns of users and applications that consume your network resources. Any form of proactive monitoring, whether it is implementing QoS strategies in your network or capacity planning for anticipating growth in network and system resources, requires a detailed understanding of how your network is being used and by whom. Answering this question was easier when networks consisted primarily of shared network devices, but gathering performance data has become more difficult in switched network environments because there is no single source from which to gather performance data.



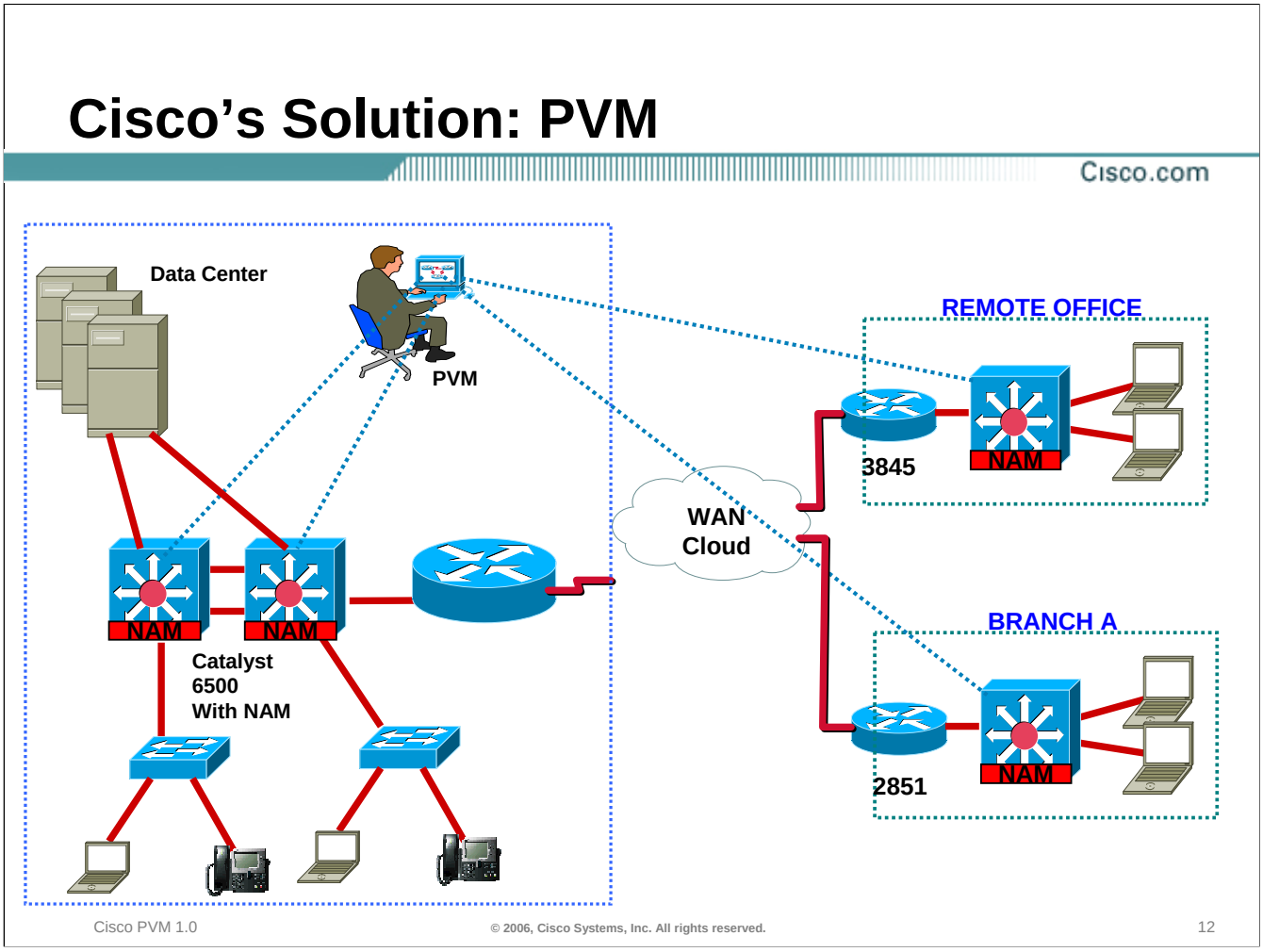
Visibility: The Answer to Some of Our Monitoring Needs

What is needed to solve some of the challenges that you face when it comes to managing your network? Visibility, the ability to see and analyze the traffic that consumes the resources on your network, will help you solve many of the management problems just mentioned. Visibility means many things in the context of today's complex networks, so to understand what is required and why, let's look at the issues in more detail.

Network traffic consists of discrete units called packets. Everything you want to know about the traffic on your network exists in the protocol headers of a packet. By examining the headers that are created at different protocol layers, you can identify who is talking with whom, what QoS priority has been assigned to a packet, what application created the packet, and so on. Just from the information in the packet headers, you can create very meaningful reports that help you understand how your network is being used. Collecting information from the packet itself is the best way to gain visibility into your network.

But visibility is not just about what you gather, it is also about where you gather it from. Most networks today employ some form of Layer 2 switching and VLANs at critical points in the network such as aggregation points and server farms where a significant percentage of network traffic converges. Collecting data from the switch itself provides visibility into the packets that traverse your network, the switch fabric, the switch ports that provide access to application servers, and trunk ports where traffic aggregates. Monitoring the traffic that flows through the ports, VLANs, and Cisco EtherChannel® tunnels on a switch serve as an extremely valuable collection point for performance monitoring that cannot be gathered anywhere else.

Monitoring at the switch provides other benefits as well. It also offers the ability to monitor critical devices, such as servers, closest to their source at the port that connects the devices to the network. This enables you to collect information from a response-time perspective because traffic can be time stamped as it enters and exits ports. Collecting response-time data provides a direct way to measure the end user's experience of your network. That is visibility!



Cisco's Solution: Performance Visibility Manager

The Network Analysis Module (NAM) for Cisco Catalyst 6500 series switches and Cisco 7600 series Internet routers, as well as for ISRs, referred to herein as the NAM, is a network monitoring system that combines a rich set of embedded data collection and analysis capabilities with a web–based management console. And all of this functionality resides in a single module. In addition, the NAM has dedicated resources for all management functions, thus eliminating any load it might impose on the host switch. Now, large volumes of performance data can be gathered about the switch and the traffic traversing it without impacting the switch itself.

Cisco PVM builds on the rich traffic analysis capabilities of the NAM, by allowing the user to aggregate and correlate information from multiple NAMs. By leveraging the intelligent traffic and response time monitoring capabilities of Cisco Network Analysis Modules (NAM), Cisco PVM provides an integrated end–to–end view of application and network behavior, host to application–tier communications, and various performance baselines. Acting as a central performance dashboard, Cisco PVM can continuously and proactively monitor for performance violations so that abnormalities can be identified and addressed before they become problems.

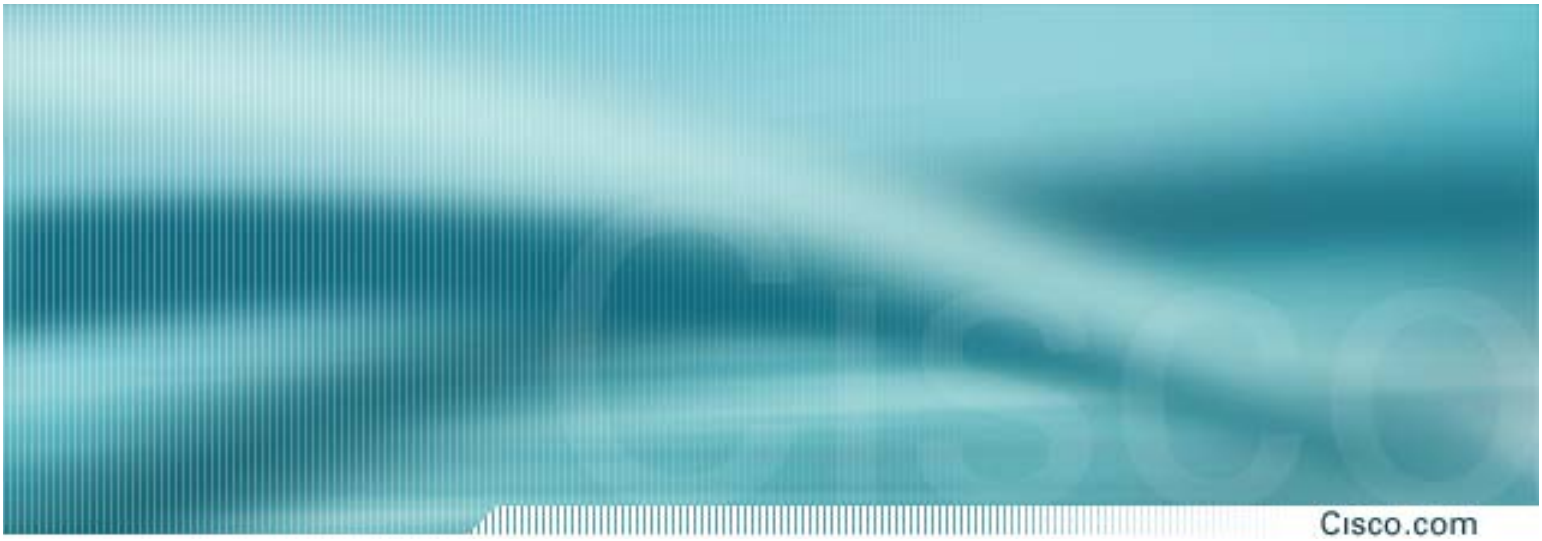
Cisco PVM aggregates and correlates data from multiple NAMs and network devices to analyze traffic on your network. It provides details about the protocols, hosts, conversations, differentiated services, VLANs, switch ports, and router interfaces. Cisco PVM performs TopN analysis to identify top talkers and top protocols in the network. It supports several data visualization modes including tabular text and graphics so that you can easily see what is going on in your network. The system also stores the collected and analyzed information for historical reporting and further analysis on demand.

The Cisco PVM User Guide is available online as Cisco.com. You can download and print the guide using Adobe Reader through your Web browser, or you can order a copy of the guide (P/N OL–8620–01).

The User Guide provides information and specific procedures for:

- An overview of the application
- Setup
- Monitor
- Reports
- ART
- Alerts
- Administration
- NAM Import File Formats
- Report Samples
- Database Archiving

As mentioned in the previous chapter, Cisco PVM leverages the Cisco Network Analysis Module to gather traffic statistics from the network. In release 1.0, Cisco PVM is focused on providing a centralized NAM solution along with several key features.



Chapter 2

Using Cisco PVM

Cisco Performance Visibility Manager 1.0

Key Features of PVM

Cisco.com

- **Data Collection and Aggregation**
- **Traffic and Bandwidth Utilization Analysis**
- **Application Response Time Monitoring**
- **Real Time, Historical and Trending Reports**
- **Proactive Monitoring**

Key Features of Cisco PVM

Data Collection and Aggregation

Cisco PVM collects traffic statistics from multiple NAMs and their associated devices. Once traffic statistics are collected, it aggregates this information and presents the information in a high–level operations view that enables the user to quickly pinpoint trouble spots in their network. Cisco PVM also presents information in multiple ways so that the user can quickly access and visualize the mst relevant information and make intelligent decisions based on the data.

Cisco PVM collects the data from several MIBs in the NAM and also from the associated Switch or Router. From the NAM, Cisco PVM gathers information from the following MIBs : RMON I , RMON II, DSMON and ART . From the associated Switch or Router, Cisco PVM gathers information from the Interface Tables, and SMON MIBs.

Traffic and Bandwidth Utilization Analysis

Cisco PVM allows the user to perform traffic analysis based on the data collected. The user can gain visibility into the network by performing a TopN analysis to find out:

a. Which applications are using the most bandwidth?

b. Which locations are using the most bandwidth?

c. Which hosts are using the most Bandwidth?

Cisco PVM allows the user to perform Application Analysis by fully leveraging the NAMs capabilities to differentiate traffic based on static ports, dynamic ports and HTTP sub–classification by URL. The user can also perform Hosts and Conversations analysis that enables them to identify the top talkers in the network and who they are talking to.

Since Cisco PVM also collects information from Switches and Routers, it gives you the ability to perform VLAN analysis by identifying applications, hosts and protocols that are consuming bandwidth on a given VLAN. It also allows you to analyze information per port on the Router or Switch, watch the link utilization on individual ports and plan and take action accordingly.

Application Response Time Monitoring

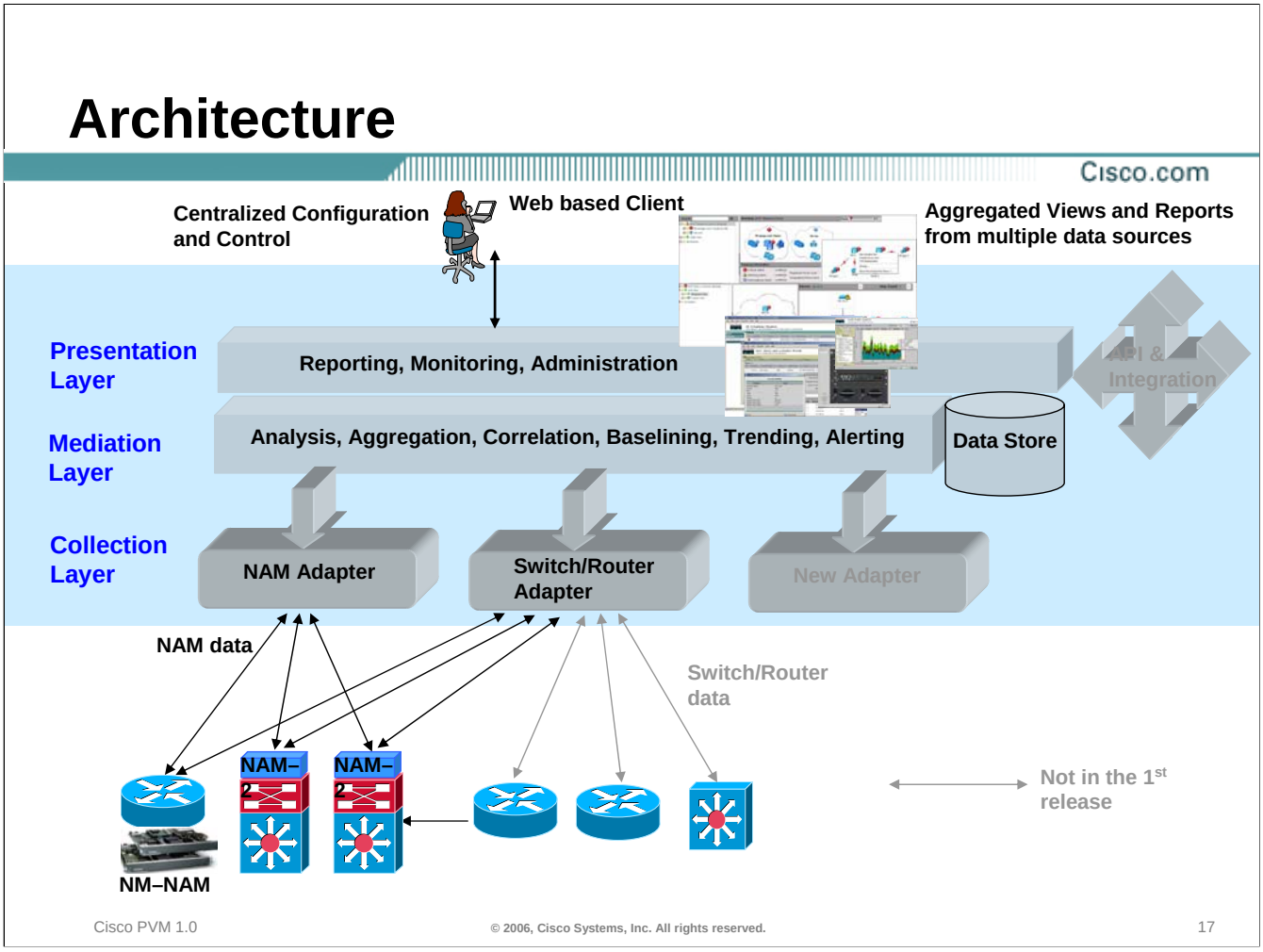
Cisco PVM's Application Response Time monitoring feature allows you to measure response time at the server and the network to identify if a given performance problem is caused by the network or the server. It allows the user to measure response times for individual applications, hosts and subnets/locations by correlating application response time data from multiple NAMs. Based on the configuration, it allows you to visualize application response time in near real time and troubleshoot response time problems by drilling down to the appropriate NAM cards or devices. It presents current and historical performance data in intuitive tables and graphs that allows quick and easy access to the relevant data.

Real Time, Historical and Trending Reports

Cisco PVM features a strong reporting engine. A comprehensive report set that includes real–time and trending reports allows the user to do effective capacity planning, trend analysis and network status monitoring. Cisco PVM can retain performance data for up to three years, and this retention period is user configurable. The ability to provide real–time and near–term historical information is very valuable in troubleshooting a network performance problem, allowing you to distinguish what is happening now as supposed to what has happened in the recent past.

Proactive Monitoring

Cisco PVM allows the user to baseline their network traffic. Once setup, Cisco PVM automatically baselines and learns your network traffic patterns, and can alert you in case of any deviations. This allows you to proactively monitor the network and identify performance problems before the end users are affected.



Cisco PVM Architecture

PVM adopts a 3–tier architecture, consisting of the Collection Layer, the Mediation Layer and the Presentation Layer.

Collection Layer

The Collection Layer consists of device adapters that are tasked with gathering traffic statistics from the various configured devices. These device adapters collect information via SNMP, and are of 2 types: the NAM Adapter and the Switch/Router Adapter. This layer features load balancing, with failover protection : adapters are spawned as and when needed to handle collection for new devices, and are restarted automatically if they stop abnormally.

Mediation Layer

The Mediation Layer consists of processes that act upon the data gathered by the Collection Layer. Collected data is stored in the application data store, and the mediation layer processes correlate the data from various sources, and aggregate the information according to user–specified groups. These processes are also responsible for the base–lining and alerting features of Cisco PVM.

Presentation Layer

The Presentation Layer consists of the web application and a robust reporting engine, and is responsible for interacting with the user and presenting the analyzed data.

Supported Devices & Scalability

Cisco.com

- **Supported Cisco Devices:**
  - **NM–NAM**
  - **WS–SVC–NAM–1**
  - **WS–SVC–NAM–2**
  - **Cisco Catalyst 6500 Series Switches**
  - **Cisco 7600 Series Routers**
  - **Cisco Branch Routers (2600, 2800, 3660, 3700 and 3800 series)**
- **Supported NAM Software versions:**
  - **NAM Release 3.4 and 3.5**
- **Scalability Factors**
  - **NM–NAMs or NAM1/NAM2**
  - **Collection Interval**
  - **Data Retention Period**

Supported Devices

NAM support in Cisco PVM encompasses the NM–NAM, NAM 1 and NAM 2. These NAMs can be used in the Cisco Catalyst 6500 series switches, 7600 routers and the 2600, 2800, 3660, 3700 and 3800 series Branch Routers. Cisco PVM supports the 3.4 and 3.5 software versions of the NAM Traffic Analyzer.

Note: NAM software Release 3.3 is not supported.

Scalability

Cisco PVM is scalable to 100 NAM 1/NAM 2's and 300 NM–NAMs. It can also be configured to collect traffic statistics from the devices at certain intervals. This collection interval defaults to 5 minutes but is configurable from 1 minute to 1 hour. The collected data is aggregated into hourly, daily and monthly information, and can be retained for user–configurable lengths of time.

The retention period for aggregated data defaults to 3 months of hourly data, 1 year of daily data and 3 years of monthly data. The raw traffic statistics collected by the collection layer is retained for 2 days before being purged from the application data store. All these scalability factors play a role in the hardware configuration needed to support PVM.

Cisco PVM features a rich GUI interface that allows up to 5 concurrent users access to the traffic data.

Hardware Requirements

Cisco.com

- **Minimum Server Requirements**
  - **2 Intel Xeon CPU – 3.4 GHz**
  - **2 GB RAM**
  - **4 GB HD space available for the application and 3rd–party software**
  - **70 GB HD space available in the host installation directory**
  - **100 MB Ethernet card**
- **Minimum Client Requirements**
  - **Pentium 4 Processor**
  - **256 MB RAM**
- **Recommended Server Configurations**

Maximum NAMs	CPUs	RAM	Disk Space
5 NAM–2s	2 Intel Xeon – 3.4 GHz	2 GB	70 GB
50 NAM–2s + 50 NM–NAMs	4 Intel Xeon – 3.4 GHz	4 GB	850 GB in high–performance array configuration
100 NAM–2s + 300 NM–NAMs	4 Intel Xeon Dual–Core – 3.0 GHz	8 GB	4,600 GB in high–performance array configuration

Cisco PVM 1.0 19

Minimum Server Requirements

To support up to five NAM–2s, you'll need 70 GB available in the installation directory plus 4 GB for the PVM application itself and third–party software. On the server, the following network infrastructure is required:

- Reserve 100 MB Ethernet Administrative ports 1521, 8443, 443, 161, 162, and 1099
- Configure the network devices for delivery and collection of statistical data
- Configure port 1099 for LDAP

Minimum Client Requirements

To support up to five NAM–2s, you'll need 70 GB available in the installation directory plus 4 GB for the PVM application itself and third–party software.

Recommended Configurations

Cisco PVM supports a maximum of 200 NAM–2s, or the equivalent of 100 NAM–2s plus 300 NM–NAMs. The hardware requirements for Cisco PVM installations differ depending on the number of NAMs your system is intended to support. The requirements are broken down into three configurations:

- **Large** – used in configurations of up to 200 NAM–2s or 300 NM–NAMs + 100 NAM–2s
- **Medium** – used in configurations of up to 50 NM–NAMs + 50 NAM–2s
- **Small** – used in configurations of up to 5 NAM–2s

If the minimum hardware requirements are not met, Cisco PVM may not install or run properly.

Software Requirements

Cisco.com

– **Server**

- **Red Hat Linux Advanced Server Version 3 with Kernel 2.4 (Update 2 or higher)**
- **Adobe Reader 6.01 – 6.04**

– **Client**

- **Windows XP or 2000**
- **IE 6.0 (JavaScript and cookies enabled)**
- **Adobe Reader 6.01 – 6.04**

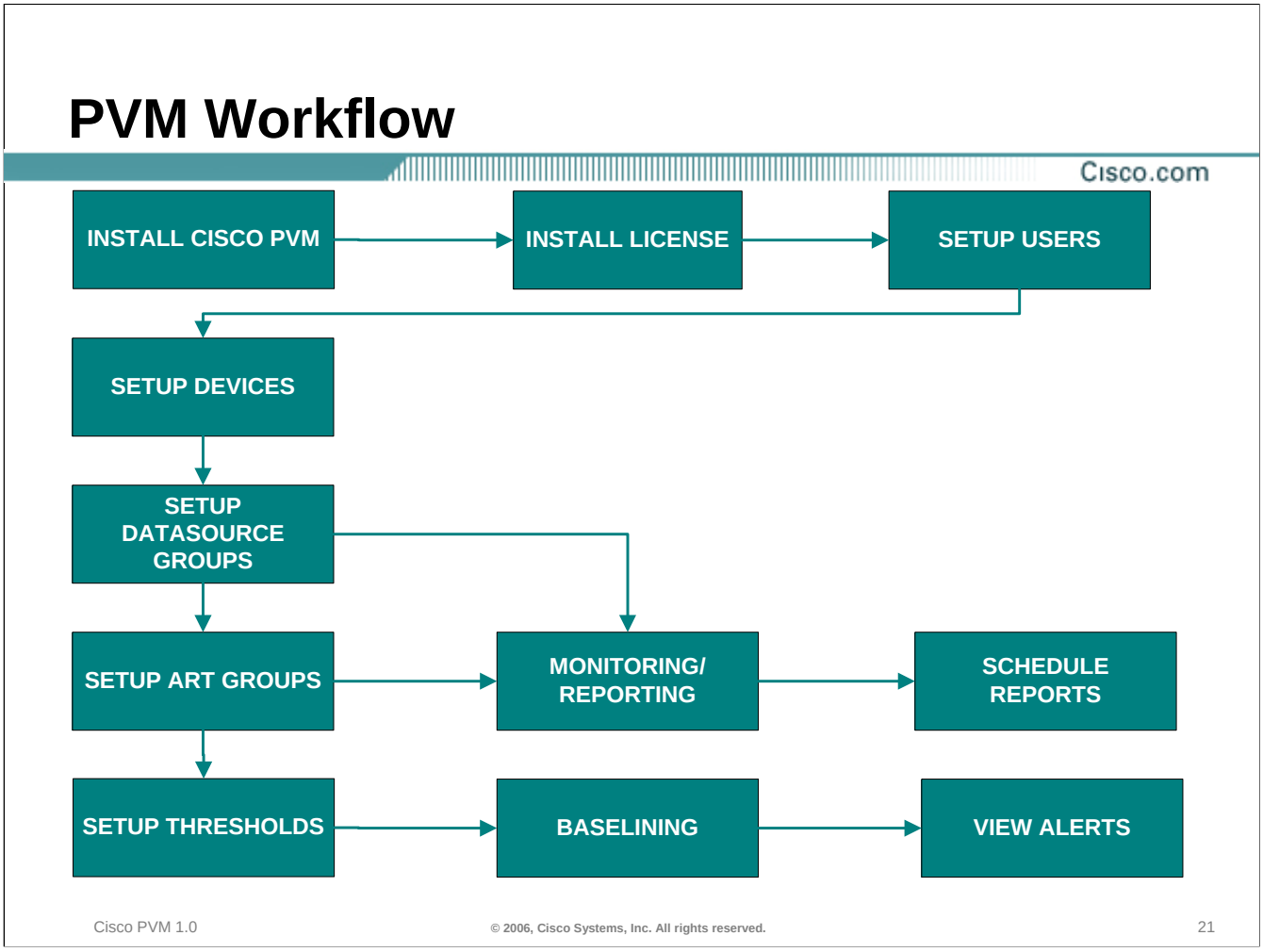
Software Requirements

Internet Explorer 6.0 SP2 is recommended. Users running Windows 2000 and IE 6.0 SP1 must ensure that all Microsoft updates for both windows and IE have been installed.

To ensure that the correct browser functionality is enabled, go to Tools > Internet Options > Advanced in the browser menu and click Restore Defaults > Apply > OK.

Enabling Java

Sun Java Runtime Environment (JRE) version 1.4 or greater needs to be installed. To ensure that all Sun Java options are enabled for SSO and other functionality, go to Tools > Internet Options > Security in the browser menu, select Custom Level, and ensure that Scripting of Java applets is enabled.



PVM Workflow

A typical user can expect to perform the above sequence of actions to configure and use PVM. A default Administrator user is available in the system immediately after installation, but the installation procedure asks you to change the default password to prevent unauthorized access to the system. The following sections explain each of these steps in more detail.

Installation Guidelines

Cisco.com

- Partition Management
- Disk Space Requirements
- Install Procedure
- Uninstall Procedure

Partition Management

Cisco PVM requires that a certain amount of disk space be available in specific directories for the installation to proceed. The following directories or partitions are required:

- Oracle data partition – default: /u01
- Install directory – default: /opt/CSCOpvm
- Oracle install directory – default: /opt/oracle

Note: Cisco PVM's install procedure asks the user to specify the Install directory and the Oracle data partition during the installation process. However, the Oracle install directory is fixed and cannot be changed.

Disk Space Requirements

The individual partition's disk space requirements are as follows:

PVM and Oracle install directory (/opt) > 3.5 GB of free disk space

Oracle data partition (/u01) > 70 GB of free disk space (depending on the number of NAMs you want to support in PVM)

The install will not proceed if the above disk space requirements are not met. If installing on a network directory, it is necessary to ensure that the correct permissions are set for the user on the network directory.

If the environment you are installing in is configured for NIS, make sure that 'oracle' and 'pvmadm' users are not created, since Cisco PVM will create these users.

Install Procedure

Insert DVD into DVD drive.

Open a command shell and go to the DVD drive root (login as root).

Example: cd /dev/cdrom

Start the install using ./installpvm.

Follow the prompts and change the install directories if necessary.

Install the License File:

su – pvmadm

cp sp_license.dat <PVM_INSTALL_DIR>/server/etc

Install the SSL Certificate if necessary (you can use the java keytool utility to generate one if needed):

cd <PVM_INSTALL_DIR>/j2sdk142/bin

keytool –genkey –keyalg RSA –storepass <password> –keystore $JBOSS_HOME/server/default/conf/ssl.keystore

Note: If you have a public SSL certificate, you can use that in lieu of the self–generated certificate using keytool. Use the procedure specified by the issuer of the certificate to install it.

Start PVM using pvm start.

Check the PVM GUI at:

https://<hostname>:8443/ or https://<hostname>:8443/acapweb/

Uninstall Procedure

When you uninstall Cisco PVM, you will remove all of the application's components and data files from the server. The uninstall will stop the Cisco PVM application and remove its components, as well as Oracle and the corresponding data files. Removing Cisco PVM involves executing the uninstall routine, which is Unix shell script:

$ su – root

$ cd $PVM_BASE/server/bin

$ ./uninstall_pvm.sh

The uninstall routine for Cisco PVM performs the following steps:

- Stops Cisco PVM and Oracle.
- Removes Cisco PVM and Oracle application files.
- Removes the Oracle database.
- Cleans up system files and environment variables.

Licensing

Cisco.com

- **License Modes and License Packs**
- **Base Software**
- **License File Installation**
- **Licensing Operations**

Licensing

Cisco PVM requires a license file to be installed to operate in the non–evaluation mode. The license file is not included in the Cisco PVM distribution; instead, Cisco PVM must first be installed on a host computer and then a license file must be acquired and installed for that particular host. This chapter describes how to install and test the Cisco PVM license file.

Cisco PVM uses the FLEXlm License Manager for its licensing operations.

License Modes and License Packs

Cisco PVM functions in the following modes depending on the type of license acquired:

No License file: Evaluation Mode (90 days). This mode of operation is limited to 90 days irrespective of how many times PVM is installed.

Valid license file:

- Demo License (6 months)
- Production License (valid for duration of license)

Without a valid license file installed, Cisco PVM will operate in Evaluation mode and will cease operating after 90 days. When a valid license file is installed, Cisco PVM will operate in Production mode. The Production license has no expiration date. Changes to the license file (such as adding NAMs over the number of current supported licenses) do not require reinstallation of Cisco PVM. In this case, replace the current license file on the Cisco PVM host computer with the new license file and issue the command lmreread.

Base Software

The Cisco PVM base software kit includes the necessary software for installing PVM on a single server running Red Hat Linux. Licensing right–to–use is based on the number of Cisco Catalyst 6500 Series and Cisco 7600 Series Network Analysis Modules (NAM 1/2) and Cisco Branch Routers Series Network Analysis Modules (NM–NAM) managed by the Cisco PVM software. In addition to purchasing the base software kit, you are also required to purchase one of the following license options.

- **CPVM-1.0-6K-10 –** license for up to 10 NAM1/NAM2
- **CPVM-1.0-6K-25 –** license for up to 25 NAM1/NAM2
- **CPVM-1.0-6K-50 –** license for up to 50 NAM1/NAM2
- **CPVM-1.0-NM-10 –** license for up to 10 NM-NAMs
- **CPVM-1.0-NM-25 –** license for up to 25 NM-NAMs
- **CPVM-1.0-NM-50 –** license for up to 50 NM-NAMs

License File Installation

The following steps need to be taken to install the license file:

Obtain a license from the Cisco website.

Once the license file is obtained from Cisco, it should be placed in: <PVM_INSTALL_DIR>/server/etc

Licensing Operations

By virtue of the fact that Cisco PVM uses the FLEXlm licensing server, Cisco PVM provides the following useful licensing operations that can be performed via the command line:

lmstat – indicates the status of the license server, whether it is up or down.

lmreread – re–reads the license file. This is necessary when the license file (sp_license.dat) is replaced as in the case of obtaining new licensed features.

lmhostid – provides the host id information that is necessary for generating the license file. All license files are node locked to the host computer for which PVM is installed.

User Administration & Security

Cisco.com

- **Authentication, Authorization, Auditing**
- **User Privileges**
- **User Management**
- **Security Logs**

User Administration & Security

As part of user administration and security, Cisco PVM provides the authentication, authorization and auditing capabilities listed below.

Authentication

Based on the standard Java SDK security features, Cisco PVM provides:

- Username/Password Authentication – The username and passwords are stored in the local database
- LDAP Authentication
- X509 Server Authentication supported by SSL/TLS – This feature is provided by the standard Java SDK which comes packaged with Cisco PVM. The 'keytool' utility can be used to generate a X508 server authentication certificate. This is done as part of install, since PVM provides only secure (https) access to the PVM GUI.

LDAP Authentication and Authorization

If you have set up your system to invoke Lightweight Directory Access Protocol (LDAP) user authentication and authorization, login IDs and passwords are not assigned through Cisco PVM user management. Check with your system or network administrator for login information.

Authorization

As part of the authorization feature, Cisco PVM provides LDAP Integration. If LDAP integration is not desired, Cisco PVM allows you to perform user configuration via the PVM GUI.

Auditing

Cisco PVM maintains security logs as part of the auditing feature. If necessary, the Admin can look at these logs to trace back user actions.

Administrator and General User Privileges

Depending on whether you are a Cisco PVM Administrator or a General User, you can access either some or all system functions. Access permissions are set by the Administrator, and determine the tabs and functions you'll see in the GUI. Administrators can view all tabs and functions, while General Users are limited to Monitor, Reports, and ART reporting functions, as well as the Change Password function under the Admin tab.

All users can click the Help link available at the top of every Cisco PVM window to view topics that pertain to all system functions. For example, if you are a General User, you can see how the NAMs, collection parameters, Data Source Groups, and ART Groups are set up in the system, but you cannot create or edit them.

User Access to Cisco PVM GUI Functions by User Type

Cisco PVM GUI Function	Administrator	General User
Setup		
NAMs, Switches, Routers: add, edit, delete, view, enable, and disable	x	
Thresholds: add, edit, delete, view, enable, and disable	x	
Data Source Groups: add, edit, delete, and view	x	
System Preferences: view and edit	x	
Monitor		
Run and view near real-time and real-time monitoring charts for single and aggregated NAM data	x	x
Reports		
Run, view, and schedule historical reports for single and aggregated NAM data	x	x
ART		
Add, edit, delete, and view ART Groups	x	
Run ART reports	x	x
Alerts		
View Threshold-crossing alarms	x	
View system events	x	
Admin		
View security events	x	
Add, edit, delete, and view user accounts	x	
Change other users' passwords	x	
Change own password	x	x

User Management

Cisco PVM Administrators can view and manage system users under the Admin tab. The General User will only see the Password menu item in the left menu. The login ID and password that you receive from your Administrator determines which access permissions you have.

Change Password

All users can change their own passwords. If you are an Administrator, you'll change the **pvmadm** login password the first time you run Cisco PVM. This action will ensure that other users cannot access the administrator functions. Refer to the Cisco PVM Installation Guide for details on logging in to PVM for the first time and changing the default Administrator password.

Creating a New User

To add a new user to the system, you'll enter the:

- Login ID – must be unique or the system will reject creation of the new user
- Name – not required, but you can enter the user's full name in this field
- Password – use 1 to 29 characters
- Confirm Password – must match the Password entry
- Account Type – defaults to either General User or to the type selected in the last set of filter criteria you used to filter the list of users

Editing a Current User

Cisco PVM Administrators can edit users currently in the system. For example, the Administrator may want to change a user type from General User to Administrator. When you edit a current user, all fields are available for modification except for the Login ID, which must remain unique.

After changes have been saved to the system, new group permissions and passwords will take effect for subsequent login sessions. Existing login sessions for the edited user (if any) are not affected.

Security Logs

Cisco PVM uses HTTPS to provide secure communication between the browser client and the server components. The security configuration is set in the system and does not require any user intervention or setup. PVM polls system data for security violations and other events, including:

- Login events
- Logout events
- Login failures
- NAM Traffic Analyzer launch events from the PVM GUI

Administrators can display the logged events under the Admin tab, and can filter events occurring by time period, severity, log type, source, and cause.

Device Setup

Cisco.com

- **Device Setup Overview**
- **Collection Overview**
- **NAM Setup**
- **Troubleshooting Device Setup**

Device Setup Overview

There are 3 ways to setup devices in PVM:

- Add a device through the GUI.
- Import devices from a CiscoWorks DCR CSV export file.
- Import devices from a user–defined CSV file.

The number of devices (NAMs) you can configure in PVM depends on the license pack you have purchased. You can configure a NAM and the associated device on which the NAM resides. You can configure only the NAM if you so choose, however, you cannot configure only a Switch or Router. Cisco PVM Setup for NAMs allows users to:

- View a list of all NAM devices currently loaded in the system.
- View a subset of NAM devices by filtering them based on their names.
- Manually add a NAM device to the system.
- Add multiple NAM devices by importing from a comma–delimited file.
- View and edit NAM device attributes.
- Delete NAMs and their supporting switches and routers.

NAM Database

The system automatically runs a background process that periodically updates the contents of the NAM database (once per minute). The list of NAMs loaded into the system can change due to:

- Addition or removal of devices from the system
- Changes in device relationships
- Operational changes to system devices
- You can enable or disable collection for the NAM and its associated device independently of each other.

Single Sign–On (SSO)

The single sign–on feature is available wherever you see a NAM name. The credentials used to perform single sign–on are obtained from either the User ID / Password entries from the NAM set up , or the actual login information of the Cisco PVM user. These credentials are used without user intervention of any kind. If both fail to login successfully to the NAM, the NAM login page will be displayed so that the user can login using different credentials. However, the credentials entered directly at the NAM login page are not stored anywhere by Cisco PVM.

The default value for the SNMP timeout parameter can be tweaked based on your network configuration. However, using the v2 setting for the SNMP version is recommended to prevent degraded performance for SNMP traps sent using getBulk requests.

About Switches and Routers

Similar to NAMs, supporting switch and router devices can be added to Cisco PVM either manually or through the import function on the NAM home page. You might want to add a switch or router to collect interface statistics, for example, since the system retrieves this data from switches and routers and not from NAMs. It is not necessary, however, to add supporting device information when adding NAMs; the Cisco PVM NAM edit function provides an option for adding supporting switch and router device information after NAM collection has already begun in the system. The Cisco PVM System–wide Collection Cycle setting applies to both switches and routers and to NAMs. A switch or router device can be added to the system only if it currently hosts a NAM. Additionally, since the functional emphasis of Cisco PVM is centralized NAM management, the NAM home page displays NAM device information only.

Collection Overview

Collection interval is system wide and ranges from 1 – 60 minutes. SNMP Data is collected from: Interface Tables, RMON1, RMON2, SMON, DSMON, ART MIBs. Configuration information is read from the application data store at the beginning of every collection cycle and collection for new devices is initiated, if necessary, by launching new collection agents.

Traffic statistics are cached when they are collected, and the database is updated only if a ‘delta’ is found from the previously collected data. This minimizes database updates.

The default collection interval is 5 minutes, and can be reset under **Setup > Preferences**. This collection cycle applies to all NAMs, switches, and routers you have set up in the system. Additionally, NAMs available in Cisco PVM can have data collections (and therefore report aggregation statistics) turned on or off to isolate network traffic problems or analyze the hardware setup.

It is important to note that although Cisco PVM automatically begins collecting traffic statistics for a NAM as soon as it is added to the system, collection of data in the ART database occurs only if you have set up one or more ART Groups under **ART > Setup**. A Reporting Interval value is available for each ART Group you create that sets the ART–related data polling interval for the NAM device included in the ART Group.

Traffic statistics

Cisco PVM uses both a NAM adapter and a switch/router adapter to collect data. The system allows users to set a system–wide collection interval that controls the frequency of the data collection by waiting for the interval between completion of a collection and the start of the next. The adapters monitor performance data from all the data sources on devices that have been set up in Cisco PVM, such as SPAN and NetFlow Data Export (NDE), on the NAMs as well as the VLANs and ports on the switches and routers.

The following MIBs supply performance data to PVM:

- **Interfaces**
- **RMON1**
- **RMON2**
- **SMON**
- **DSMON**
- **Application Response Time (ART)**

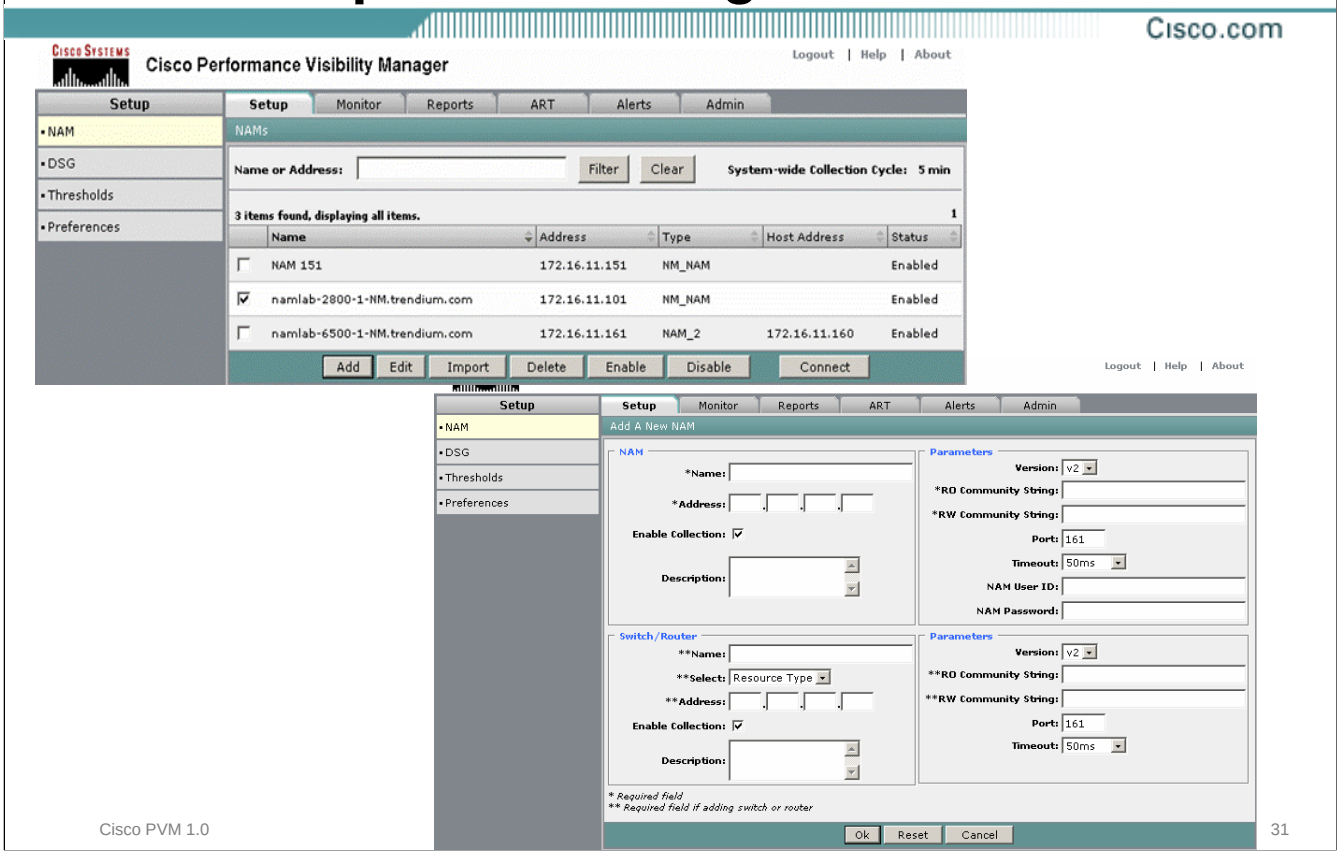
The following statistics are collected by the NAM Adapter:

- **Application–level conversation**
- **Client–Server Response Time**
- **Layer 3 host (IP host)**
- **Layer 2 host (MAC host)**
- **Application Protocol**
- **Differentiated Service Code Point**

The following statistics are collected by the Switch/Router Adapters:

- **Interface statistics if the router is hosting the NAM or**
- **Ethernet and VLAN statistics if the switch is hosting the NAM.**

NAM Setup - Add through GUI



Cisco PVM 1.0

31

NAM Setup

PVM allows the user to setup devices in two ways:

- Adding through GUI
- Importing via a CSV File

Add NAM through GUI

The Setup tab defaults to the NAMs window, where all functions for adding or modifying NAMs and their supporting devices are available, including an access button for the NAM Traffic Analyzer. You may want to edit a NAM to add its supporting device (switch or router) information, or to include the ID and password for signing on to the NAM Traffic Analyzer from links in reports.

You might use the Enable/Disable functions on the NAMs screen to troubleshoot collection problems by shutting down or re–enabling collection for one or more specific NAMs. The System–wide Collection Cycle defaults to five minutes; this cycle is set under Setup > Preferences.

You can add a NAM individually using the Add A New NAM window in the Setup GUI or import NAMs from Device Credential Repository Exports. If you choose to add a NAM without adding its supporting switch/router information, you'll see a hyperlink in the Edit NAM window, beneath the NAM and Parameters sections, that says, "Add Switch/Router." Clicking the link opens the Switch/Router and Parameters sections so that the window appears similar to the figure above.

NAM Setup – Import from CSV file

Cisco.com

- **Import file formats**

DCR Export File

```
>#Wklv#ilch#lv#jhqhudwhg#e|#GFU#H{sruw#kwldw|
Flvfr#V|vwhp v#Q P #Gdwd#p sruw/#Vrxufh@GFU#H{sruw#W|sh@GFUFVY>#Vhuvlrq@613
>
>Vwduw#r i#Vhfwlrq#3#DEdvlf#Fuhghqwldov
>
>KHDGHU=p dqdjhp hqwblsbdgguhvv/krvwbqdp h/grp dlqbqdp h/ghylfhblghqwlw|/glvsod|bqdp h/v|vR emnfwG/gfubghylfhbw|sh/
p glbw|sh/vqp sby5burbfrp p bvwulqj/vqp sby5buz bfrp p bvwulqj/vqp sby6bxvhublg/vqp sby6bsdvvz rug/vqp sby6bhqjlqhblg
/vqp sby6bdxwkbdqjrulwkp /sulp du|bxvhuqdp h/sulp du|bsdvvz rug/sulp du|bhqdednbsdvvz rug/kwwsbxvhuqdp h/kwwsbsdvvz ru
g/kwwsbp rgh/kwwsbsruw/kwwsvbsruw/fhuwbfrp p rqbqdp h
>
431::153<194////431::153<194/4161914171411<18173/3/59;76;3;8///xvhu5/xvhu5//P G 8/xde/xde//////
>Hqg#r i#FVY#ilch
```

User–Defined Export File

```
>#Wklv#ilch#lv#fuhdwhg#e|#wkh#xvhu
>KHDGHU=p dqdjhp hqwblsbdgguhvv/vqp sby5burbfrp p bvwulqj/vqp sby5buz bfrp p bvwulqj/kwwsbxvhuqdp h/kwwsbsdvvz rug
4:5149144134/sxedf/sxedf/dgp lqlvwudwru/dgp lqbsdvvz rug
```


Import from CSV File

Clicking the Import button from the NAMs window opens the Import NAM dialog. From the dialog, you can browse to a local CSV file, then upload it to the PVM server. The system runs a daemon that checks for new device information once per minute.

Only devices that do not already exist in the system will be imported. If a device already exists in Cisco PVM, the system logs an exception to the system log table.

The import process will list the status of the import in the Alerts page. Since the import process takes up to a minute to start processing the import file, click refresh on the Alerts page after a few minutes to see the status of the import.

To import device attributes and credentials for NAMs and their associated switches and routers, you can use:

CSV files generated by the CiscoWorks DCR Export Utility (DCR v3) or

User–defined CSV files containing a header record that specifies the meta data for describing and parsing the file.

DCR v3 Files

The Cisco PVM Import Manager supports keywords in CSV files generated by the CiscoWorks DCR Export Utility, including:

- **management_ip_address**
- **host_name**
- **domain_name**
- **display_name**
- **snmp_v2_ro_comm_string**

Troubleshooting Device Setup

The following general guidelines should be followed when setting up devices in Cisco PVM:

- Ensure the NAMs are collecting the data you want to see.
- Make sure you have created data source groups that have the appropriate data sources.
- Check the Alerts to see if there are any issues that have been reported as causing a problem.
- If you see any SNMP Timeouts for devices, change the Timeout value in the Device setup page.
- Ensure that you can ‘ping’ the devices from the machine hosting Cisco PVM.
- Make sure that you have checked the ‘Enabled’ checkbox for the device.

For more detailed troubleshooting help, refer to Online Help or the Cisco PVM Troubleshooting Guide.

Data Source Groups

Cisco.com

- **Data sources in PVM**
- **Data Source Group(DSG)s**
- **Managing Data Source Groups**

Data sources in PVM

In the context of Cisco PVM, a data source is a source of data that PVM can monitor and use for collection and reporting of traffic statistics. NAMs collect statistics from different data sources. For example, SPAN sessions, NDE exports, and RSPANs can all be considered NAM data sources.

Cisco PVM can collect information from any data source that the NAM is monitoring. The information collected for these data sources come from the MIBs that the NAM supports. Cisco PVM can collect information for switch ports and their associated VLANs. The information collected for VLANs comes from the SMON MIB. Ethernet statistics are collected from the RMON MIB and Interface information from the MIB II Interface table. Cisco PVM can also collect information for associated router interfaces. The information for the Interfaces comes from the MIB II Interface table.

Collection for the associated devices (Switches and Routers) follows these rules:

If the device supports mini–RMON, the statistics will be collected from the EtherStats table in the RMON MIB as well as the MIB II Interface table. So in the case of the Catalyst 6500 Switch and 7600 Series Router, Cisco PVM will display Ethernet statistics, and Interface statistics.

If the device does not support mini–RMON, as in the case of the 2800/3800 Series Edge Routers, statistics are collected from the interface (ifTable) table specified in MIB II. In this case, Cisco PVM will display the interface statistics only.

Data Source Groups (DSGs)

A Data Source Group (DSG) is a logical collection of raw data sources that can be customized into groups for NAMs, switches, and routers. Cisco PVM uses DSGs to calculate statistics over multiple data sources. DSGs are essential for Monitoring and Reporting functionalities, as well as for setting up Thresholds.

There are two types of DSGs :

- **NAM Type – a group of data sources from NAMs**
- **Switch/Router Type – a group of data sources from Switches and Routers**

When creating DSGs, include data sources that carry traffic you want to monitor and ensure that the data makes sense if aggregated. Because of the reasons outlined in the last section, exercise care when grouping Switches and Routers in data source groups. If you group a Edge Router data source with a 7600 Series Router data source or a Catalyst 6500 Series Switch data source, you will see only the Edge Router data source in Interface reports and the other two data sources in the Ethernet Statistics and Error reports.

Default Data Source Groups

Cisco PVM creates default data source groups whenever a switch or router is added.

- When a Router is added, a default ALL_INTERFACES group is created.
- When a Switch is added, in addition to the ALL_INTERFACES group, a default ALL_VLAN group is created.

Note: Although PVM allows you to group together Switch and Router data sources, there is no Aggregated view for Switch/Router data source groups, since Switches and Routers do not support the same set of statistics.

You can view the default DSGs using the DSG Edit function under the Setup tab, but these DSGs cannot be modified. You can, however, add, edit, and delete your own DSGs for switches and routers.

Switch/Router DSGs

Switch/Router DSGs can be chosen when viewing reports in the Switch/Router or the VLAN suites under the Monitor or Reports tabs. You can also choose these DSGs, including the defaults and any new DSGs you've created for Switches or Routers, when defining Thresholds for Switch/Router or VLAN statistics. Data sources for switches and routers are the interfaces in the SNMP Interface table. They can be Ethernet ports, Ether Channels, or VLANS.

NAM DSGs

You can add, edit, or delete a NAM DSG under the Setup tab. Examples of data sources available for NAMs include:

- NetFlow
- WLAN–Monitor
- ERSPAN
- NDE (NetFlow Data Export)

Adding DSGs

The Add a New Data Source Group window allows you to create DSGs for multiple NAMs or switch/routers. The system will not, however, allow creation of a DSG:

- with the same name as an existing DSG
- starting with the name "SYSTEM_" or
- that contains the same set of data sources as an existing DSG.

The system will not allow creation of two DSGs with identical devices and data sources. However, you can add data sources across multiple NAMs or switch/routers in a single window. After you assign data sources to the group from one device, you can select another device of the same type and add its data sources to the group also.

Data Source Group Views

The Cisco PVM GUI allows you to select key traffic views based on NAM aggregation data types using a drop–down menu available in the parameters panes for Monitor and Reports. Once you select a DSG, then you'll select a view based on the data you want to see collated in the report. These *data views* are found next to the DSG drop–down lists in both the Monitor and Reports parameter panes.

Note: The Data Source view is sometimes called the *single* view. The PVM GUI always lists this view, however, as Data Source. The All NAM view becomes *All Device* when a switch or router DSG has been selected for the report.

Report Types

Data views represent which data sources PVM will use in a report. They differ from the *report types* – such as Cumulative Rates, Current Rates, or TopN – that define the format of the displayed report. The displays can be either graphical (TopN) or tabular (Rates). Both the data view and report type drop–down lists are adjacent to the DSG drop–down in the Monitor and Reports parameter panes.

You can select which data to view on generated reports:

- Data Source – a single, specific data source from the selected DSG
- All NAM – data sources grouped by each NAM defined in the selected DSG
- Aggregated – a combined view across all NAMs in a Data Source Group

These data views can be represented schematically.

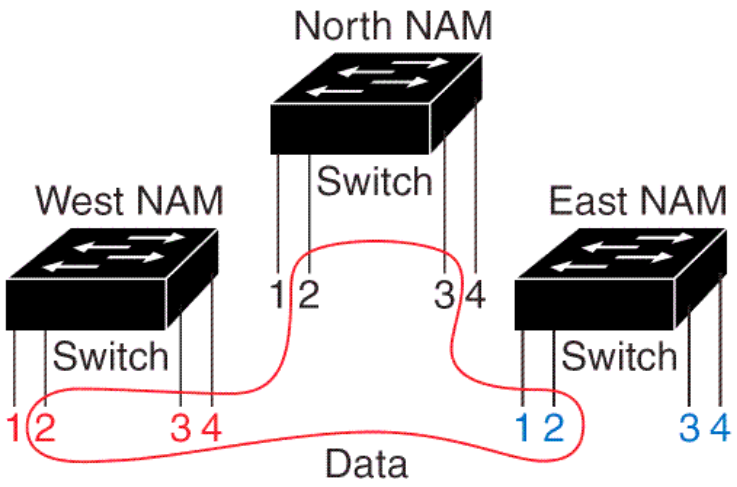
Data View Schematic

The red line in the above figure encircles theoretical data sources from specific NAMs as defined in the DSG:

Sources 2, 3, and 4 are from the NAM named "West".

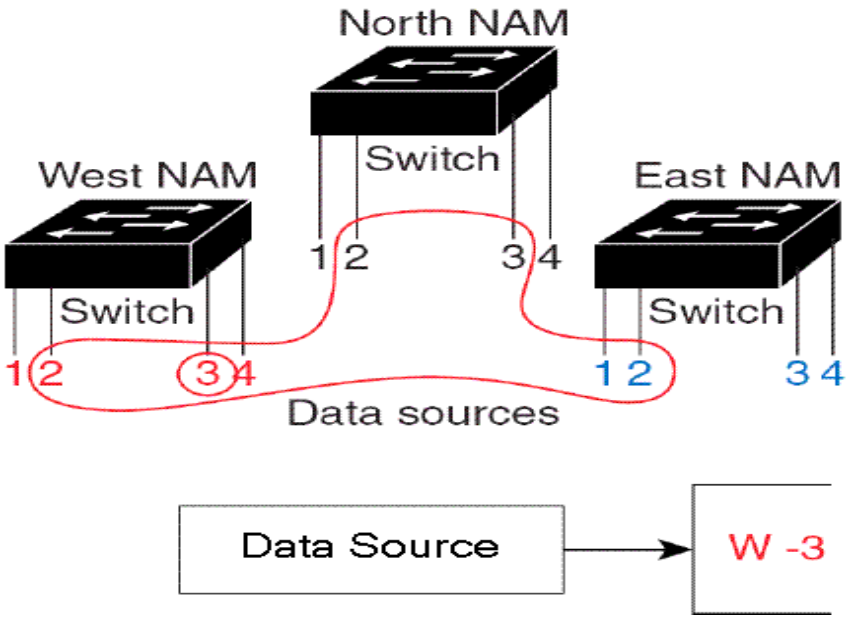
Sources 2 and 3 are from the North NAM.

Sources 1 and 2 are from the East NAM.



Following are examples of the three data view types based on these theoretical NAMs and data sources. The figures depict which data sources from the DSG are included in each of the data views.

Data Source View



The red circle in this figure indicates that data from only a single data source (W3) from the selected DSG will be used to generate the report. The data coming from W3 is a subset of the selected DSG, which contains all the data sources from all the NAMs that are encircled by the red line in the figure. When specifying report parameters in the PVM GUI, you would select the DSG containing the data sources shown above, then select Data Source from the drop–down list next to the selected DSG.

When you select a DSG and the Data Source to run a report in PVM, the system automatically populates an additional drop–down list that displays all of the data sources defined for that DSG. In the case above, you would:

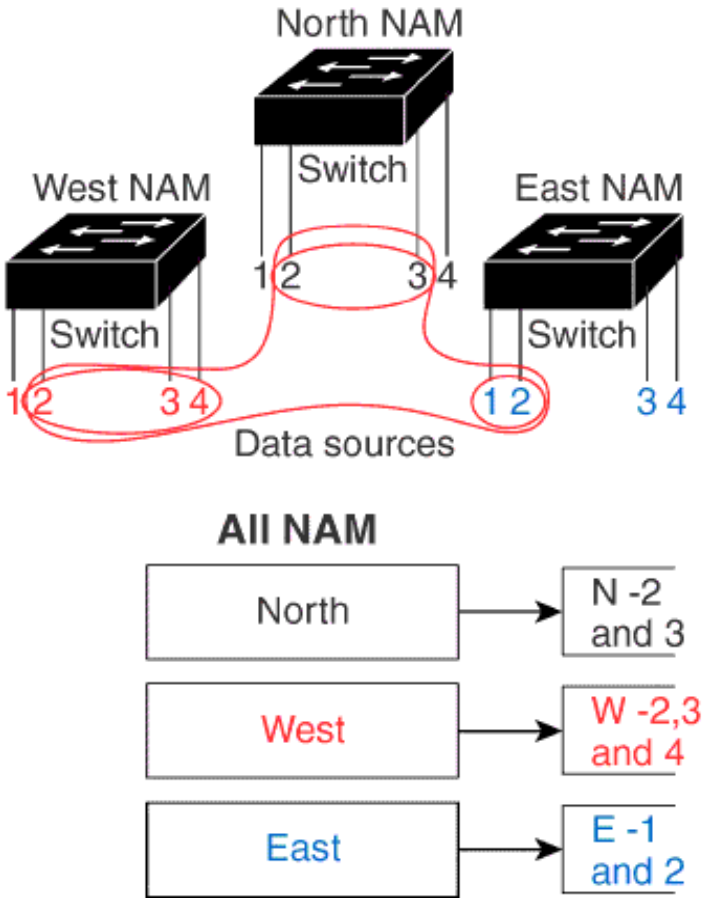
Select the DSG.

Select Data Source as the data view.

Select W3 from the Data Source drop–down list (in the Reports parameters pane, this list lies adjacent to the data view selection).

To determine which DSG you want to select initially, you could also view the individual DSGs defined under Setup > DSG.

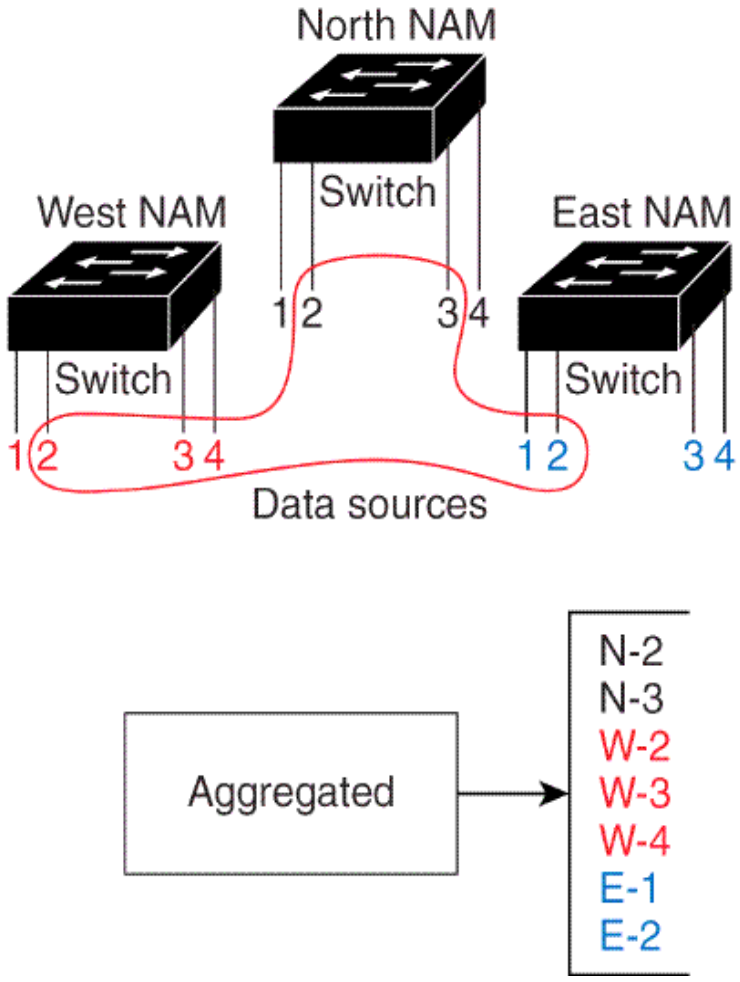
All NAMs View



The red ovals in the figure above show that data sources from all of the NAMs defined in the selected DSG will be used to generate the report. In this case, if multiple NAMs have been defined in the DSG, the report will display the data from each NAM on separate pages, which you can navigate through using the links in the report header. The individual NAMs are also listed in the TOC.

Note: This view is called *All Device* in the report parameters when a switch or router DSG has been selected for the report.

Aggregated View



This figure shows that the entire DSG has been selected for generating the report. Here, PVM generates a report that shows data collated for all NAMs in the DSG, rather than displaying a separate page for each NAM. This view is sometimes called the *combined* view.

Note: DSGs containing both switch and router data sources do not support the Aggregated data view.

Cisco PVM Features

Cisco.com

- **Traffic Analysis**
  - **Monitoring**
  - **Reporting**
- **Application Response Times**
- **Alerts**
- **Base-lining**

Traffic Analysis

Cisco PVM allows the user to perform traffic analysis on their network. By collecting, aggregating and correlating the information from various points in the network, Cisco PVM allows the user to see relevant traffic statistics quickly and easily. When the user uses the Cisco PVM traffic analysis features to analyze traffic through their network, the user can answer questions like:

- **Which applications are consuming bandwidth?**
- **How much bandwidth is consumed by business–critical applications versus recreational traffic?**
- **Who is talking to whom? And from what locations?**
- **What is the distribution of traffic over a period of time?**
- **What is the typical utilization of your LAN links?**
- **What applications are running in the network?**
- **What is their current performance?**
- **What are the load and distribution statistics for these applications?**
- **Which applications are talking to whom?**
- **What are the QoS policies?**
- **What is the duration of the conversations?**

Cisco PVM also allows the user to perform advanced analysis of the traffic in the following ways:

TopN Analysis

Cisco PVM allows the user to look at the Top N figures for the following categories:

- **Hosts – Analyze which hosts are overloaded**
- **Conversations – Analyze who is talking to whom**
- **Protocols – Analyze what protocols are being used to do the talking.**

Multi–dimensional Analysis

Cisco PVM also allows the user to perform the following types of analysis to quickly view the relevant information:

- Cumulative Rate Analysis – Analyze traffic based on historical data
- Current Rate Analysis – Analyze traffic based on recently collected data
- Grouped Analysis – Analyze traffic from multiple sources singly, collectively or based on groupings

Monitoring

The Cisco PVM Monitoring feature is useful in obtaining information that is near real-time, i.e., up to 7 days old. This feature is very helpful in troubleshooting issues where information from the past few days needs to be analyzed quickly and efficiently to obtain an idea of traffic patterns and trouble spots. The Monitoring feature has the following characteristics:

- Used for near real–time traffic analysis
- Has an auto–refresh feature
- Displays Trending charts
- Displays Real–Time charts
- Reports are not archived
- Reports run automatically whenever the Monitor tab or a report is selected

Reporting

Cisco PVM provides a Reporting feature which can be used for longer term analysis of traffic. This feature has the following characteristics:

- Used for historical traffic analysis
- Allows scheduling
- Archives reports
- Has Trending and Real–Time charts available

Monitoring versus Reporting Functionality

The following table summarizes the similarities and differences in the functions available under the Cisco PVM Monitor and Reports tabs:

Comparison of Monitoring versus Reporting Functionality

Function	Monitoring	Reporting
General Purpose	Real-time monitoring of data sources	Historical reporting
Available data ranges (report scope)	• Today • Last minute or hour • Date range	• Today • Current week, month, year • Previous day, week, month, year • Previous calendar day, week, month, year • Date range
Overview display	Y	N
Reports Run Automatically	Y	N
Display Auto-Refresh	Y	N
Real-Time Charts link	Y	Y
Trending Reports link	Y	Y
Scheduling	N	Y
Archiving	N	Y

Report Suites

Cisco PVM provides a rich set of report suites in both the Monitoring and Reporting sections. The reports available under the Monitor and Reports tabs differ as follows:

Monitor

- Overview – this is the default report that opens automatically whenever you log in to the system or when you select the Monitor tab.
- Applications
- Hosts (IP) and Hosts (MAC)
- Conversation
- DSCP, DSCP Application and DSCP Host
- Switch/Router Interface, Ethernet Traffic and Ethernet Error
- VLAN ID and VLAN Priority

You can view the Generate Reports menu by clicking the expansion icon in the upper left corner of the Monitor GUI.

Reports

- Applications and Application Details
- Hosts (IP), Hosts (MAC) and Host Details
- Conversation
- DSCP, DSCP Application and DSCP Host
- Switch/Router Interface, Ethernet Traffic and Ethernet Error
- VLAN ID and VLAN Priority

The table below shows the available report suites.

Suite Name	Description
Overview	Displays, in graphic format, the Top N active hosts, Top N active DSCP applications and Top N active applications monitored on the selected DSG.
Applications	Applications reports provide the ability to see which applications are consuming network bandwidth. Reports on the number of packets and bytes for each application protocol.
Switch/Router	Displays Port Name, Bytes, Packets, Broadcast Packets, Multicast Packets, and Errors collected for switches and routers. The Interface report also shows the % utilization of the links.
Conversations	Displays data on the conversation traffic between various sources and destinations. Information displayed includes Source IP address, Destination IP address, Packets, and Bytes/. Reports on Source/Destination IP Addresses, Packets/Bytes.
DSCP	Differentiated Services Code Point reports include data on specific encoded information related to how the packet traverses the network. These reports display data on the Aggregation Group, In/Out Packets, In/Out Bytes, Application protocols, and Host IP address.
Hosts	Host reports provide an analysis of the traffic for each specific host. These reports display data on the Host IP address, In/Out Packets, In/Out Bytes, and Non–unicast, Broadcast and Multicast Packets collected.
VLANs	Displays data on the VLAN ID, Errors, Packets, Bytes, Non–unicast Packets, and Non–unicast Bytes collected.

Monitoring Features

The Monitor tab allows you to monitor resources based on information from a single NAM or from multiple NAMs across the network, in near real time. This gives the operator the ability to monitor specific sections of the network or to access an All NAMs view that displays multiple NAMs across the network for quick comparisons.

Real–Time Charts allow you to perform real–time monitoring of any metric from generated reports.

Trending Reports allow you to perform trend analysis based on historical data from generated reports.

You can click on any of the hyperlinks available in a generated report to:

- Drill–down to a report detail
- Open a Trending Report
- Open a Real–Time Chart
- Open the NAM Traffic Analyzer for the NAM chosen to generate the report

Drill–Down Capabilities

The following table summarizes the reports to which you can drill–down from reports generated under both Monitor and Reports:

Drill-Down Capability

Report Name	Drill-Down Reports Available
Overview	• Host Details • Application Details • DSCP Applications
Applications	Application Details
Hosts (IP)	Host Details
Hosts (MAC)	N/A
Conversations	• Source Host Details • Destination Host Details
DSCP	N/A
DSCP Application	Application Details
DSCP Host	Host Details
Switch/Router	N/A
VLAN ID	Applications
VLAN Priority	N/A

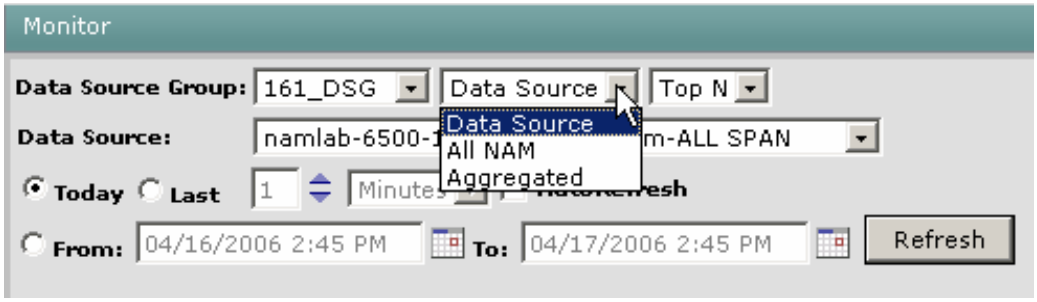
Cisco PVM rep ɔrts:

- Each time you see a Host IP address, you can drill down to the host details.
- Each application allows you to drill down to the application details.
- Each time you see a NAM name, you can click on the name to open a new window for the individual NAM GUI and automatically sign him in.
- Real–time charting drill–down: each time you see an “R” hyperlink, you can click on the “R” to open a new window to monitor this report row details graphed in real–time. Drill–down capability is available on both Data Source view and All NAM view, for all tabular reports.
- Trend Reports drill–down: each time you see a “T” hyperlink, you can click on the “T” to drill down to this report row details graphed against the selected time period. This drill–down capability is available for Data Source, All NAM, and Aggregated views for all tabular reports.

Parameters – Data Views

The reports available under both Monitor and Reports support each of the data views:

- Data Source
- All NAM
- Aggregated



Note: Because switch and router data sources do not support the same set of statistics, data cannot be aggregated for Data Source Groups containing both switches and routers. Therefore, Data Source Groups containing both switch and router data sources do not support the Aggregated view for monitoring and reporting.

Parameters – Report Views

Available Report Types

Report	Tab	Report Type(s) Available
Overview	Monitor only	TopN only
Host Details	Reports only	• Cumulative Rates • Current Rates
Application Details	Reports only	• Cumulative Rates • Current Rates
All other reports	Monitor and Reports	All

The reports you can generate under the Monitor tab can be viewed as either graphical (TopN) or tabular (Cumulative or Current Rates). The only report under Monitor that does not allow tabular views is the Overview report. The value of N – or the number of graph bars that appear in any TopN view – is configurable under Setup > Preferences.

The table above shows Host and Application Details reports, which can be generated directly from the Reports tab Generate Reports menu. They are available through Monitor by drilling down from Applications or Host reports, but do not support the TopN view.

Monitor Navigation Options

The Monitoring page has the following features:

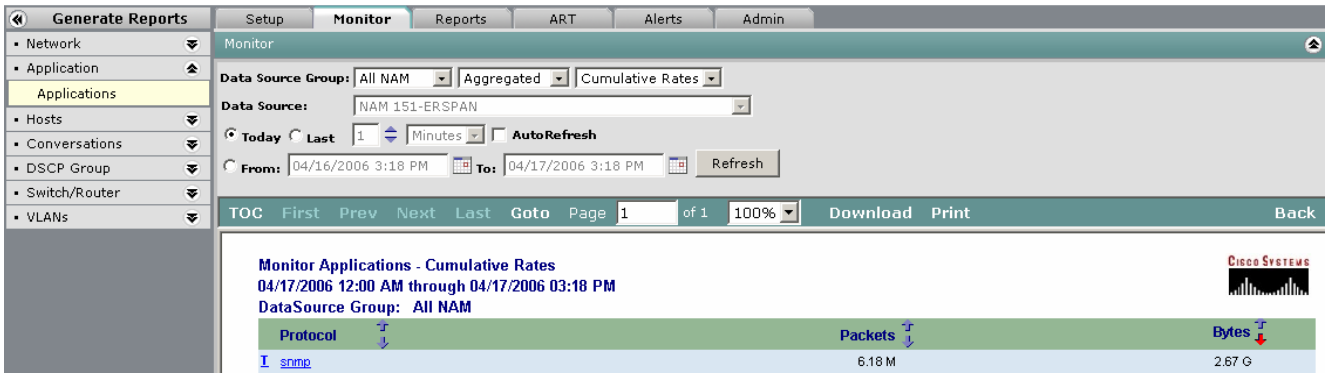
Parameters Pane

Each time you select a report from the Generate Reports menu, the system will generate that report based on the last set of parameters selected in the parameters pane. You can change those parameters at any time by expanding the parameters pane using the icon at the upper right corner of the Monitor GUI. Once you change the parameters, you can either click **Refresh** to regenerate the report, or choose a time interval and check the **AutoRefresh** checkbox.

Report Header Navigation

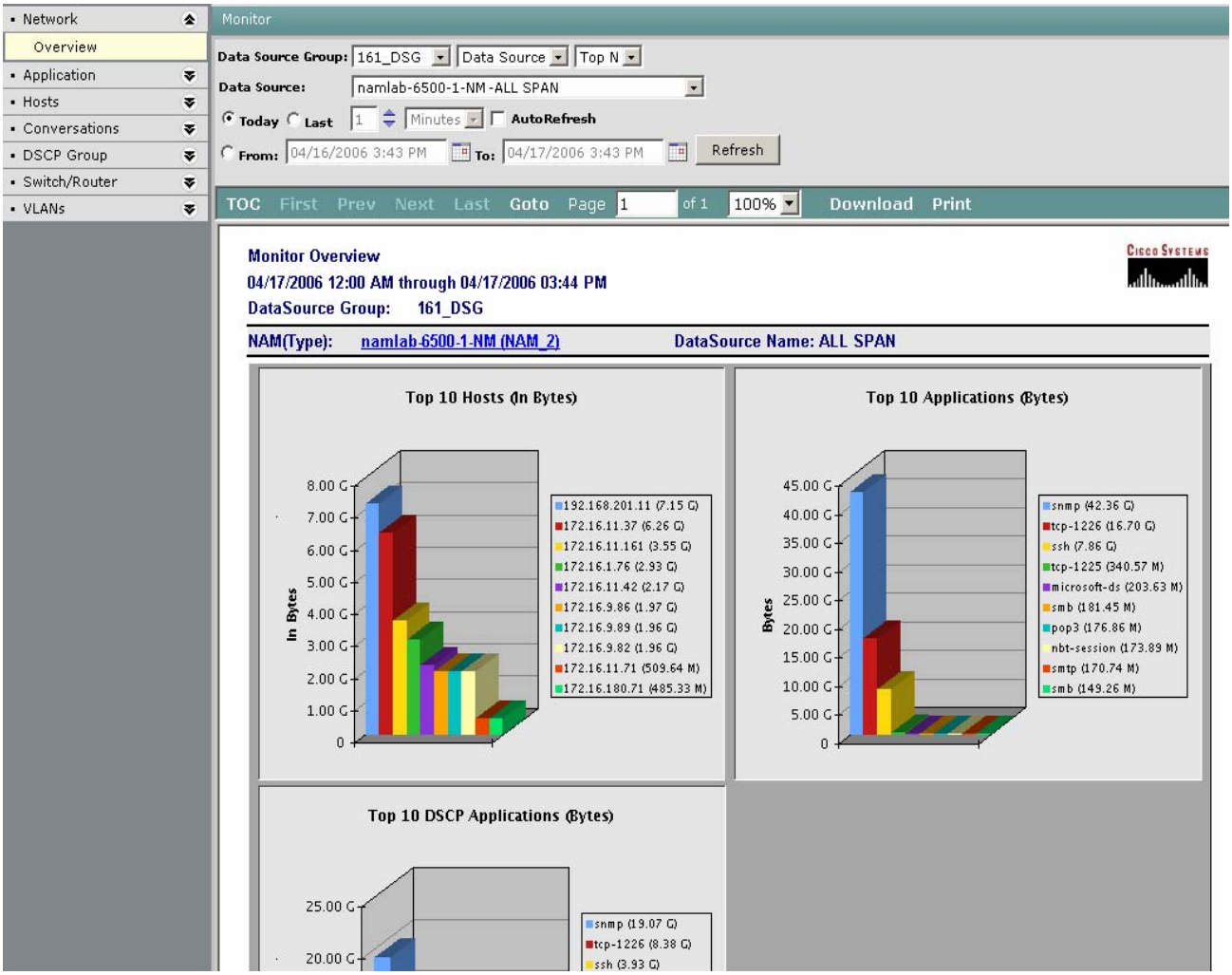
- TOC – Gives a tree–view of the contents in the report.
- First, Prev, Next, Last & Goto – Navigation links to move around in a multi–page report.
- Page Number – You can also directly enter the page number in the text field.
- Size – You can enlarge or reduce the report using the % size drop down
- Print – Print the current report.
- Back – Navigate to the previous report.
- Download – You can download the report and save it in PDF, Excel, or RTF formats.

These are shown in the figure below.



The individual reports and their features are shown in the following pages.

Network Overview Report



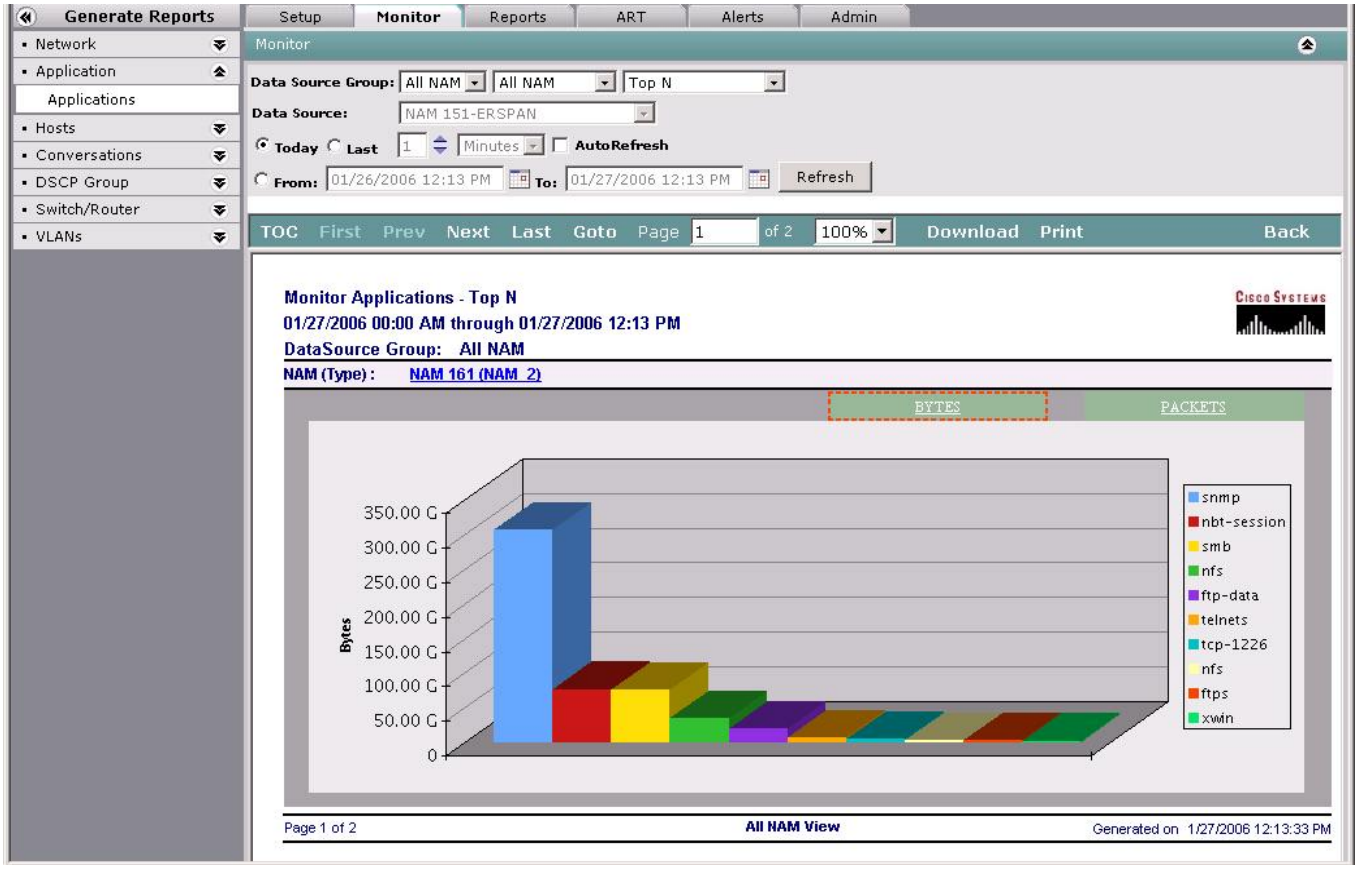
The Overview Report generates automatically using the TopN view, showing the TopN number of:

- Hosts
- Applications and
- DSCP Applications.

When the report opens, the Generate Reports menu and parameters pane are hidden and the report displays the All NAM data view, where no specific Data Source is selected. The above figure shows these expanded, as well as the data view changed to Data Source, the selected Data Source Group and its accompanying Data Source. Note also the hyperlinked NAM name beneath the report title, which opens the NAM Traffic Analyzer for this specific NAM in a new window.

The number (N) of graph bars that appear in each TopN view can be set in **Setup > Preferences** to a value of 1 – 15.

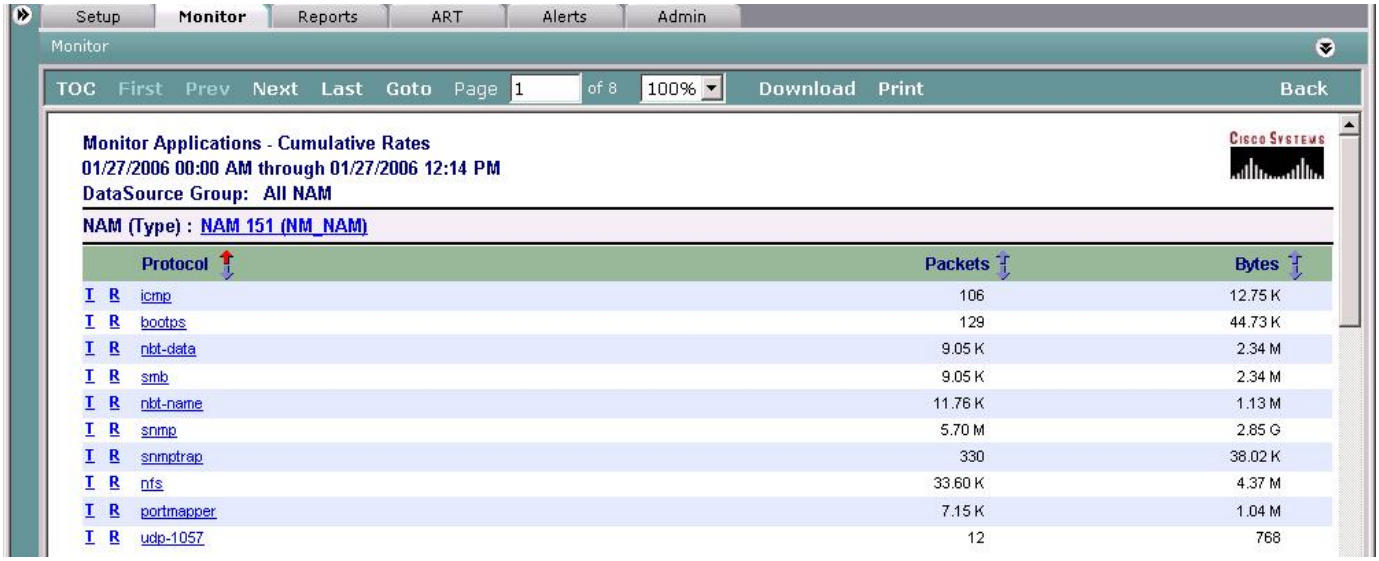
Applications Top N Report



With the exception of the Overview, whenever a TopN report is displayed, you can switch the view between all available metrics. The metrics displayed in tabular report columns appear as links with green backgrounds above the TopN chart. For example, n the case of Applications, these metrics are Bytes and Packets. In the case of Hosts (IP), the available metrics include In Bytes, Out Bytes, In Packets, and Out Packets.

The link to the NAM that appears beneath the report title opens the Cisco NAM Traffic Analyzer, allowing you to probe more deeply into the NAM's configuration, network parameters, diagnostics, and other settings. These NAM links appear in reports for Data Source and All NAM views; Aggregated views show data across multiple NAMs in a Data Source Group simultaneously, and therefore do not display hyperlinks to individual NAMs.

Applications Cumulative Report

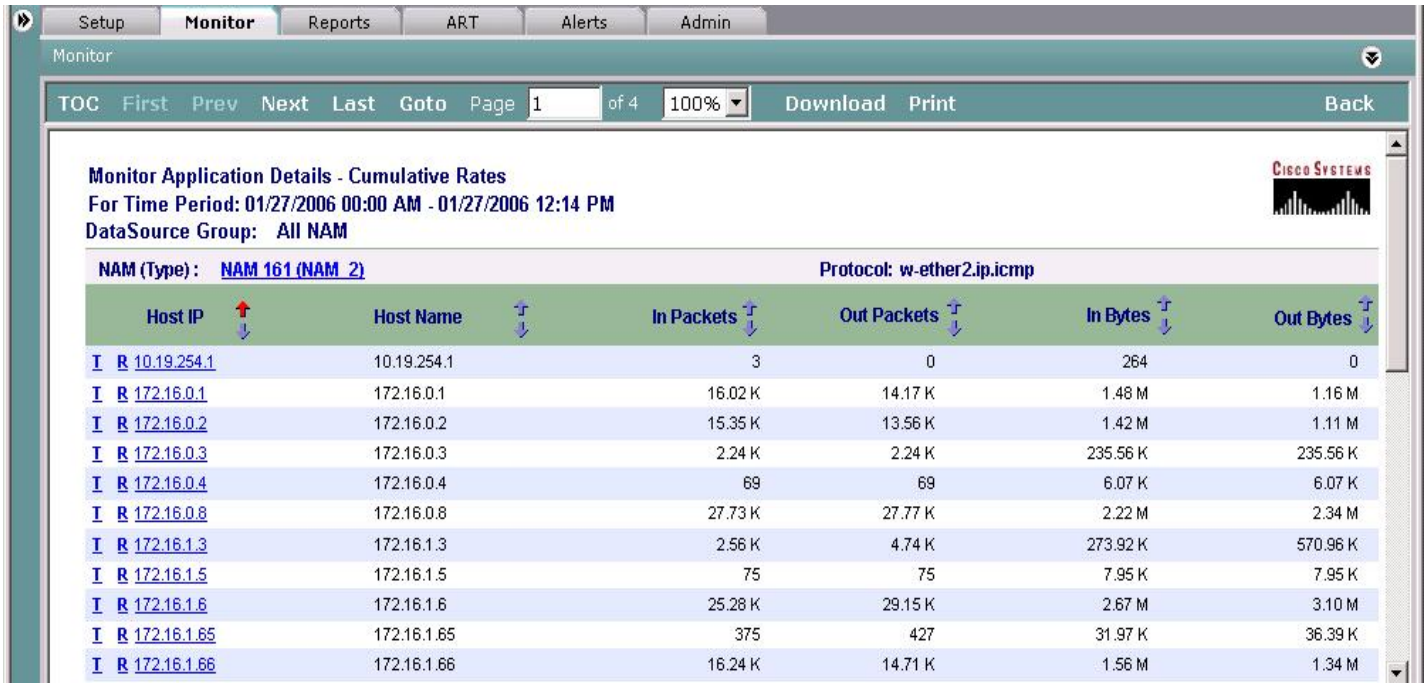


Tabular reports such as the Cumulative Rates report contain multiple interactive elements. In addition to the NAM hyperlink for Data Source and All NAM views, tabular reports also contain sorting arrows in the column headers that allow you to sort metrics and other variables in ascending or descending order. The sort capability can save you time by avoiding navigation through multiple pages of the report to find, for example, the most active protocols in an Applications report.

The “T” and “R” hyperlinks open the Trend Report and Real–Time Chart, respectively, for an individual protocol, host, IP address, DSCP group, VLAN, or device. The Trend Report opens directly in the report viewer, showing raw data for the last 12 hours overlain with a polynomial trend. The Real–Time Chart opens in a pop–up window, displaying true real–time data that is updated every 5 seconds by data source and variable (metric per second rate).

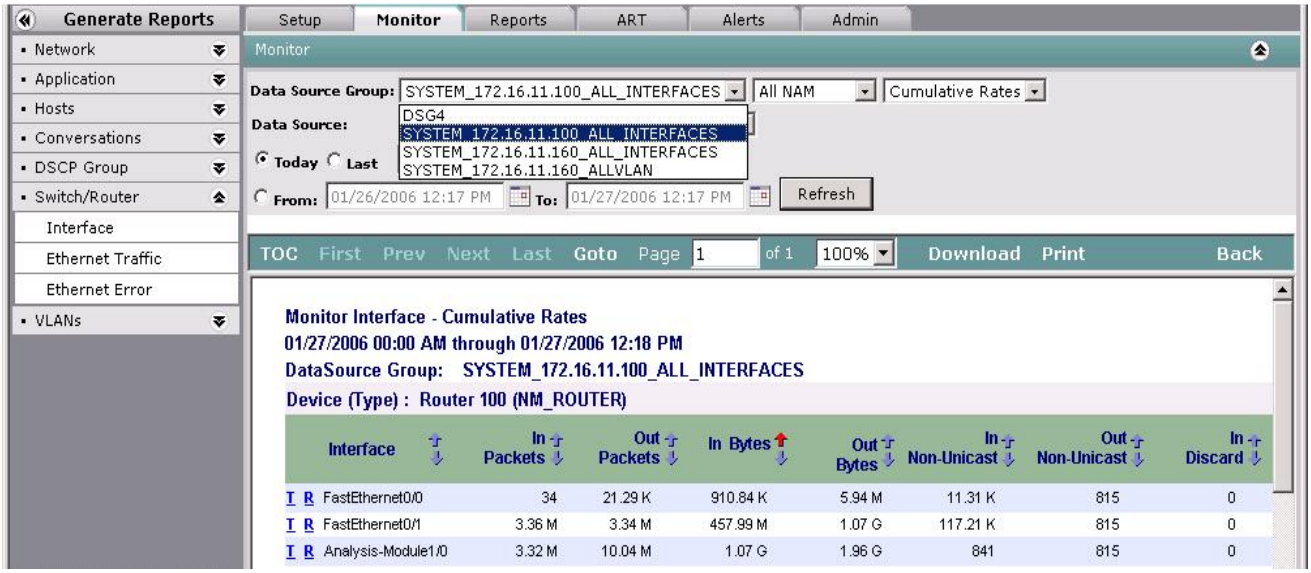
Tabular reports also contain hyperlinks to individual protocols that open the Application Details report for that protocol directly in the report viewer. The details report allows you to view more deeply into the activity of the selected protocol by IP address, as shown on the following page.

Application Details Report



The Application Details report is available in the Monitor GUI only by drilling down from a specific application (a hyperlink in the Protocol column). Notice that from here, you can still view Trend Reports and Real–Time Charts for individual IP addresses, as well as drill–down to the Host Details report for that address. Once again, the Monitor GUI allows you to view Host Details only through drill–down from other reports. Application and Host Detail reports are available from the Generate Reports menu under the Reports tab only.

Switch/Router Report



This suite provides reports on metrics from switches and routers. Reports contain:

- Ethernet statistics if the switch/router supports the mini–RMON MIB.
- Interface statistics if the switch/router does not support the mini–RMON MIB.

Statistics displayed include:

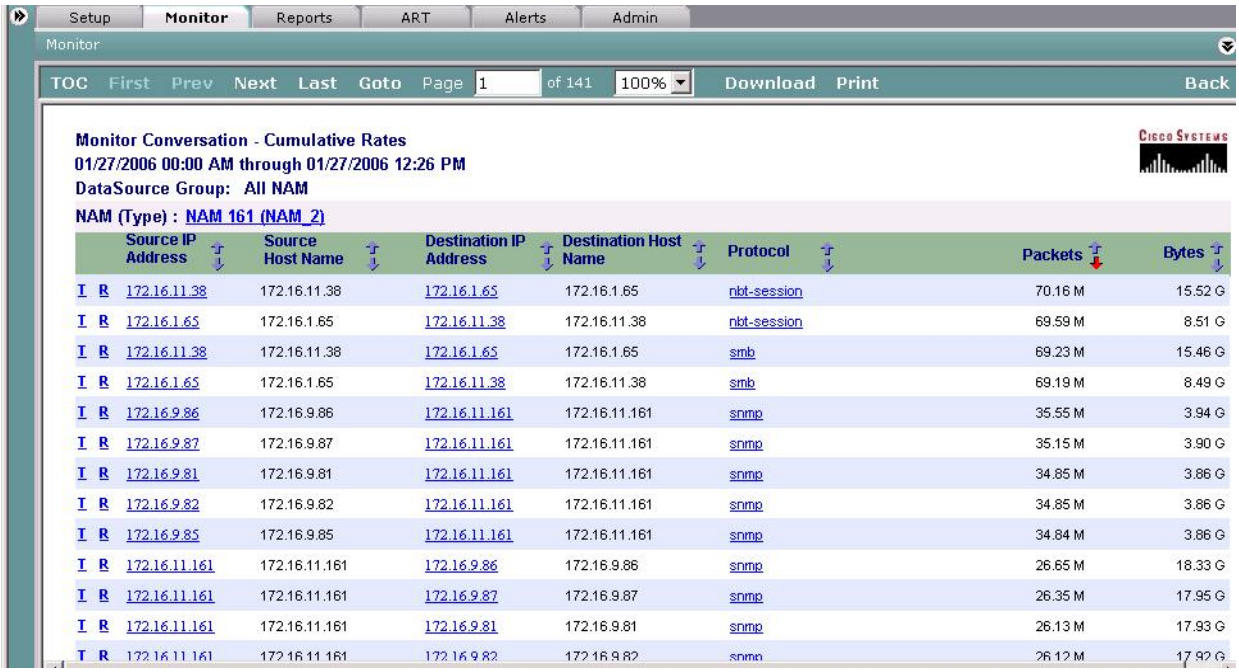
Interface – Reports on the Interface Name, In/Out Bytes, In/Out Packets, In/Out Non–unicast Packets, In/Out Discards, In/Out Errors, and In/Out Link Utilization percentages.

Ethernet Traffic Statistics – Reports on the Port Name, Bytes, Packets, Broadcast Packets, Multicast Packets, and Errors collected.

Ethernet Error Statistics – Reports on the Port Name, Dropped Events, CRC Align Errors, Undersize Packets, Oversize Packets, Fragments, Jabbers, and Collisions collected.

For switches and routers that do not support the mini–RMON MIB, the Interface Report displays in/out traffic, the amount of discarded traffic data, the number of errors, and the percent link Utilization. The interface data collection includes data for both edge and core routers and switches. For switches and routers that support the mini–RMON MIB, the Ethernet Traffic Report displays traffic by NAM and the Data Source Group assigned in Cisco PVM. For switches and routers that support the mini–RMON MIB, the Ethernet Error Report displays detailed errors by NAM and the Data Source Group assigned in Cisco PVM.

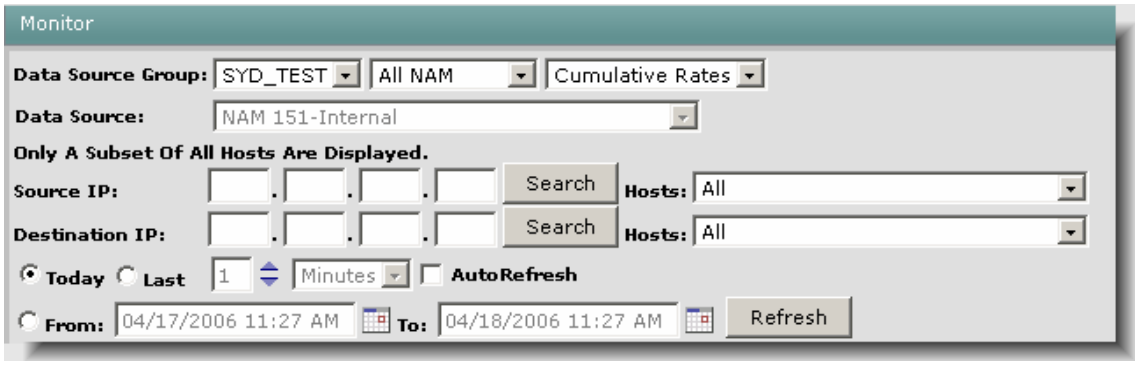
Conversations Report



The Conversations suite contains a single Conversation Report that displays data on the traffic between various sources and destinations. Notice the numerous drill–down links for source and destination IP addresses as well as the protocol. The IP address links open the Host Details report, and the protocol links open the Application Details report.

Since a large number of conversations can occur during a given time period on a single NAM, the Conversation Report normally presents a large number of pages. You can reduce the number of pages in the report by either shortening the reporting time period or by reporting on specific hosts only. You can do this by adjusting your selections in the parameters pane, as shown on the following page.

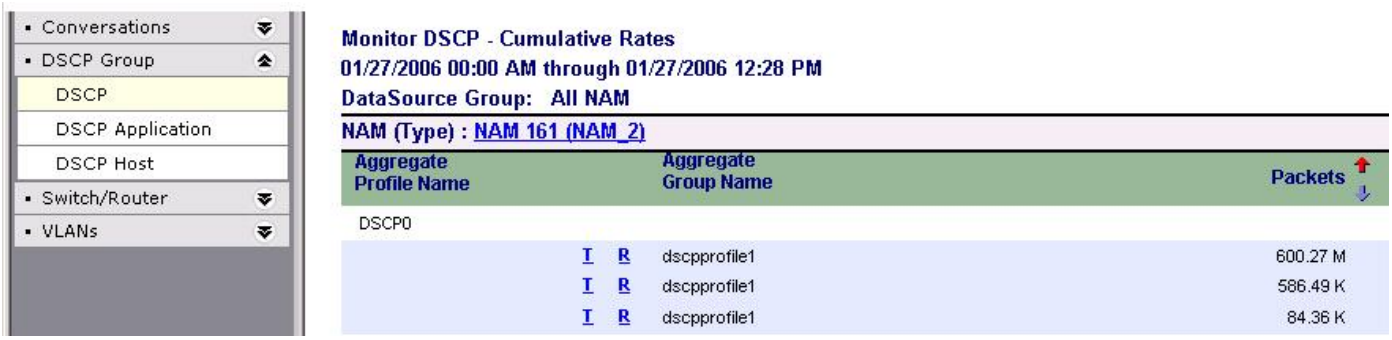
Conversation report parameters



To limit the number of conversations in a single report, you can search for specific hosts by IP address, or select the source and destination IPs from the Hosts drop–down lists. Alternatively, you can select just the Source or Destination address, click **Refresh,** and the resulting report will contain far fewer conversations and be easier to navigate**.**

You can also limit the reporting period used in the data display. For example, you can select the Last 20 Minutes or the Last 1 Hour, click **Refresh,** and the number of conversations is substantially reduced in the report.

DSCP Report



The Differentiated Services Code Point (DSCP) suite reports on specific encoded information related to how a packet traverses the network. DSCP monitoring allows you to validate and fine–tune planning and Quality of Service (QoS) allocations.

DSCP reports are based on the data obtained from the DSMON MIB, which is an extension of RMON–2 that looks into the IP header of every packet to identify the code point that defines how that packet should be handled by DiffServ–enabled devices. DSMON MIB allows creation of DSCP counter aggregation profiles for up to 64 values that can be grouped for aggregation. Each DSCP value may be given a different treatment by a forwarding device, affecting which packets get dropped or delayed during periods of network congestion. The DSCP reports show traffic information for the various configured DSCP aggregation groups.

Aggregation Profiles

By monitoring DSCP bits, throughput for different services can be determined. The DSMON MIB allows different DSCP values to be aggregated into aggregation groups, and associates these groups with aggregation profiles for the following reasons:

- To reduce the number of DSCP counters to monitor.
- Some DSCP values may never be used in a network.
- Different DSCP values may have similar packet treatments.
- To reduce the network management station polling data.

Cisco PVM aggregates the DSCP statistics collected from multiple NAMs. For reporting purposes, Cisco PVM assigns each DSCP profile a unique ID in the database. The system distinguishes one profile from another by examining the definition of each profile. Cisco PVM treats profile definitions as follows:

- If two profiles have the same name but differing DSCP groups, the system will assign a new ID to one of the groups, the data will be aggregated separately, and the groups will appear as two different profiles in the reports.
- If two profiles have the same definition but differing names, the system ignores the name of the new profile and aggregates the newly collected data along with other data belonging to the previously existing profile.

In each case, the system sends an alert that Administrators can view under the Cisco PVM Alerts tab.

Note: Aggregation Groups are configured in the NAM Traffic Analyzer, external to Cisco PVM.

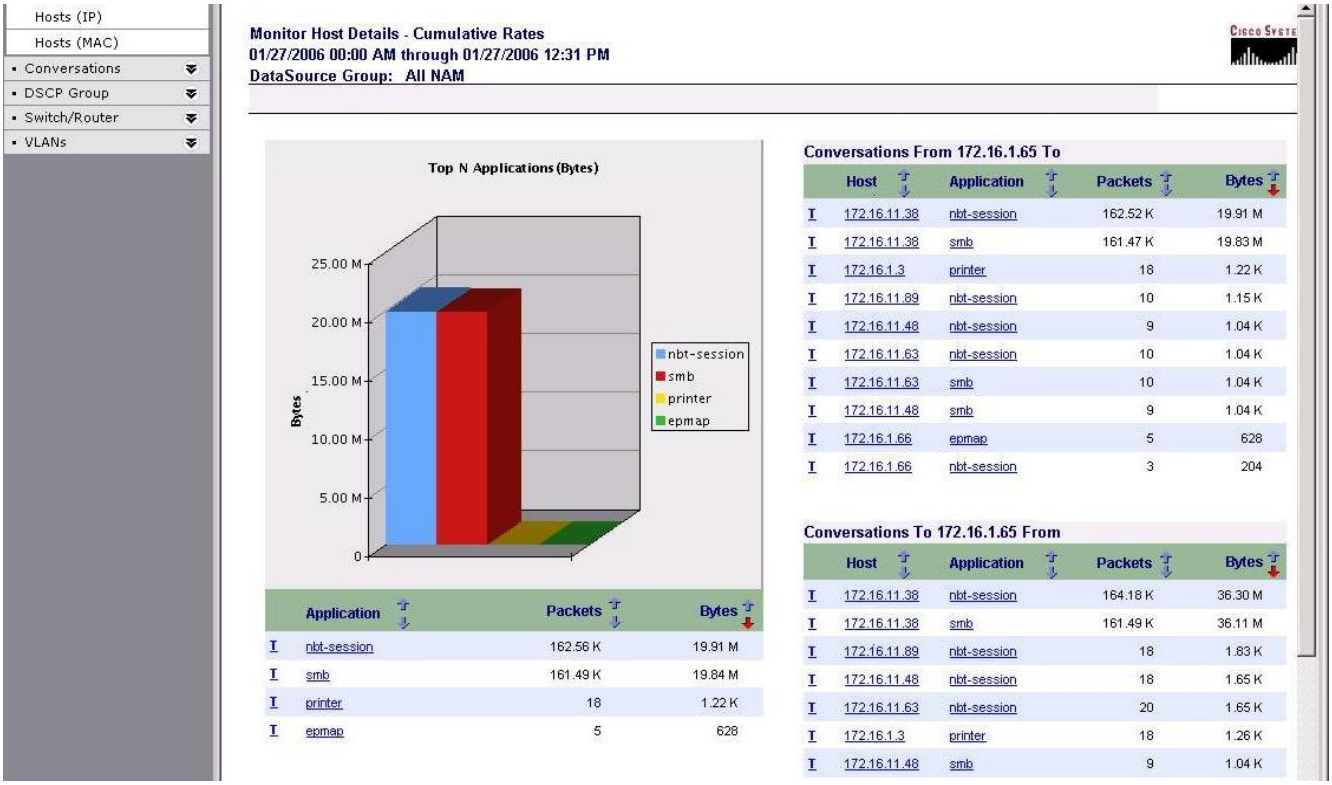
The DSCP Report provides details on the Aggregation Index and traffic. The DSCP Application Report displays details on the Aggregation Index, applications, and traffic. The DSCP Hosts Report displays information on the Aggregation Index, host IP address, and traffic.

Hosts Report

Host IP	Host Name	In Packets	Out Packets	In Bytes	Out Bytes
10.19.254.1	10.19.254.1	3	0	264	0
10.254.27.220	10.254.27.220	80	83	8.24 K	8.53 K
128.118.25.5	128.118.25.5	3.52 K	0	341.66 K	0
144.160.131.17	144.160.131.17	26.61 K	24.10 K	2.10 M	32.34 M
172.16.0.1	172.16.0.1	19.74 K	23.62 K	2.12 M	2.59 M
172.16.0.2	172.16.0.2	17.60 K	21.32 K	1.65 M	2.03 M
172.16.0.3	172.16.0.3	11.18 K	11.18 K	846.36 K	846.29 K
172.16.0.4	172.16.0.4	9.01 K	9.02 K	614.38 K	614.45 K
172.16.0.8	172.16.0.8	71.24 K	71.27 K	6.52 M	6.75 M
172.16.1.3	172.16.1.3	1.74 M	1.62 M	182.90 M	345.53 M
172.16.1.5	172.16.1.5	156	147	15.71 K	16.01 K
172.16.1.6	172.16.1.6	35.05 K	44.53 K	3.54 M	4.30 M
172.16.1.65	172.16.1.65	150.31 M	150.63 M	32.76 G	26.27 G
172.16.1.66	172.16.1.66	417.16 K	426.85 K	114.96 M	87.66 M

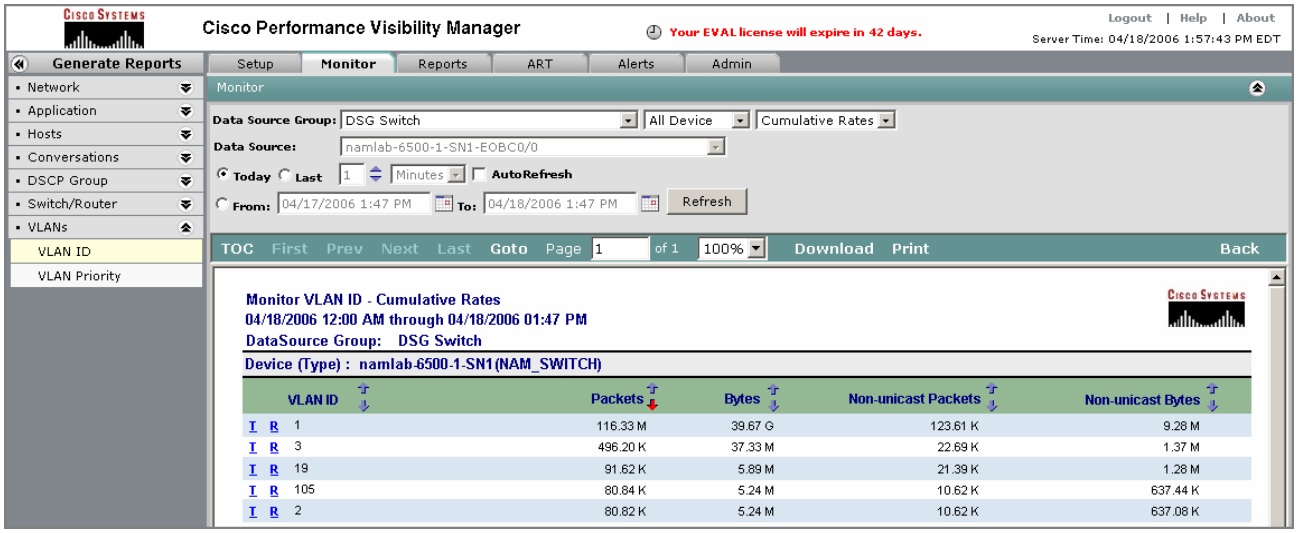
Host reports provide an analysis of the traffic for each specific host, including the host IP and MAC addresses. The Hosts (IP) Report displays traffic information by host IP address. The report contains drill–down links to the Host Details report for individual IP addresses. The Hosts (MAC) Report displays traffic information by MAC address, but does not display drill–down links to a details report.

Host Details Report



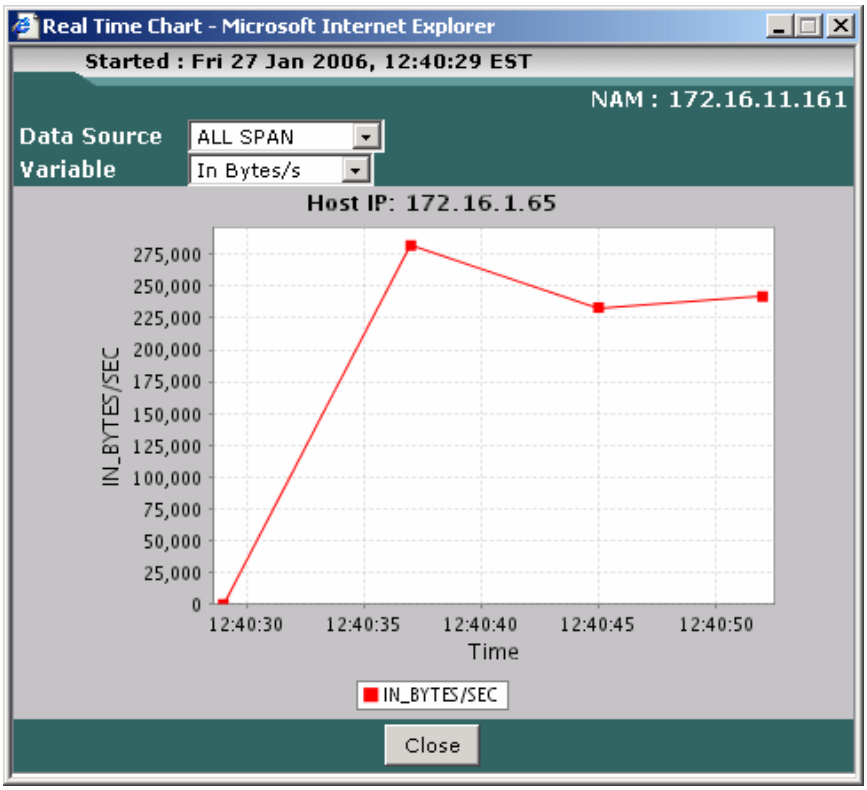
The Host Details Report is available in the Monitor GUI from any report that displays an IP address. In the Reports GUI, this report is available directly from the Generate Reports menu. It displays detailed traffic information by application, including the network address of the host, the name of the application, number of packets collected and number of bytes collected. Drill–down links are also available to detailed reports for applications and other host addresses.

VLAN Report



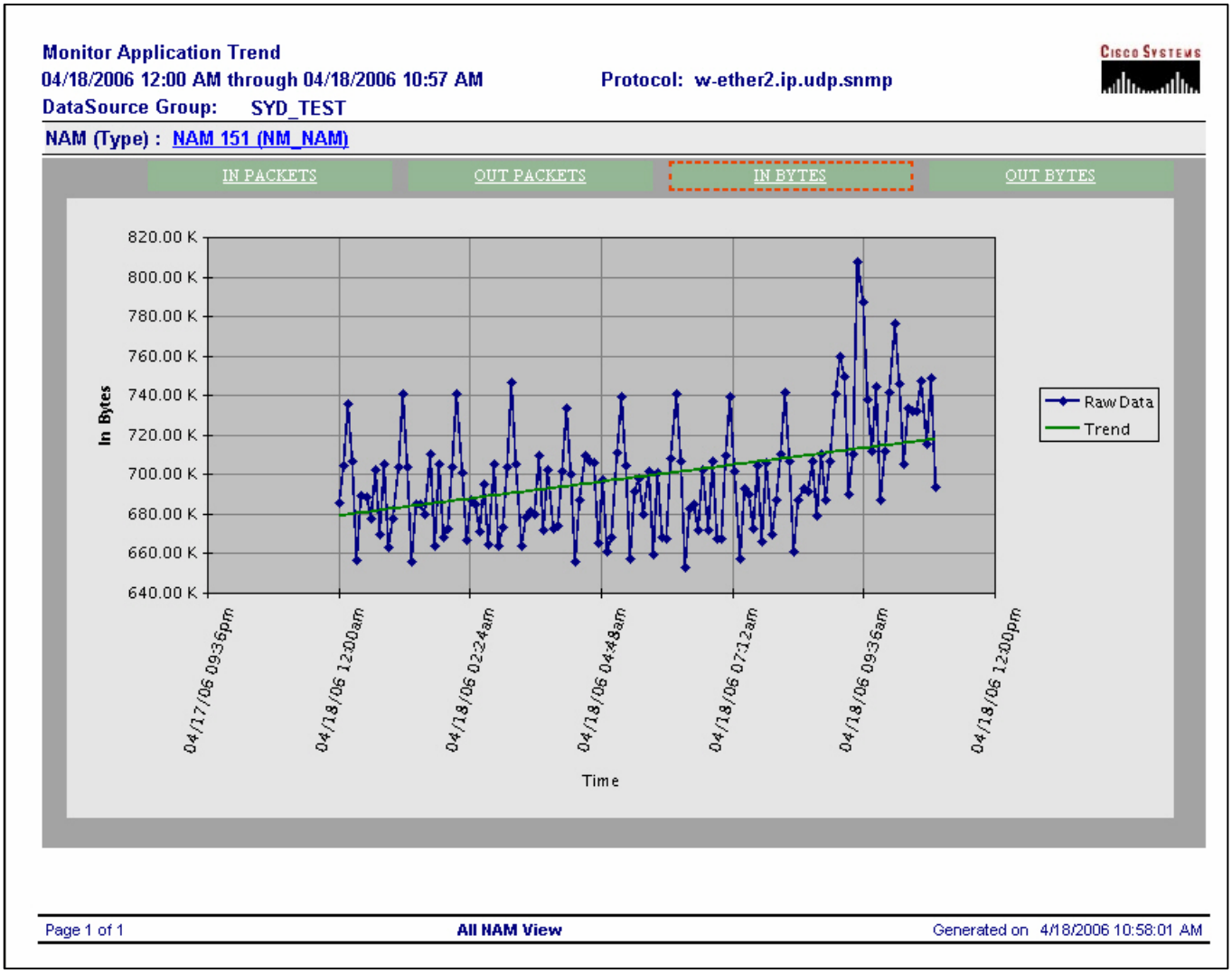
The VLANs suite displays detailed information on data collected for each VLAN ID and VLAN Priority. The VLAN ID Report details traffic collected per second over the selected time interval by VLAN identifier.

Real-time Chart



Real–Time Charts are available from all tabular reports except for those displaying Aggregated data views. Once you open the chart from the “R” hyperlink in the tabular report, you can select another Data Source or Variable (metric/second rate) at any time and the chart will refresh with the new selections automatically.

Trending Chart



Trend Reports are available from all tabular reports. Once you open the report from the “T” hyperlink in the tabular report, Cisco PVM shows the individual data points collected for the given report period and shows the trend for the given period.

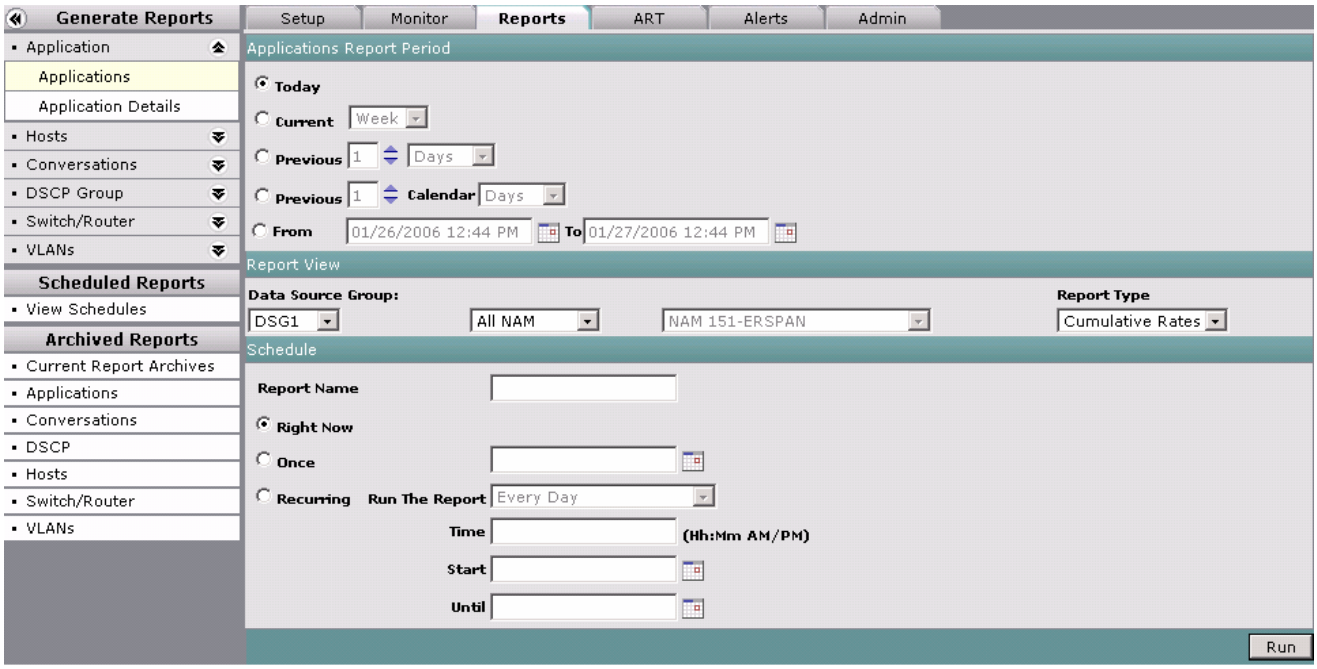
Reporting Features

The Reporting feature in Cisco PVM can be used to perform historical traffic analysis. Cisco PVM retains the collected traffic information for long periods of time, and the user can use the reporting feature to view this data. Reporting features a flexible scheduling engine, which allows you to run reports periodically, at a later date, or right now, on the traffic or statistic you are interested in. Once run, these reports are automatically archived, and available for historical analysis.

The Report feature has the following features:

- Flexible Scheduling.
- Archival of reports.
- Report Portal to view Scheduled, Running and Completed Reports.

Reporting Dashboard



Report Period

The user can choose from the following:

- Today – Run a report for today.
- Current – Run a report for the current week, month or year.
- Previous n – Run a report for the previous n days, weeks, years , taking today into account.
- Previous n Calendar – Run a report for the previous n calendar days, weeks, years
- From – Run a report for the specified date/time range.

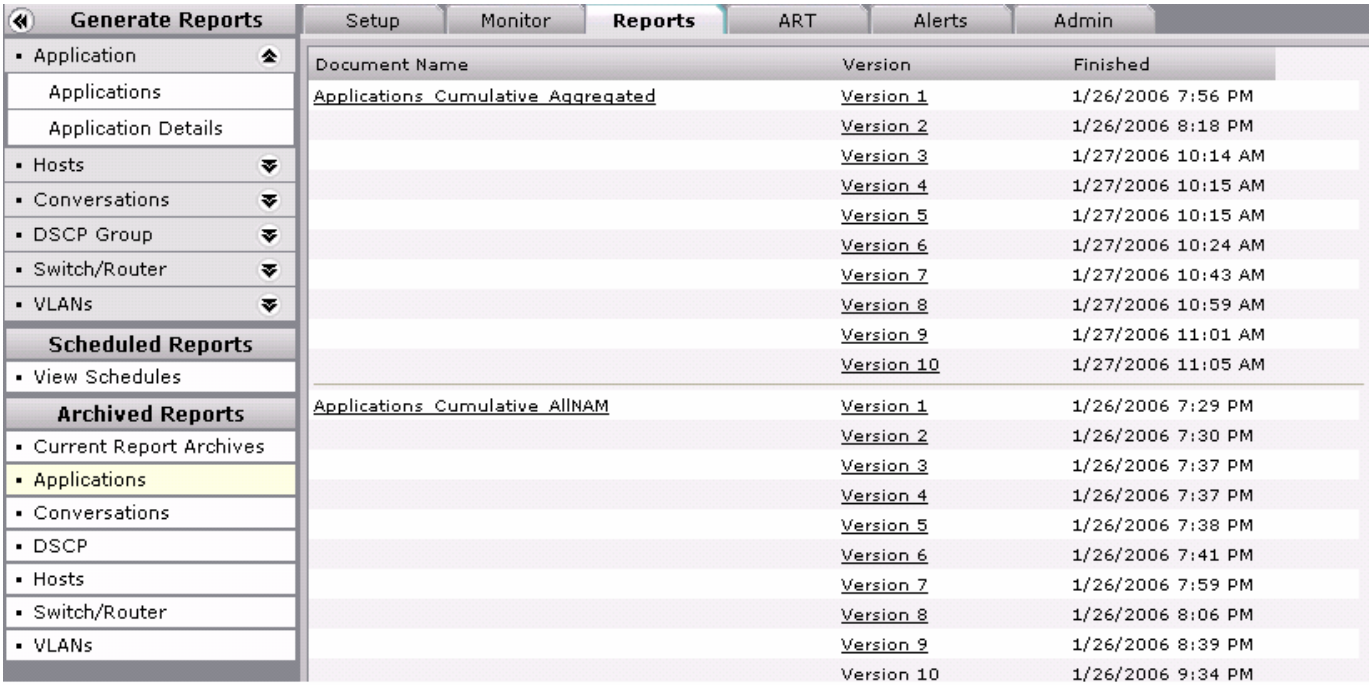
Report View

Select the DSG you want to run the report on and the aggregation scheme you want. If the aggregation scheme is data source, select the data source. Then select the report view you want.

Schedule

You can name a report and specify when you want it to run: immediately, once at a specific date and time, or recurring. Once you schedule a report for a future time point and click **Run**, the report appears under the Schedules tab in View Schedules.

Report Archives



The Archived Reports menu provides quick navigation to the repository of all reports available in the archive database. The first menu item shows the archive for the report currently selected under the Generate Reports menu (such as Application Details or DSCP).

The Report Archive contains a repository of all archived reports for each report suite in the Reports GUI. Following is a sample Report Archive display for the Hosts suite; clicking a Version link opens the report.

Additional report Parameters

The Reports GUI displays an extra section in the report setup window called Report Parameters when you select the following reports from the Generate Reports menu:

- Application Details
- Hosts (IP)
- Host Details
- DSCP Host
- Hosts (MAC)
- Conversation

Each Report Parameters section contains either an extra drop–down list or address box or both. When running an Application Details report, you must select the specific protocol for which you want to see data.

When running a Host Details report, you must select the specific host for which you want to see data; when running either a Hosts (IP) or DSCP Host report, this parameter is optional. In this section, you must either select a specific host from the Hosts drop–down list (Host Details report), or leave the default All selection to return data for all hosts in the Data Source Group (Hosts (IP) and DSCP Host reports).

When running a Hosts (MAC) report, you must either run the report for all MAC addresses in a selected Data Source Group or specify a single address using the Host MAC address block in the Report Parameters section. You can leave the Host MAC address block blank to return a list of all MAC addresses in the Data Source Group you selected, or you can enter a MAC address to see data for that address only.

When running a Conversation report, you must either run the report for all sources and destinations in the Data Source Group or select the specific hosts for which you want to see data in the Report Parameters section. In this section, you can select:

- All sources and destinations (default)
- One source and all destinations
- All sources and one destination
- One source and one destination

Note: You can use wildcards in any of the address blocks to narrow the list of hosts; the Hosts (MAC) address block requires a complete, valid MAC address.

Application response Time

ART allows you to:

- Measure response time at the server and the network to identify if the performance problem is caused by the network or the server
- Measure response times for individual applications, hosts and subnets/locations by correlating application response time data from multiple NAMs
- Visualize Application Response time in near real time
- View current and historical performance data in intuitive tables and graphs
- Troubleshoot Response time problems by drilling down to the appropriate NAMs or devices
- Enable Application Response time collection on NAMs

The ART GUI allows all users to generate Server Response Time, Network Flight Time, Client/Server Investigation, and Client/Server Response Time reports based on ART Groups set up by Cisco PVM Administrators. You can also view report schedules and archives for each report type. Cisco PVM Administrators can set up ART Groups that define aggregation of ART data by data source.

Cisco PVM enables you to troubleshoot performance problems by collecting Application Response Time (ART) data from NAMs and correlating the data to clients and servers. Administrators set up ART data collection definition using defined domains of NAM data sources that have little or no interaction with one another. ART Groups enable you to quickly find relevant NAMs and identify and troubleshoot performance problems.

All Cisco PVM users can generate the following ART reports:

Network Flight Time – enables you to find out whether the network or the server is the cause for delayed responses

Server Response Time – shows the response times for each server in an ART Group

Client/Server Investigation – shows the response times for each client/server pair of a data source in an ART group by client IP

Client/Server Response Time – enables you to check whether a response time problem exists between two sites by showing the response times for each client/server pair in an ART Group created specifically for client NAMs.

Reports you generate under the Cisco PVM ART tab can display aggregated Application Response Time data from the last 24 hours, or from the previous days, weeks, months, or years, depending on when the NAM began collecting ART data.

About Historical Data

Historical ART data associated with a data source is maintained in the database even if that data source is removed from an ART Group. Cisco PVM records the time the data source was removed, but maintains the original data source in ART report search criteria that belong to a time interval during which that data source still existed in the ART Group.

ART Group

Grouping of data sources for which ART collection will occur. The concept is similar to that of Data Source Groups (DSGs), but ART Groups are explicitly for Application Response Time collection.

To monitor response times across the network, you will need to create an ART group which contains data sources from the appropriate NAMs Collection will be enabled on NAMs if not already enabled for the data sources in the ART Group.

PVM uses the NAM default values for response time buckets while enabling ART collection in the NAM. If a data source is present in 2 ART Groups, the second configuration will override the first.

An ART Group has the following features:

- Grouping of data sources for which ART collection will occur. The concept is similar to that of Data Source Groups (DSGs), but ART Groups are explicitly for Application Response Time collection.
- To monitor response times across the network, you will need to create an ART group which contains data sources from the appropriate NAMs
- Collection will be enabled on NAMs if not already enabled for the data sources in the ART Group.
- PVM uses the NAM default values for response time buckets while enabling ART collection in the NAM.
- If a data source is present in 2 ART Groups, the second configuration will override the first.

Understanding ART Groups

An ART Group is defined as a set of data sources for one or more NAMs attached to client and server machines. All ART reports in Cisco PVM are run based on ART Groups created by Administrators. Before creating an ART Group, you should decide:

- which client, server, or client/server pair you want to monitor and
- the data source(s) from the NAMs closest to each client and server that you want to see in the reports.

Cisco PVM displays all ART Groups that have been defined in the system in tabular form under ART > Setup; groups can be added, edited, or deleted from this window. ART data collection is functionally separate from all other statistics, where users create Data Source Groups to view data under Monitor and Reports. In the case of ART, you must create ART Groups if you want to view ART reports. Additionally, ART functionality includes only reporting capability and not monitoring; ART reports function as snapshots of response–time activity.

Creating ART Groups

Creating ART Groups allows Administrators the convenience of being able to quickly select client and server NAMs for monitoring and reporting by limiting the number of relevant NAMs available for selection. The ART Group creation process involves the following steps:

- Enter a group name and description.
- Select the NAM to populate the list of all available data sources.
- Select the NAM data source(s) for which you want to collect ART data.
- Repeat steps 2 and 3 to select more NAMs if desired.
- Specify the Report Interval (in seconds), which specifies the ART–related polling interval for the NAM device.
- Specify the Max Entries value, which represents the maximum number of data points the NAM device can store in that polling interval for ART–related data.
- Specify the Maximum Response Time (in milliseconds).

Caution: If the same data source is added to more than one ART Group, the three parameter values (Report Interval, Max Entries, and Maximum Response Time) must be the same as the other ART Group(s) containing the same data sources to maintain consistency. If you attempt to enter values for a data source that differ between the ART Groups in which it appears, the system will return an error message indicating that the new ART Group cannot be saved because the values you entered don't match those in the previously created ART Group.

ART Data Collection

Cisco PVM automatically begins collecting traffic statistics for a NAM as soon as it is added to the system. However, collection of data into the ART database occurs only if ART Groups have been set up in Cisco PVM. It is important to note that even if the NAM has been configured to collect ART statistics, you will not be able to view the data in ART reports until ART Groups have been set up in Cisco PVM. Cisco PVM is able to recognize whether ART data collection has been disabled for a specific data source, and will raise an alert since data collection has ceased. To restart collection in this case:

- delete and re–apply the data source to an ART Group or
- check whether the data source's attached device needs to be enabled in Cisco PVM Setup or has another problem that requires troubleshooting.

If a data source is part of any ART Group, then PVM will enable data collection for that source. To disable data collection entirely in Cisco PVM, the data source must be removed from all ART Groups.

Note: Historical ART information associated with a data source is maintained in the database even if the data source is removed from an ART Group.

Adding an ART Group

Factors to Consider

- Unless you have a specific need to collect ART data over the long term, ART groups should normally be created for short–term monitoring and troubleshooting of problematic areas of the network to avoid storage of unnecessary or excessive data.
- ART report data will be more meaningful and easier to interpret if you limit the number of data source types you attach to each NAM within an ART Group.
- To generate Network Flight Time reports, it is necessary to include both server and client NAMs in a single ART Group.
- To ensure easier ART Group selection when generating reports, give careful consideration to the name you assign to each group; the drop–down group selection lists in report parameters shows only the group name and not the description.

Note: Although Cisco PVM collects data from both server and client NAMs, the system cannot identify which NAM is closest to each server or client. Therefore, when you generate ART reports, the system lets you decide which NAMs you want to see. If you have a significant number of NAMs, remember that you can name individual NAMs to give them a more meaningful designation when they appear in Cisco PVM drop–down lists.

Report Interval – the ART–related data polling interval by the NAM device, in seconds. The default value is 1800 seconds (30 minutes).

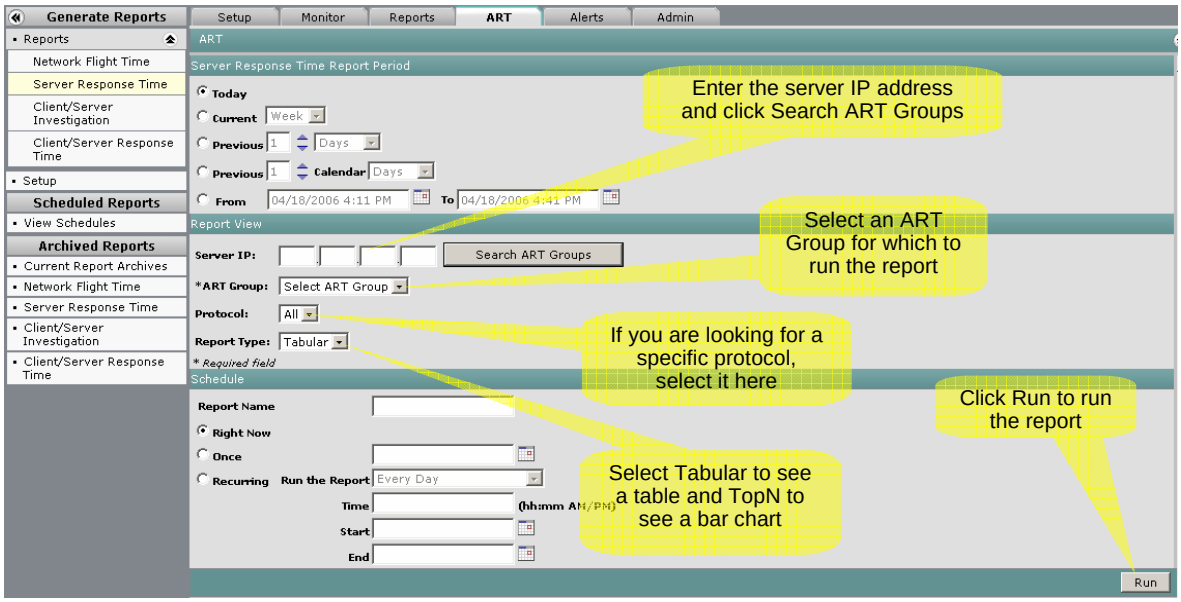
Maximum Entries in Table – the maximum number of data points the NAM device can store in the assigned polling interval for ART–related data. The default value is 500.

Maximum Response Time – the maximum time, in milliseconds, that the NAM will wait for a response between a client/server pair before tagging the data as timed out. The default value is 3000 milliseconds.

The next few pages provide directions on how to generate the reports themselves.

Server Response Time Chart

Parameters



The Server Response Time (SRT) report shows the response times for each server associated with a data source in an ART Group. The SRT report can be used to analyze whether slow network response time is due to a particular server. Since a data source may belong to multiple ART Groups, a selection of ART Group is needed to present the relevant data. You can select a specific protocol, if desired, or view data for all protocols in the selected ART Group.

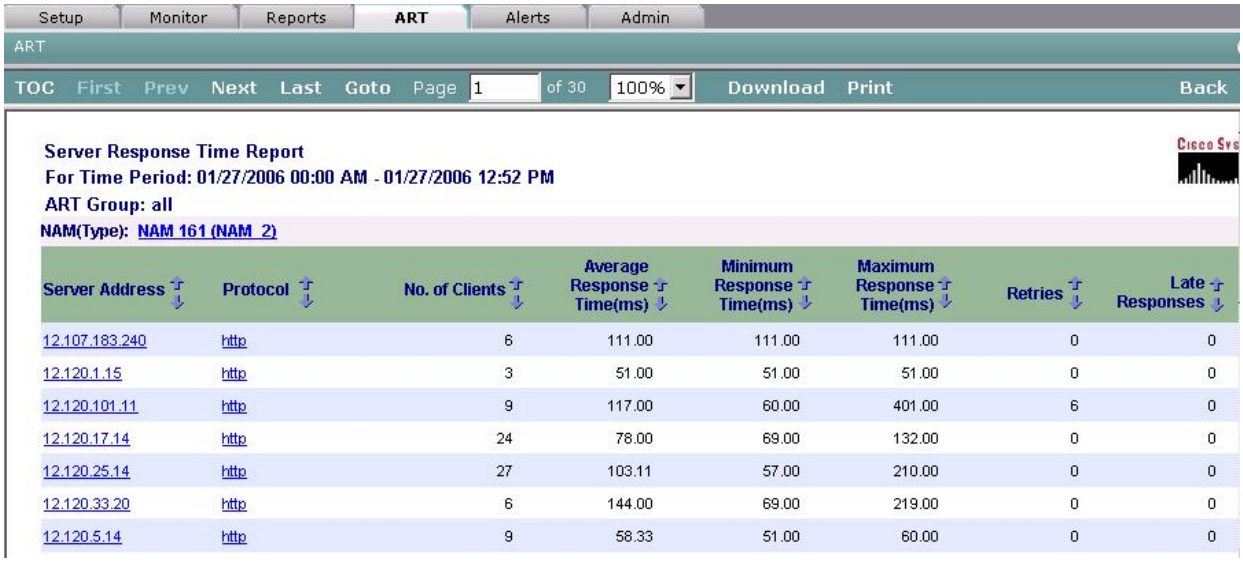
SRT Report Generation Process

To generate a report, specify the:

- Reporting period – the number of previous days (defaulted to today), weeks, months, or years, or a specific date range that defaults to the previous 30 minutes
- Server IP – optional
- ART Group – the system provides a list for selection based on the selected reporting period and optional server IP
- Protocol – defaults all protocols available, but provides a list for selection based on the selected ART Group, reporting period, and optional server IP
- Report Type – tabular or TopN chart display
- Scheduling – immediately, at a later time, or recurrent

Server Response Time Chart

Report



Server Address	Protocol	No. of Clients	Average Response Time(ms)	Minimum Response Time(ms)	Maximum Response Time(ms)	Retries	Late Responses
12.107.183.240	http	6	111.00	111.00	111.00	0	0
12.120.1.15	http	3	51.00	51.00	51.00	0	0
12.120.101.11	http	9	117.00	60.00	401.00	6	0
12.120.17.14	http	24	78.00	69.00	132.00	0	0
12.120.25.14	http	27	103.11	57.00	210.00	0	0
12.120.33.20	http	6	144.00	69.00	219.00	0	0
12.120.5.14	http	9	58.33	51.00	60.00	0	0

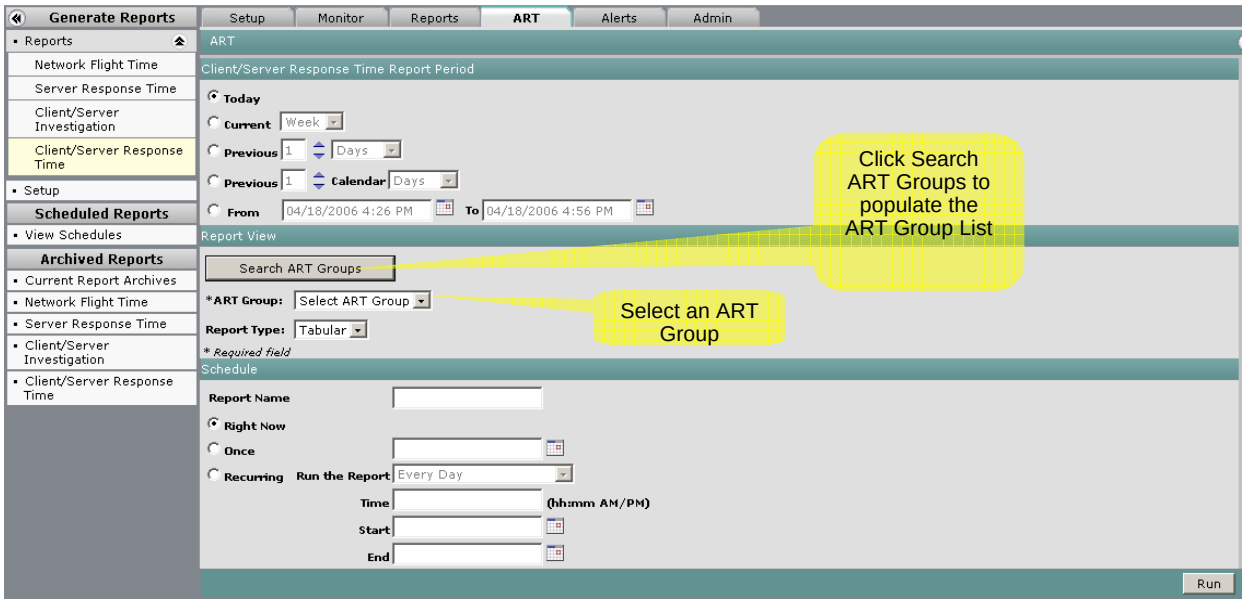
The Server Response Time report (Figure 5–24) displays the server response time for each server assigned to an ART Group, including:

- NAM name
- Server IP address with a drill–down link to the Host Details report
- Protocol with a drill–down link to the Application Details report
- Number of clients
- Average response time
- Minimum response time
- Maximum response time
- Number of retries
- Number of late responses

The Server Address hyperlinks open the Host Details report for each IP address, and the Protocol hyperlinks open the Application Details report for each protocol.

Client Server Response Time Chart

Parameters



The Client/Server Response Time (CSRT) report displays the average round–trip delay times for all the Client/Server pairs that exist for the data sources in a selected ART Group.

CSRT Report Generation Process

To generate a CSRT report, enter the following parameters:

- Reporting period – the number of previous days (defaulted to today), weeks, months, or years, or a specific date range that defaults to the previous 30 minutes.
- ART Group – provides a list of available groups for selection based on the selected reporting period.
- Report Type – either tabular (default) or TopN.
- Scheduling – immediately, at a later time, or recurrent.

Before selecting the ART Group, you'll need to click the Search ART Groups button to populate the drop–down list. Because ART Groups are not always long–lived, the system searches for groups that contain data during the time period you specify. If you receive a message that no ART Groups were found, you can change the report period and search again.

Client Server Response Time Chart

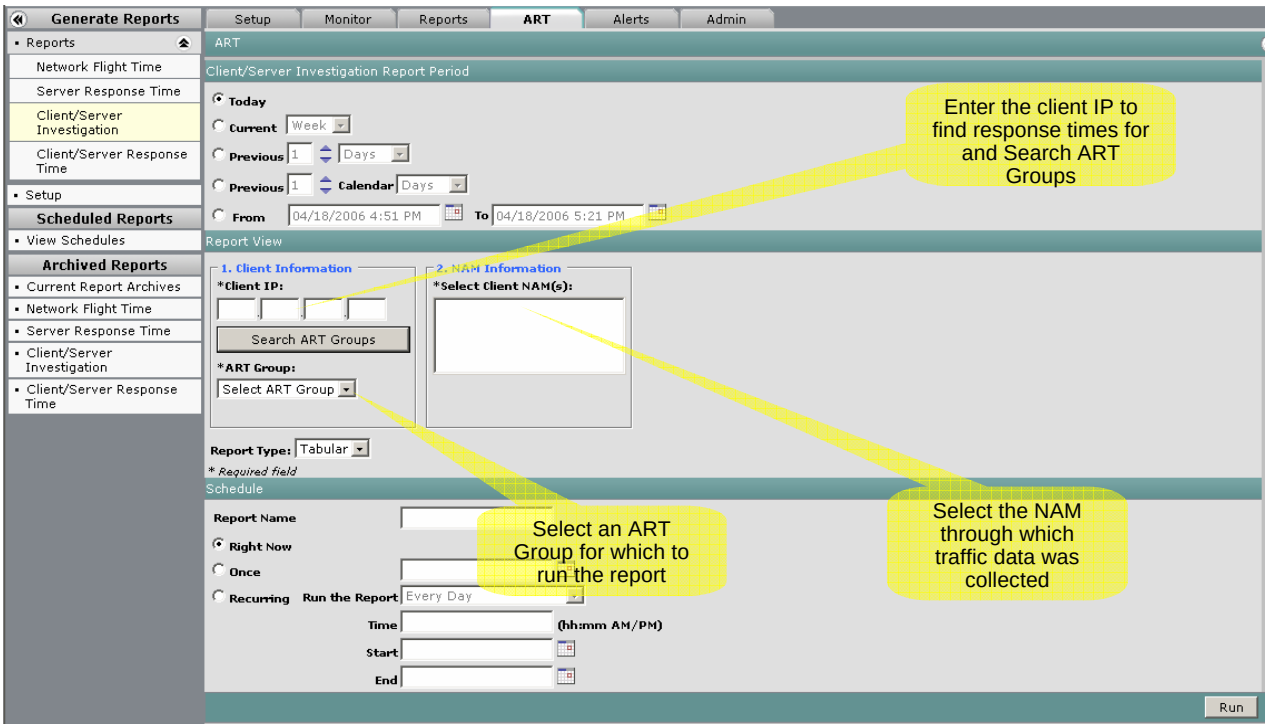
Report

Server Address	Client	Protocol	Average Response Time(ms)	Minimum Response Time(ms)	Maximum Response Time(ms)	Retries	Late Responses
207.46.2.151	172.16.11.42	msn-messenger	2.44 K	110.00	60.18 K	3	3
207.68.178.16	172.16.190.4	http	2.33 K	117.00	24.03 K	54	3
207.46.2.42	172.16.11.42	msn-messenger	1.65 K	111.00	22.94 K	0	3
207.46.2.94	172.16.11.57	msn-messenger	1.60 K	103.00	48.23 K	0	9
207.46.2.104	172.16.190.233	msn-messenger	1.49 K	98.00	85.32 K	3	12
207.68.178.16	172.16.180.71	http	1.22 K	1.22 K	1.22 K	0	0
207.46.0.147	172.16.11.67	msn-messenger	1.12 K	111.00	2.45 K	3	0
64.12.24.153	172.16.17.65	aim	1.04 K	33.00	60.43 K	0	12
4.79.181.12	172.16.8.29	smtp	1.03 K	72.00	4.80 K	3	6
207.46.2.68	172.16.11.42	msn-messenger	933.44	111.00	50.25 K	0	3
172.16.1.66	172.16.11.88	epmap	908.09	0.00	29.97 K	0	3
172.16.9.49	172.16.11.38	smb	782.98	0.00	6.04 K	0	1.63 K

The CSRT report displays response times, in milliseconds, between specific servers and clients, and contains drill–down links to the Host and Applications Details reports.

Client Server Investigation Chart

Parameters



The Client–Server Investigation Report (CSIR) shows the response times for each Client–Server pair of the data source in a selected ART Group and client IP address.

Note: You must be familiar enough with your network setup to be able to determine which NAMs reside closest to servers and clients.

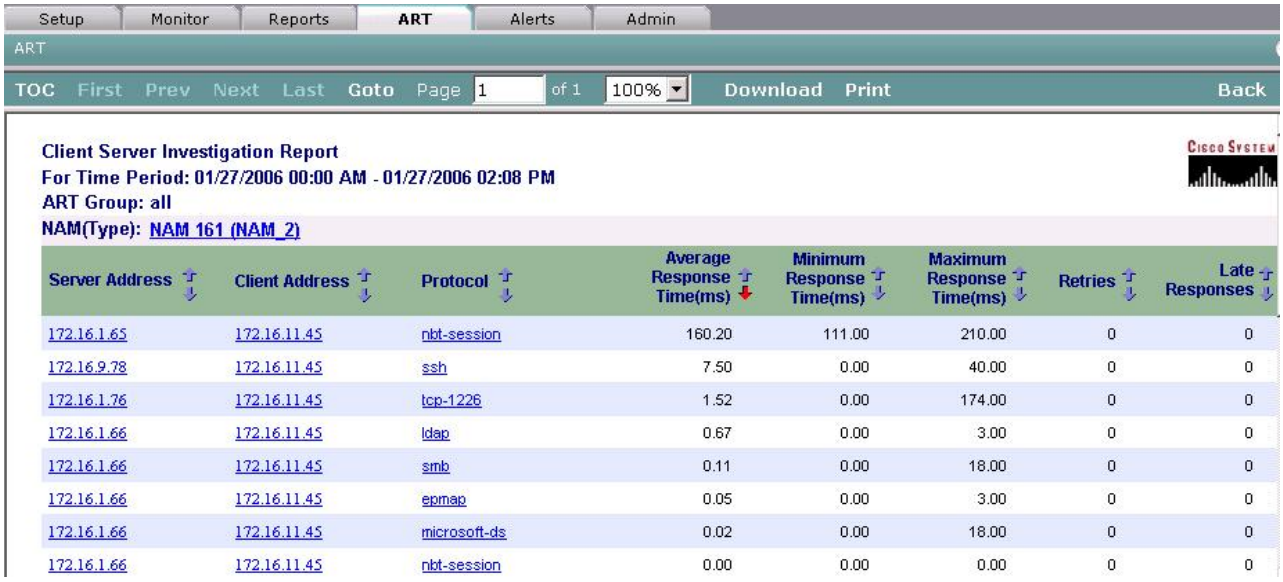
CSIR Report Generation Process

To generate a CSIR report, enter the following parameters:

- Reporting period – the number of previous days (defaulted to today), weeks, months, or years, or a specific date range that defaults to the previous 30 minutes.
- Client IP – a required field with no set default value.
- ART Group – provides a list of available groups for selection based on the entered client IP and selected reporting period.
- Client–side NAMs – provides a list of NAMs based on the selected client IP, ART group, and reporting period.
- Scheduling – immediately, at a later time, or recurrent.

Client Server Response Time Chart

Report

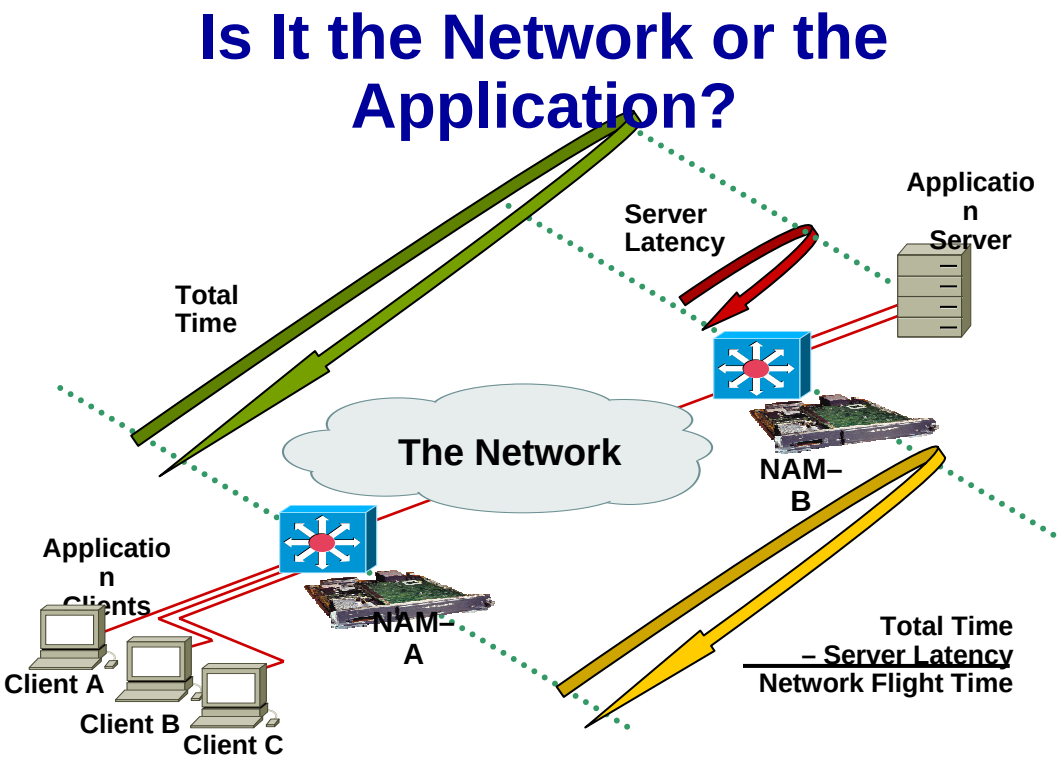


Server Address	Client Address	Protocol	Average Response Time(ms)	Minimum Response Time(ms)	Maximum Response Time(ms)	Retries	Late Responses
172.16.1.65	172.16.11.45	nbt-session	160.20	111.00	210.00	0	0
172.16.9.78	172.16.11.45	ssh	7.50	0.00	40.00	0	0
172.16.1.76	172.16.11.45	tcp-1226	1.52	0.00	174.00	0	0
172.16.1.66	172.16.11.45	ldap	0.67	0.00	3.00	0	0
172.16.1.66	172.16.11.45	smb	0.11	0.00	18.00	0	0
172.16.1.66	172.16.11.45	epmap	0.05	0.00	3.00	0	0
172.16.1.66	172.16.11.45	microsoft-ds	0.02	0.00	18.00	0	0
172.16.1.66	172.16.11.45	nbt-session	0.00	0.00	0.00	0	0

The CSIR report displays the following information:

- The name of the ART Group whose data sources were used to run the report
- The name of the NAM for which the client and server protocol information is displayed
- The host address of the server with drill–down to the Host Details report
- The host address of the client with drill–down to the Host Details report
- The protocol running between the displayed servers and clients, with drill–down to the Application Details report
- The average response time, in milliseconds, between the client and server for the displayed protocol
- The minimum response time, in milliseconds, between the client and server for the displayed protocol
- The maximum response time, in milliseconds, between the client and server for the displayed protocol
- The number of retried responses between the displayed client and server for the specific protocol
- The number of late responses between the displayed client and server for the specific protocol

Network Flight Time Report



The Network Flight Time (NFT) report enables you to discover whether the network or the server is causing delayed response times. Network Flight Time is calculated as the difference of the response times on the NAM closer to the client versus the NAM closer to the server.

The response time collected by the NAM at the client location represents the total average round trip delay time of the request and response.

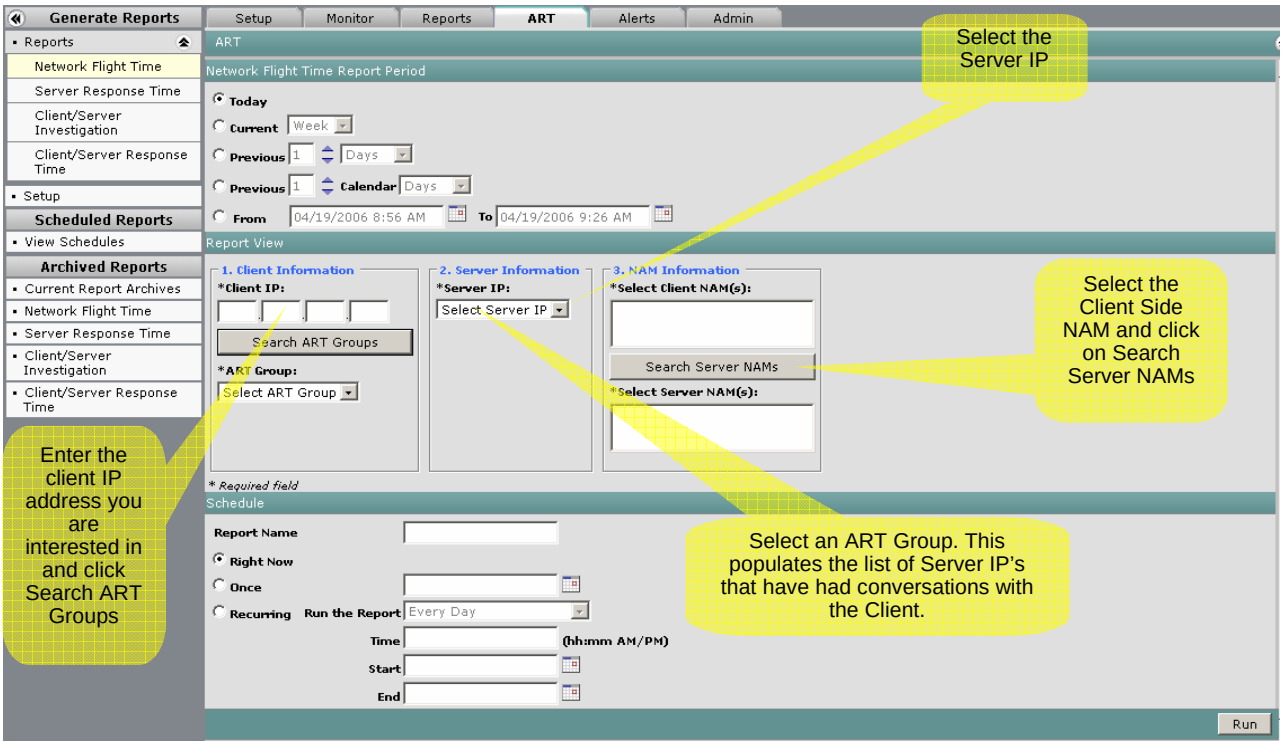
The response time collected by the NAM at the server location represents the average server latency time. Texas can therefore calculate the average network flight time for the request between the client and the server:

Network Flight Time = Total Round Trip Time – Server Latency Time

Note: You must be familiar enough with your network setup to be able to determine which NAMs reside closest to servers and clients.

Network Flight Time Report

Parameters



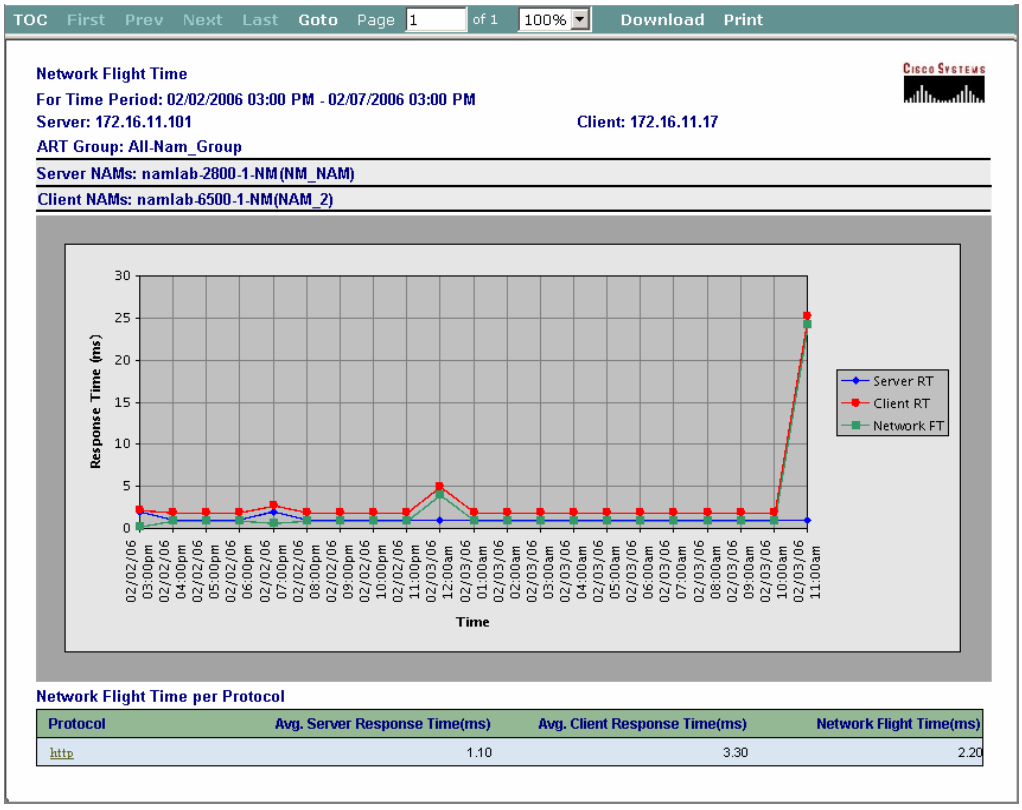
NFT Report Generation Process

To generate an NFT report, enter the following parameters:

- Reporting period – the number of previous days (defaulted to today), weeks, months, or years, or a specific date range that defaults to the previous 30 minutes
- Client IP – a required field with no set default value
- ART Group – provides a list of available groups for selection upon search
- Server IP – provides a list of available NAMs for selection upon search
- Client–side NAMs – provides a list of NAMS based on the selected client IP, ART group, server IP, and reporting period upon search
- Server–side NAMs – provides a list of NAMs for selection excluding those selected as client–side NAMs upon search
- Scheduling – provides the option to run a report immediately, at a later time, or recurrently.

Network Flight Time Report

Report

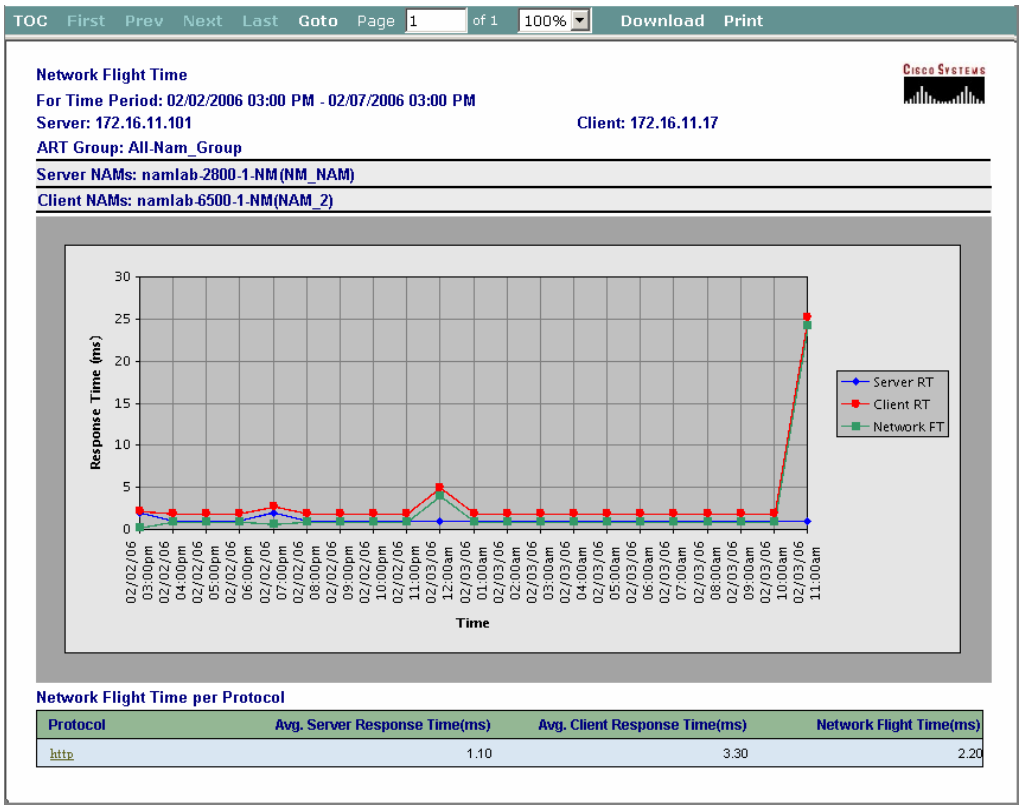


The Network Flight Time report contains the following information:

- Server Response Time – an average based on the ART information provided by the selected server–side NAMs.
- Client Response Time – an average based on the ART information provided by the selected client–side NAMs.
- Network Flight Time – the difference between the client and server response times.
- NFT per Protocol table – shows average values for Server Response Time (SRT), Client Response Time (CRT), and NFT, and contains hyperlinks to the Network Flight Time per Protocol report. You can click on a protocol link to view a protocol–specific NFT report, where the values displayed are specific to the protocol rather than the average over all protocols.

Network Flight Time Report

Report



The Network Flight Time per Protocol report displays an NFT graphic specific to individual protocols for a Client/Server NAM pair, rather than the average NFT for all protocols. This report is available only through the hyperlinks in the Network Flight Time per Protocol summary table at the bottom of the Network Flight Time report. This figure appears similar to the NFT Report on the previous page because that report displays only a single protocol for http.

- The NFT per Protocol report shows the following information:
- The host address of the server
- The host address of the client
- The name of the ART Group selected to run the original NFT report
- The name of the protocol selected from the NFT report protocol summary table
- The NAM(s) closest to the server whose data source(s) are included in the selected ART Group
- The NAM(s) closest to the client whose data source(s) are included in the selected ART Group[
- The response time in milliseconds versus the collection time point for the selected protocol, including:
    - Client Response Time
    - Server Response Time
    - Network Flight Time

Alerts

Alerts consist of three general types:

- NAM alarms – violations of criteria set in an external interface and sent through SNMP.
- Threshold violations – violations of criteria set in Cisco PVM.
- System events – notifications **of licensing errors, timeouts, and system health information.**

Dynamic Threshold Alert Calculation Process

For every data aggregation period, the system performs the following functions for each statistic:

Aggregates all the data collected for a specific metric (measurement) during the specified aggregation period.

Compares the results with the Dynamic Threshold value calculated based on the deviation from the baseline that corresponds to the severity level assigned to the specific Threshold.

Raises an alert if the result is greater than the percentage deviation assigned to the Threshold.

System Health

System–generated alerts include system health events. Cisco PVM monitors the following metrics:

- CPU utilization of each CPU on the system
- RAM utilization
- Disk utilization for each of the locally and remotely mounted file systems and
- Tablespace utilization for all tablespaces in the Cisco PVM database.

The NAM can generate alarms for NAM MIB Thresholds and Switch (RMON) Thresholds. Threshold–generated alarms are for Thresholds set in PVM. Threshold alerts can also generate SNMP traps. You can enable the SNMP trap and enter the community string under **Setup > Thresholds**.

NAM Alarms

NAM–generated alerts result from a violation of criteria configured for the device in either the NAM Traffic Analyzer or a third–party SNMP application. The violations are read from the RMON MIB, and include violations for:

- Rising Threshold Crossed
- Falling Threshold Crossed

All NAM alerts are listed as minor in the Cisco PVM alert viewer.

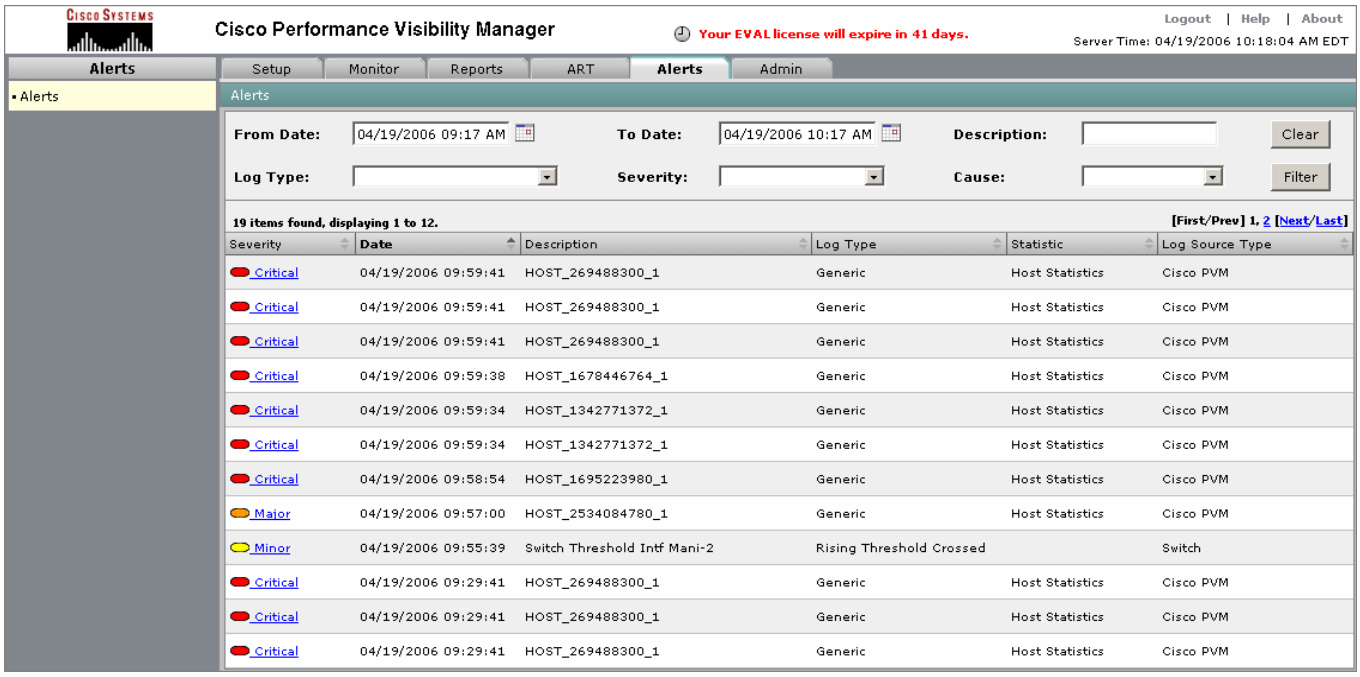
Threshold Violations

Threshold–generated alerts result from violations of user–defined criteria set in Cisco PVM. These alerts appear when a Threshold is violated for an assigned traffic metric with data aggregated for any data source in a specified Data Source Group. Administrators assign specific metrics, Data Source Groups, and alert severity levels using **Setup > Thresholds**. Administrators can define two types of Thresholds in Cisco PVM:

Dynamic Thresholds – the Cisco PVM server performs automatic baselining for each statistic–specific attribute and metric combination based on previous data collection. User–defined percentage deviations from the baseline are translated into alerts, increasing in severity with the degree of deviation.

Fixed Thresholds – the system generates an alert once a user–defined minimum value for a specific metric has been exceeded.

Alerts Page



Alert Severity Color Codes

Cisco PVM displays a color–coded icon next to each alert in the list indicating severity:

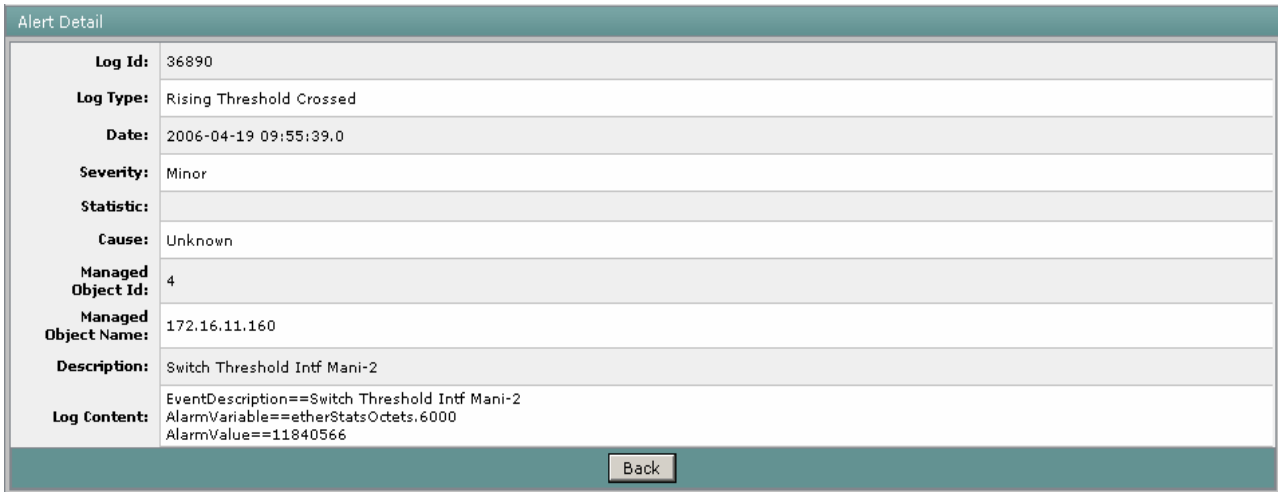
- Red – Critical
- Orange – Major
- Yellow – Minor
- Cyan – Warning
- Green – Cleared
- Blue – Indeterminate
- Gray – Information

Note: A Cleared alert has either had its Threshold adjusted, or the current traffic level no longer violates the Threshold level of the previous alert. A given alert might go through all the severity levels unless it is cleared quickly or the severity level set in Thresholds is adjusted.

Displaying Alerts

Cisco PVM displays a paginated, continuous list of performance alerts in descending order by date, and allows you to filter alerts by time period and other criteria. The display time period defaults to the last hour. The maximum number of alerts that the GUI will display is 1,000. An alert will remain in the GUI list until it falls to greater than the last 1,000 alerts logged in the system.

Alert Detail



The Alert Detail window contains the following information:

- Log Id – the sequential number of the alert as it appears in the database
- Log Type – the type of alert generated (such as Generic, Rising Threshold Crossed, System Health)
- Date – the date and time the alert was generated
- Severity – the severity level of the alert
- Statistic – the type of traffic (statistic) upon which the violation is based
- Cause – Either Generic (known to the system) or Unknown
- Managed Object Id – the classification of the managed object as it appears in the database
- Managed Object Name – the name of the managed object as it appears in the database
- Description – the device, metric, Threshold, or system check that generated the alert
- Log Content – detailed information about the actual alert as contained in the database, such as:
    - The baseline value at the time of the alert
    - The value that was actually violated
    - The DSG assigned to the Threshold (for Threshold violations only)
    - The data source that generated the traffic
    - The traffic metric monitored, such as bytes, packets, or errors
    - A device–specific identifier

Baselining

In Cisco PVM, baselining is automatically performed for metrics that have thresholds set for them. Baselines are configurable as daily, weekly or monthly moving averages. Dynamic threshold violations are based on the baseline and a percentage of the standard deviation. These percentages are configurable. The default severity levels for dynamic threshold crossings are:

- 40% - Warning
- 60% - Minor
- 80% - Major
- 100% - Critical

You can configure and modify performance threshold values for Data Source Groups (DSGs), Application Response Time (ART) Groups, statistics, and metrics that generate alerts once those values have been violated. Alerts appear as individual events under the Alerts tab in the Cisco PVM dashboard, but Thresholds are customized under **Setup > Thresholds**.

Understanding Threshold Settings

Threshold values are relative to a baseline and standard deviation. The Cisco PVM server automatically determines the baseline for each traffic type and metric (or measurement) combination based on previous data collection statistics. Deviations from the baseline are translated into alerts, increasing in severity with the degree of deviation from the baseline. The Threshold value is actually a percentage of standard deviation above the sum of baseline and standard deviation. When you define a Threshold, you are specifying the minimum severity at which the Alert Viewer will notify you of the violation.

Standard Deviations and Baselines

Using standard deviations (SDs) in generating threshold violations helps to avoid alerts for short spells of traffic spikes. The baseline as defined in Cisco PVM is a rolling average of hourly data over a group of data sources specific to the traffic type and its associated metric. The baseline calculation period is the moving average of data collected during the rolling interval. The hourly data is the average metric value for all the collections in that hour, further averaged for all the data sources in a Data Source or ART Group. The final Threshold value is therefore a percentage of standard deviation:

- above the sum of the baseline and SD or
- below the difference between the baseline and the SD.

For every data aggregation period, Cisco PVM calculates the baseline and the standard deviation for each Threshold you've defined in the system. The data for computing the baseline and standard deviation is the average of the measured value (metric) for all the collections in that period of time, further averaged for all the data sources in the Data Source Group.

Because Dynamic Thresholds adapt to the typical traffic pattern, these Threshold types are set as a percent of standard deviation, where 100% equals the calculated standard deviation. Dynamic Thresholds also involve the severity level definition, which will interpret different Threshold percentages as different severity levels. For example, 150% of the standard deviation may represent the Major severity level, whereas 200% of the standard deviation may represent the Critical level.

Baseline Period Settings

The duration of the Baseline Period (the rolling interval used to calculate the moving average) is set in the Preferences window.

Currently the baseline is calculated as a daily moving average for each configured Threshold. A Threshold can be configured on any of the metrics available in the reports. Threshold calculations occur after every collection cycle.

Fixed Thresholds

Cisco PVM allows users to define Threshold values in two ways: *Fixed* and *Dynamic*. Fixed Threshold values remain static over time based on a set value for a selected metric (such as Packets), allowing you full control of alert notifications for the severity levels they assign to individual Thresholds. Cisco PVM uses fixed metric values for each severity level and will raise alerts when these values have been exceeded. The system triggers an alert if the fixed value you have assigned has been crossed. Fixed Thresholds therefore do not use baselines to trigger alerts.

Information entered in the Fixed Threshold Value fields depends on the metric you are monitoring. For Fixed Thresholds, these values represent the fixed values for each severity level, starting with the level indicated in the Severity field. For example, if you select Major, then the system will only show the fixed percentages for Major and Critical, and will raise alerts when only these values have been exceeded. Fixed Values can have any value greater than zero, including fractional values up to 24 characters long. You will enter these values in the Add a New Threshold screen for every Fixed Threshold you create.

Dynamic Thresholds

With Dynamic Thresholds, you assign Severity Percentage values that represent the percentage deviation from the baseline for each severity level, starting with the level indicated in the Severity field. Dynamic Thresholds adapt automatically to typical traffic patterns, then generate alerts at default percentages set under Setup > Preferences or using percentages you assign when you create or edit a Dynamic Threshold.

When using Dynamic Thresholds, the Cisco PVM server will perform automatic baselining for each statistic–specific attribute and metric combination based on previous data collection. Deviations from the baseline will be translated into alerts, increasing in severity with the degree of deviation. Over time, the Dynamic Threshold values will change based on the accumulated historical data and will automatically adjust the alerts to notify you of anomalies.

Information entered in the Threshold Severity Percentage fields depends on the type of Threshold you are creating. For Dynamic Thresholds, these values represent the percentage deviations for each severity level, starting with the level indicated in the Severity field. Dynamic Threshold severity percentage values must be between 0 – 100, including fractional values up to 24 characters long.

The Threshold Setup GUI displays a list of all the Thresholds configured in the system by name, associated Data Source Group, statistic type, associate metric, severity, and status (enabled/disabled). The list can be filtered by:

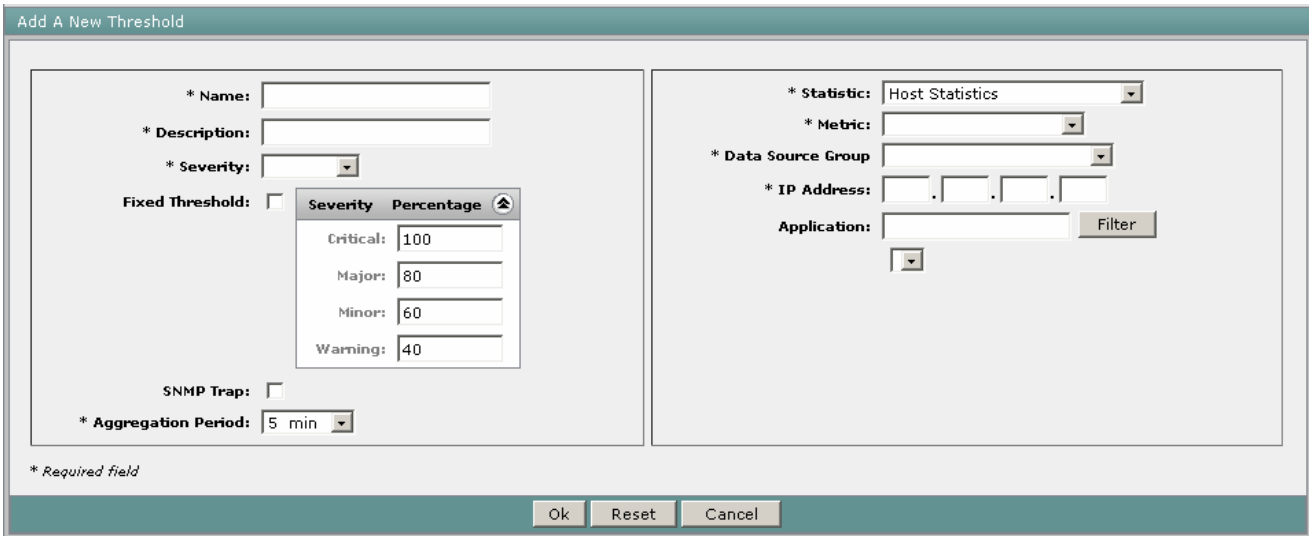
- Name
- ART / Data Source Group
- Statistic
- Severity
- Baseline values appear for Dynamic Thresholds only.

Disabling Thresholds to Suspend Alerts

Administrators can suspend alerts for individual Thresholds defined in Setup. Under the Setup GUI, Thresholds can be disabled if you no longer need or want to view traffic–related violations in the Alert Viewer. The Threshold definitions remain in the system, and they can be re–enabled if desired. Disabled Thresholds do not generate alerts.

Add a Dynamic Threshold

To add a dynamic threshold, click on the Add button and select the appropriate statistic, metric and other parameters. Do not check the 'Fixed Threshold" checkbox.



Statistics and Metrics

Cisco PVM is able to monitor a variety of performance statistics, or traffic types, and their associated *metrics*, or units of measure. After you've selected the statistic type for a Threshold, Cisco PVM automatically populates the Metric drop–down list with the measurements available for that statistic. Depending on the statistic selected, you can configure a Threshold for the following specific statistics:

- Applications
- ART (Application Response Time)
- Data Source Traffic
- MAC
- Host
- Switch/Router and
- VLAN.

The metrics available for creating Thresholds are relevant to the selected traffic type. The Metric list is populated with different units of measure depending on the statistic you select for Threshold monitoring. Additionally, other fields appear on the screen that depend on the statistic selected.

Aggregation Periods and the System–Wide Collection Cycle

When defining a Threshold, you'll set an Aggregation Period that represents the time interval used for aggregating the statistic measurements. This value is constrained by the System–wide Collection Cycle in the following ways:

When you create a Threshold, the system automatically lists the appropriate multiples of the Collection Cycle in the Aggregation Period drop–down list.

The Aggregation Period that you set for individual Thresholds must be greater than or equal to the Collection Cycle.

The system will not aggregate Threshold data for time intervals that are less than the system–wide setting for data collection from the NAMs.

Changes to the System–wide Collection Cycle

If the System–wide Collection Cycle (set in Setup > Preferences) is reset to a value higher than the Aggregation Periods for currently defined Thresholds, the system will automatically set the Aggregation Periods equivalent to the Collection Cycle. If you edit a Threshold that was originally defined with a setting lower than the new collection setting, you'll see the error messages:

"Aggregation Period must be greater than Collection Cycle"

"Aggregation Period must be a multiple of Collection Cycle"

In this case, the Edit Threshold window reflects the old Aggregation Period. You can change the Aggregation Period for the Threshold to a value that is greater than or equal to the new Collection Cycle and click OK to clear the error messages.

Low Traffic Situations

If the Aggregation Period has been set too low for the amount of traffic generated by a given statistic (such as VLAN), the system might not be able to calculate a baseline value. In this case, at least one time interval over the last 24 hours has no data. If you set the Aggregation Period to a higher value for that statistic, the system will automatically recalculate the baseline for the last 24 hours. The baseline value appears in the list of Thresholds under Setup > Thresholds and in the Edit Thresholds window for each Dynamic Threshold you have defined.

Add a Fixed Threshold

Fixed Thresholds do not use dynamically calculated baselines, but fixed severity percentage values instead. When creating a Fixed Threshold, you'll check the Fixed Threshold box and the Fixed Value box will automatically expand, containing fields for the minimum severity level you specified in the Severity drop–down list and all levels greater than that minimum. For example, if you want to assign a severity level of Major to the alert, the expansion box will show fields for Major and Critical levels only.

The Aggregation Period is the time interval, in minutes, used for aggregating the statistical data. This drop–down list is populated with values calculated dynamically as multiples of the System–Wide Collection Cycle set in Setup > Preferences.

Caution: The Aggregation Period is not applicable to Application Response Time statistics.

Changing baseline and threshold parameters

The Preferences window allows Cisco PVM you to view and edit system–wide configuration parameters. These parameters are used throughout Cisco PVM for data collection, Threshold setup, and Application Response Time (ART) reports. These settings are available in Cisco PVM as part of the Setup GUI to allow easy access to system–wide defaults. Settings such as the System–wide Collection Cycle and Threshold severity levels can be customized through other Setup menu items, such as NAM and Thresholds.

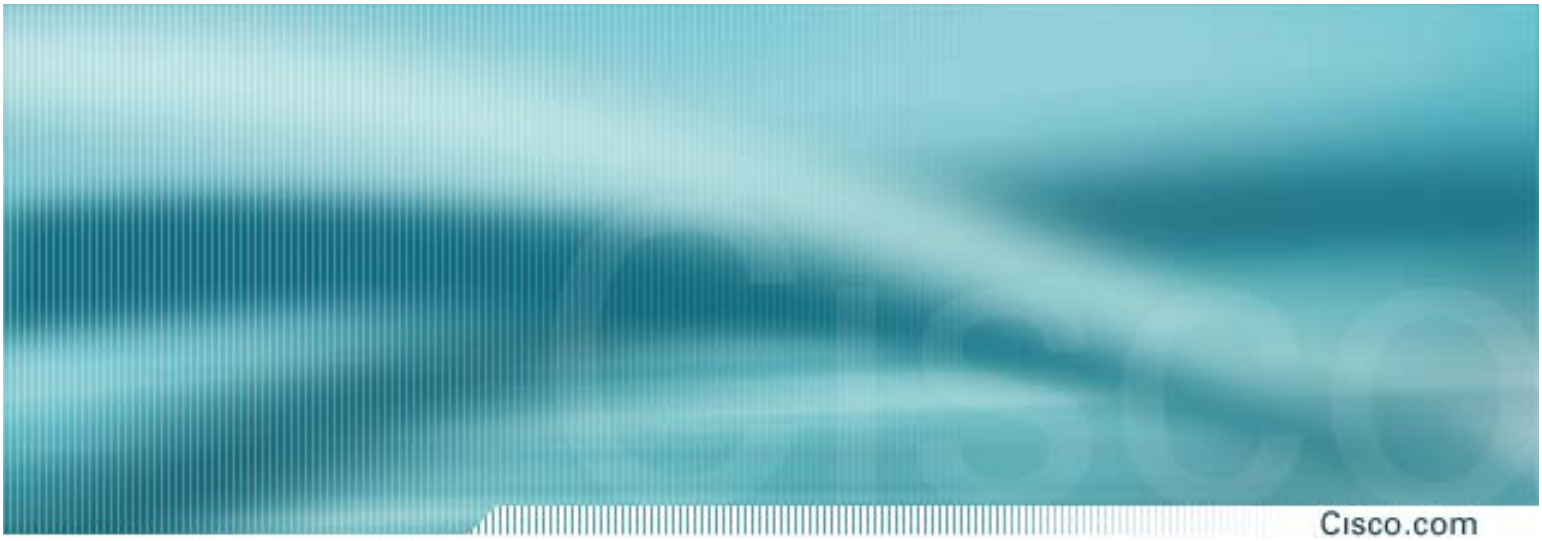
The Preferences option under the Setup tab is used to assign default values that affect the entire system. For example, the System–Wide Parameters section contains settings for the Collection Cycle and the number of graph bars that appear in all TopN report views. The default Threshold Severity Levels used for dynamically calculated baselines are also set here, although they can be customized for individual Dynamic Thresholds.

Baseline and Observation Periods

The Baseline Period setting is the duration, in days, in which the baseline for Thresholds is calculated. Another way to think of the Baseline Period is as the rolling time interval used to calculate the moving average. The default value is 1 day.

The Observation Period is the frequency at which the baseline will be recalibrated; at the end of each Observation Period, the values for the last baseline period are examined, and the baseline value is updated accordingly. The default value is 60 minutes.

The Baseline Period must be greater than the Observation Period, and an even multiple of it. For example, the system will reject an Observation Period of 1500 minutes (25 hours) if the Baseline Period is 1 day.



Chapter 3

Common Scenarios

Cisco Performance Visibility Manager 1.0

Common Scenarios

Cisco.com

- **Part 1: Traffic Profiling**
- **Part 2: Proactive Monitoring**
- **Part 3: Troubleshooting**

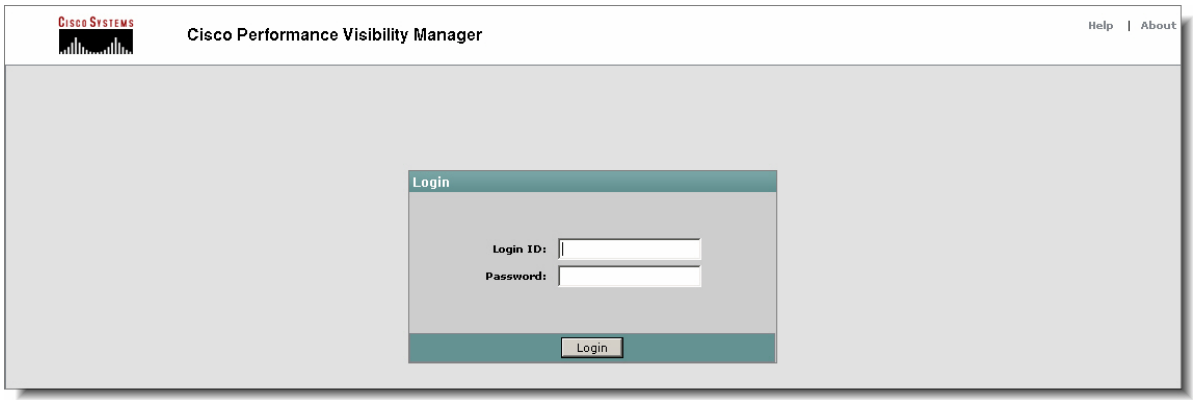
This chapter provides useful usage scenarios for Cisco PVM. It consists of three scenarios that present an overall look at the features available in Cisco PVM and how they can help you in addressing your network monitoring and troubleshooting needs.

Login

Cisco.com

Go to: https://<pvm_server>:8443/

Login as the admin user



Enter the Login ID and Password you've been given by your Cisco PVM System Administrator, or the default login information in the Cisco PVM Installation Guide if this is your first time running the application after installation.

This screen also has two system navigation links:

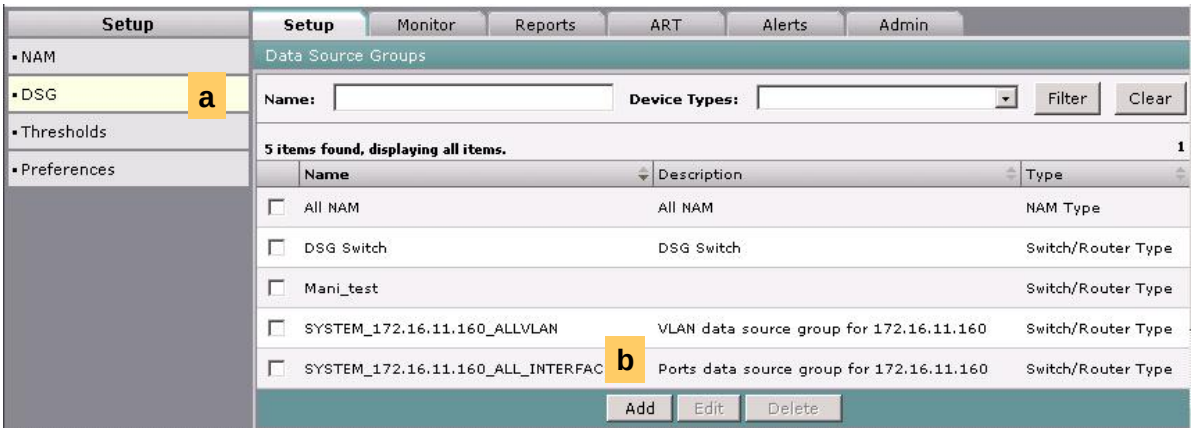
Help opens a new window containing topics matching the Cisco PVM User Guide. All users can view this content, even though all users do not have access to all PVM functions.

About opens a pop–up window that shows the current PVM version and build numbers. This information is important should you require support.

Since Cisco PVM supports only secure communications using SSL, if the installed SSL certificate is not from a trusted authority, a security alert dialog may pop up asking you if you want to proceed. Click on Yes to proceed, or install the certificate by clicking on View Certificate and then Install Certificate in the ensuing pop up dialog.

Scenario 1 – Traffic Profiling

Cisco.com



Scenario

Most enterprise networks have many protocols running on their network. Network engineers need to be able to monitor these protocols to not only see which protocols are using the available bandwidth and fine–tune them, but also to monitor unwanted protocols from being used. To do that, follow these steps:

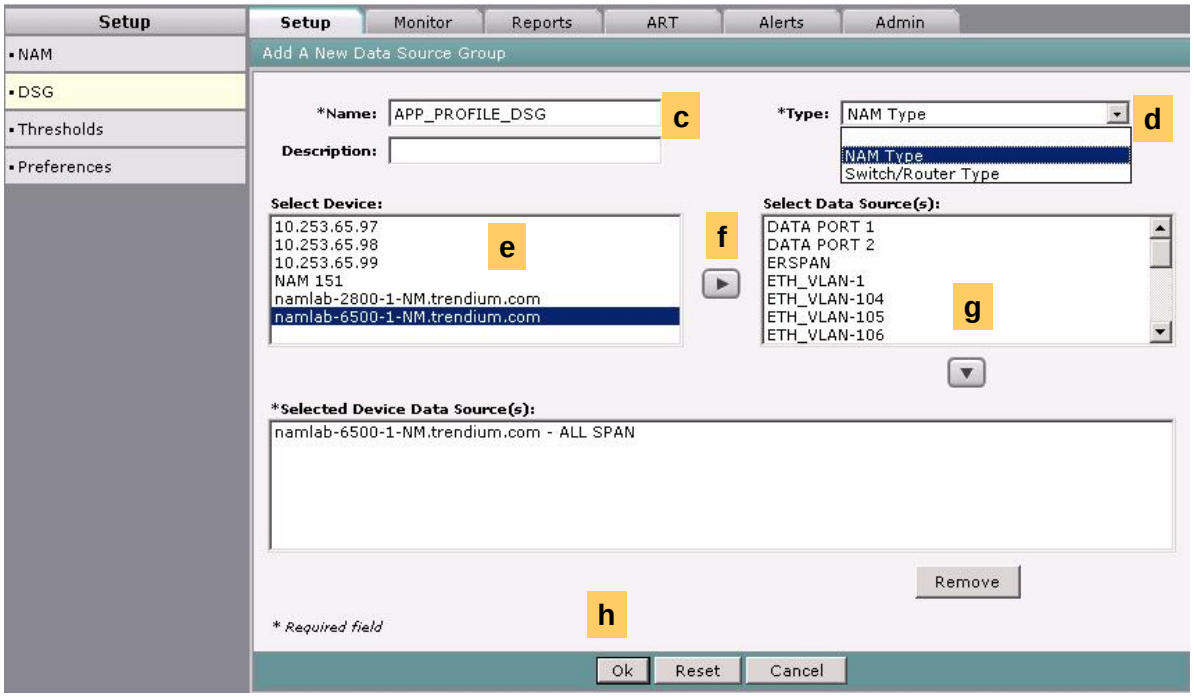
Step 1:

Create a data source Group which contains the data sources on which you want to profile the application traffic.

a. Click on Setup –> DSG.

b. Click on Add.

Scenario 1 – Traffic Profiling



Step 1 (Contd):

c. Enter the Name

d. Select the NAM Type in the Type dropdown

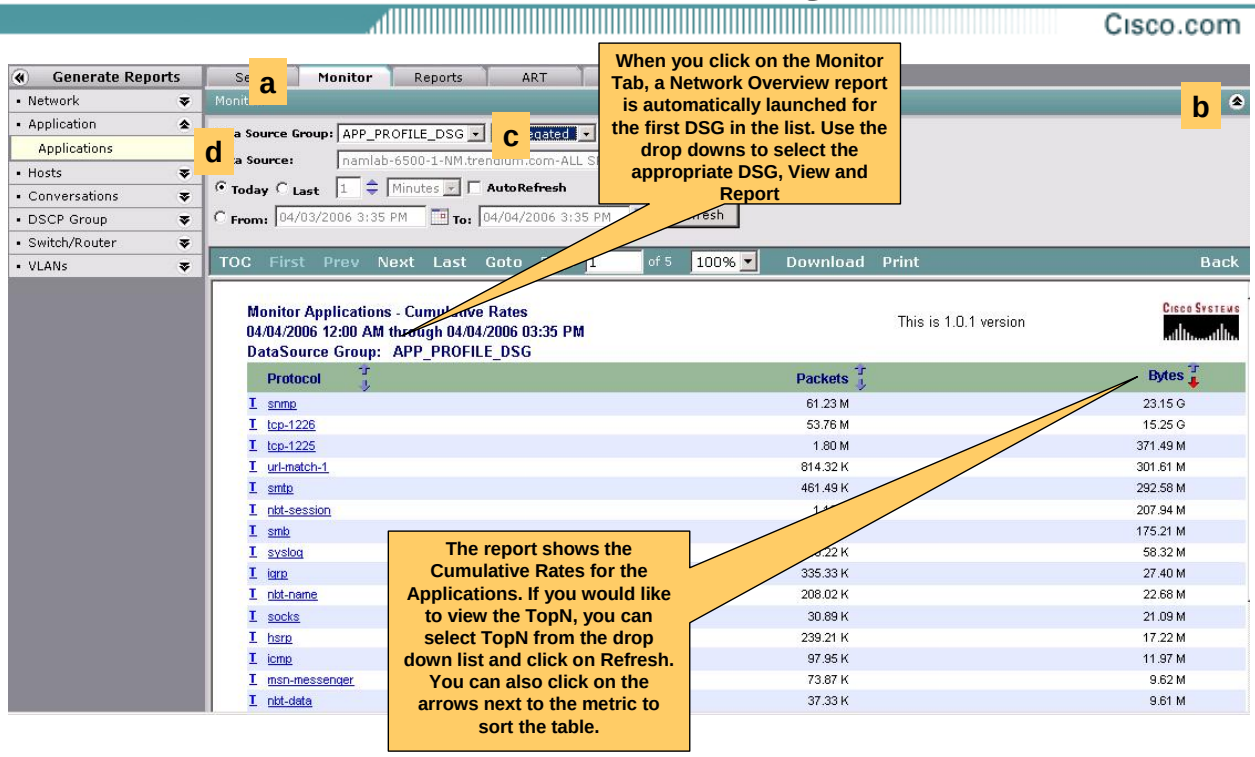
e. Select the device.

f. Click on the right arrow to see the data sources from the device.

g. Select the appropriate data source and click on the down arrow to add the data source to the group.

h. Once you have added all the data sources, click on OK to create the data source group.

Scenario 1 – Traffic Profiling



Step 2:

Go to the Monitor tab and select the Applications Report Suite.

a. Click on the Monitor Tab.

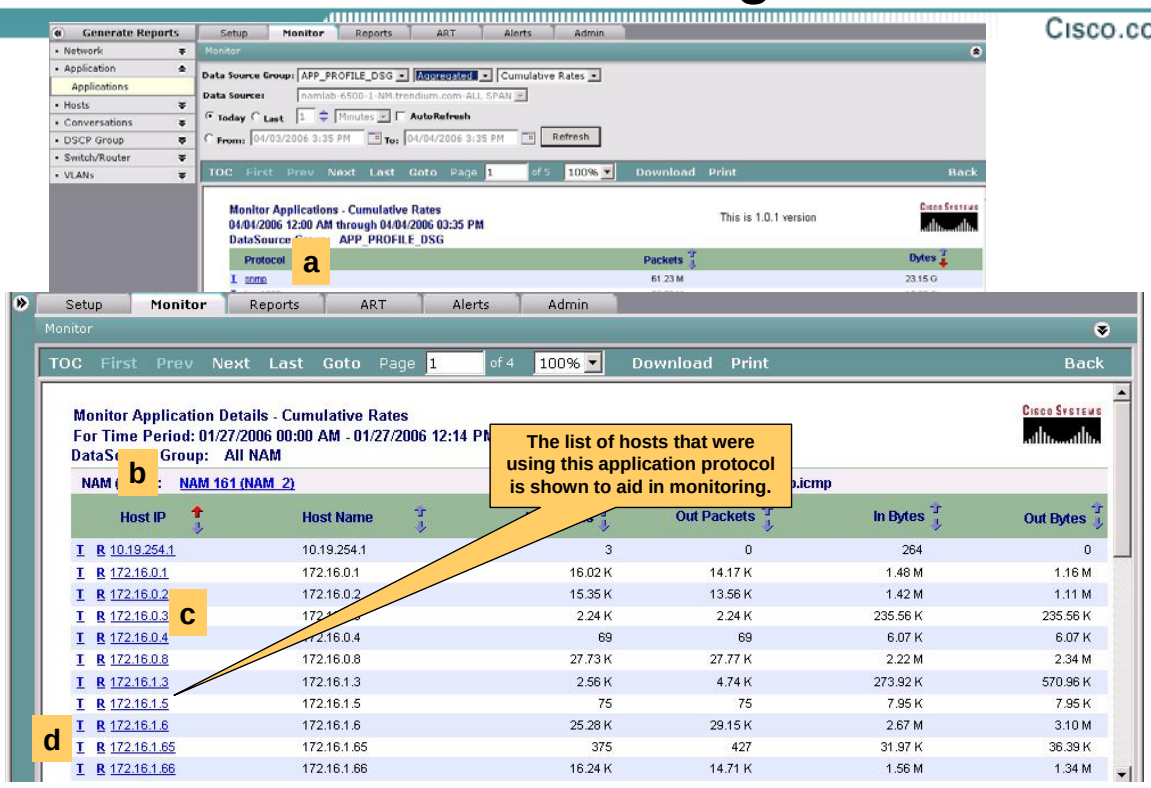
b. Click on the right arrow button at the top left corner to toggle the menu, and the down arrow button at the top right corner to toggle the parameters page.

c. Select the DSG you just created, and the Aggregated view type.

d. From the Menu on the left, click on the Applications menu item and select the Applications Report.

Note: You might find that the report displays a **"No data found"** message. This happens when Cisco PVM does not have any traffic information collected from the NAM whose information you are currently viewing, but has data for the other NAMs in the data source group. Click on Next in the navigation bar to view the information for the other NAMs. If Cisco PVM does not have information for any of the NAMs in the data source group, it displays a pop up error message **"There are no pages to display".** In this event, select a different data source group.

Scenario 1 – Traffic Profiling



Step 3:

If you find a protocol that is using excessive bandwidth, you can find out who is using it.

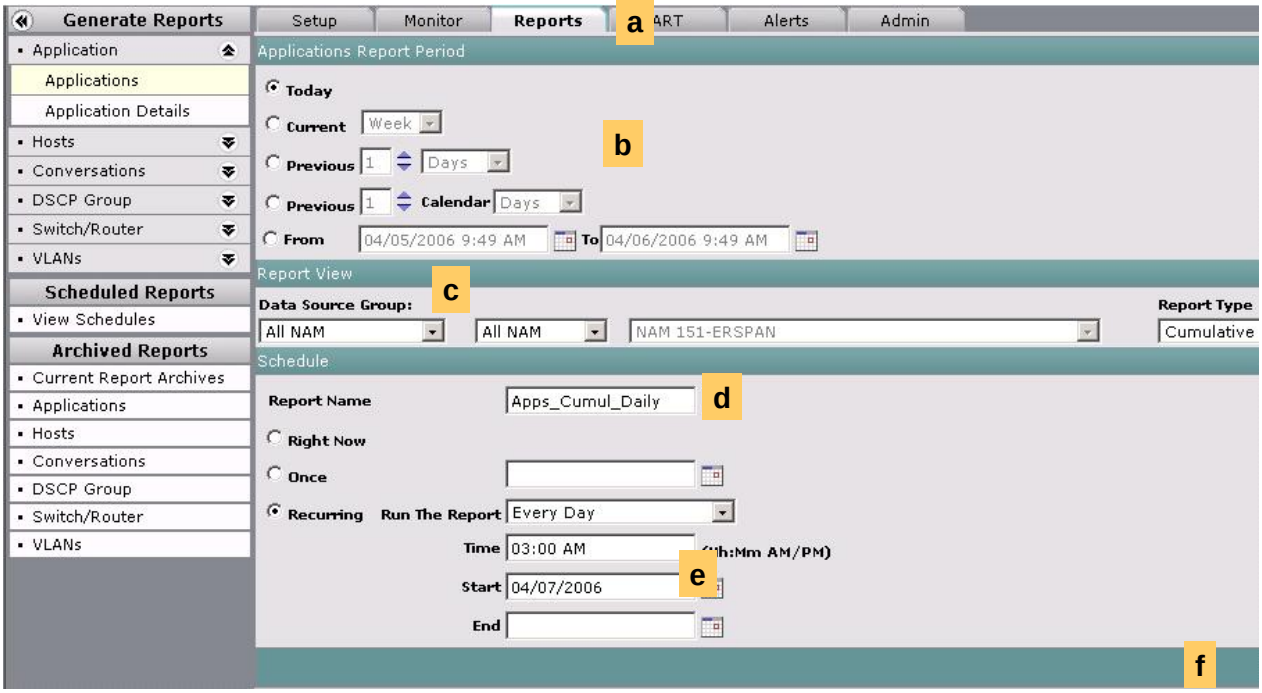
a. Click on the Protocol of interest.

b. PVM will list the hosts that were using the protocol and the amount of traffic they generated.

c. You can analyze the host in detail by clicking on the Host IP.

d. You can also analyze the trends by clicking on the 'T' hyperlink

Scenario 1 – Traffic Profiling



Cisco PVM 1.0 © 2006, Cisco Systems, Inc. All rights reserved. 88

Step 4:

You can also schedule these reports to be run at a given time for later perusal.

a. Click on the Reports Tab. By default the Applications Report page is shown.

b. Select the report period.

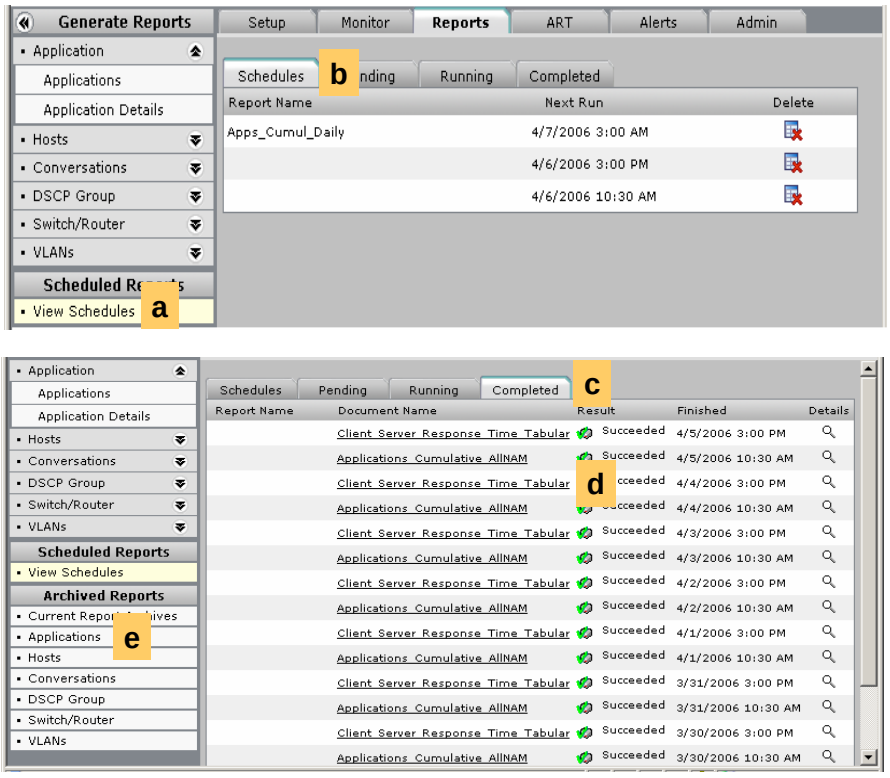
c. Select the data source group and specify the view type.

d. Enter a report name.

e. Schedule the report to run at a given time.

f. Click Run.

Scenario 1 – Traffic Profiling



Step 5:

a. **Scheduled reports are visible from the View Schedules menu item.**

b. **Click on the Schedules tab to see scheduled reports.**

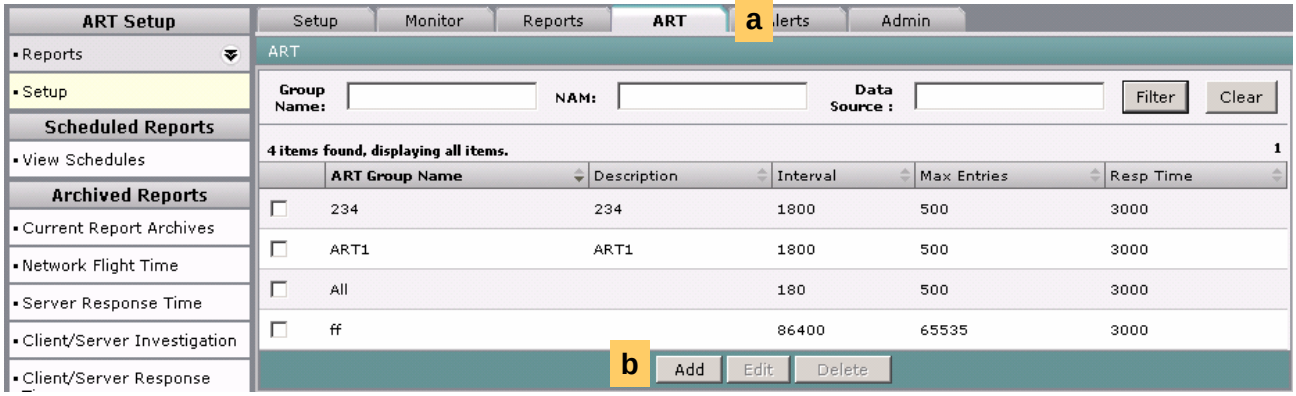
c. **Reports that have already been run are available in the Completed tab.**

d. **Click on the report hyperlink to view it.**

e. **You can also view reports of a particular type by selecting the appropriate report suite in the Archived Reports menu section.**

Scenario 2 – Proactive Monitoring

Cisco.com



Scenario

Network engineers are getting calls to troubleshoot user issues. They would like to proactively monitor the network and troubleshoot issues before users become aware of them. Assume that users are complaining of intermittent slow response times from a particular server. Cisco PVM can be used to monitor response times from the server and alert the network engineer to potential trouble, allowing the engineer to take the appropriate action before the users see any degradation in performance. The following steps allow the user to proactively monitor the network:

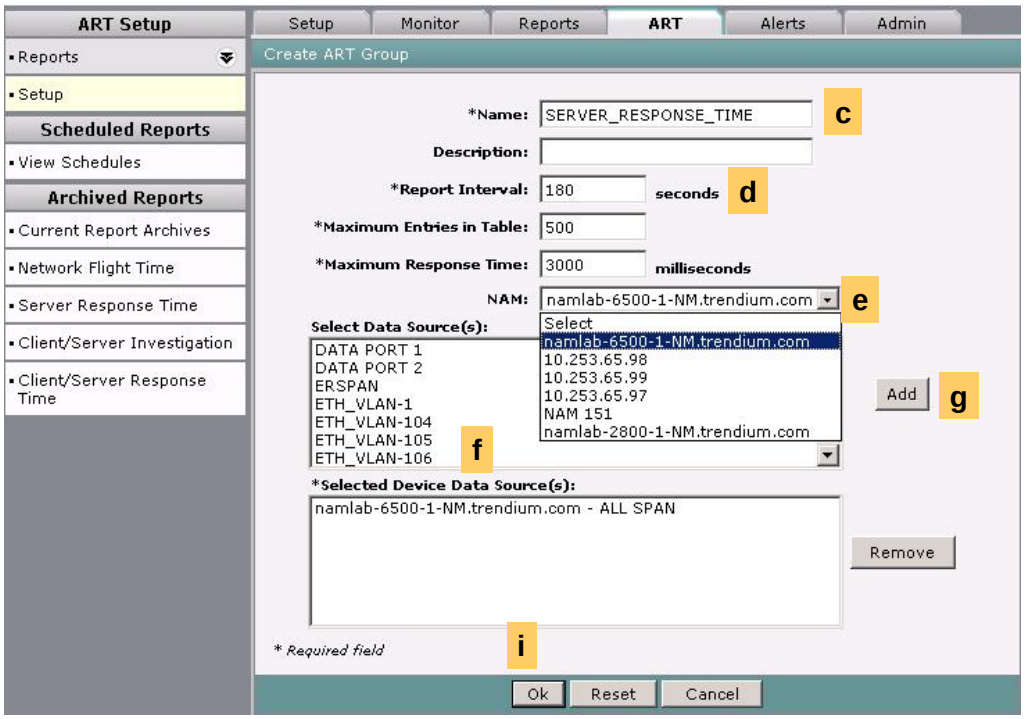
Step 1:

Create an ART Group that carries traffic you are interested in.

a. Click on ART Tab.

b. Click on Add.

Scenario 2 – Proactive Monitoring



Step 1. (Contd.):

c. Enter a Name for the ART Group.

d. Enter the appropriate Report Interval

e. Select the NAM from the drop–down

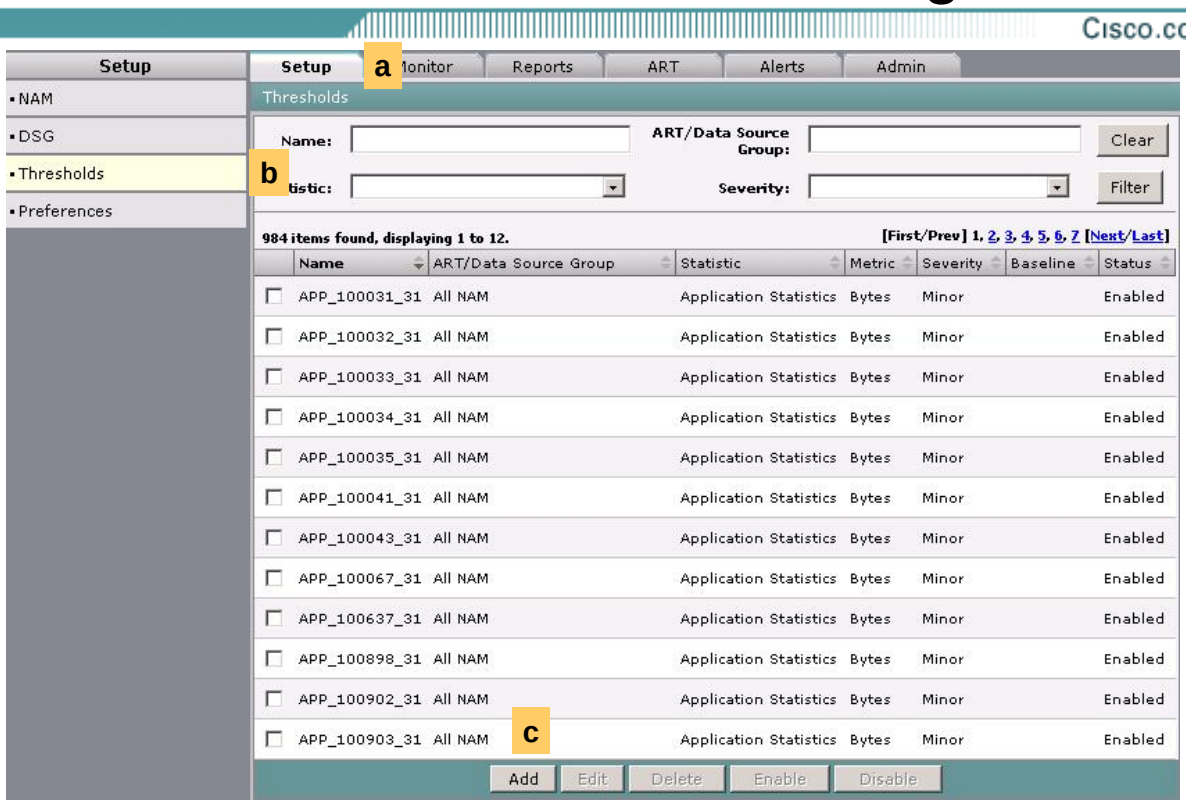
f. Select the appropriate data source from the NAM

g. Click on the Add button.

h. Repeat steps e–g to add all the data sources.

i. Click on OK.

Scenario 2 – Proactive Monitoring



Step 2:

Create a Threshold for the Application Response Time of the server you are interested in.

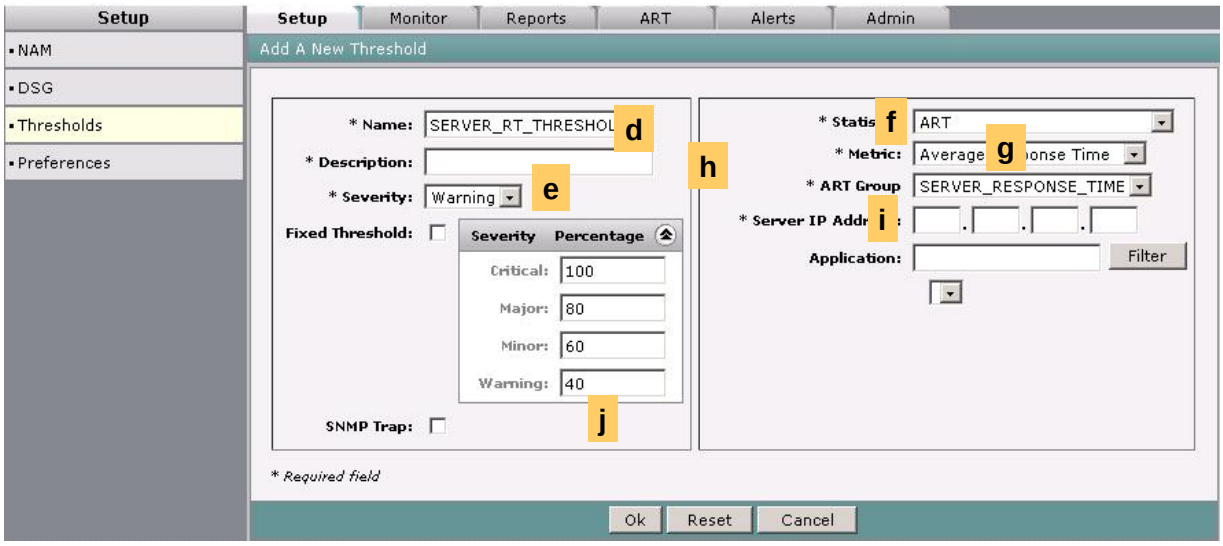
a. Click on the Setup Tab

b. Click on the Thresholds Menu item.

c. Click on Add

Scenario 2 – Proactive Monitoring

Cisco.com



Step 2. (Contd.):

d. Enter the Name for the Threshold.

e. Select the severity of the Alert to be issued.

f. Select ART from the Statistics drop–down.

g. Select the Average Response Time metric.

h. Select the ART Group you just created.

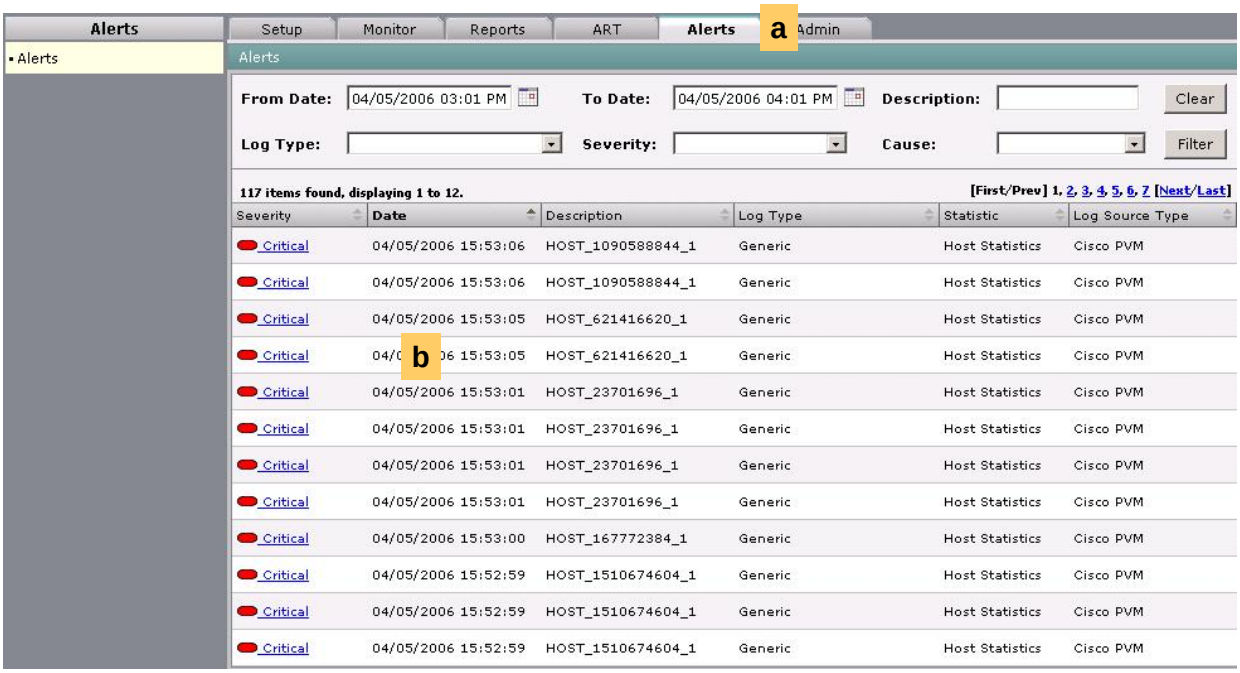
i. Enter the IP Address of the server you want to monitor.

j. Click on OK to create the Threshold.

Note: To find out which servers and clients are talking to each other, you can use the Client Server Response Time Report. Click on the Reports Menu item and select Client Server Response Time. Click on Search ART Groups, select an ART group from the drop down and click on Run.

Scenario 2 – Proactive Monitoring

Cisco.com



Step 3:

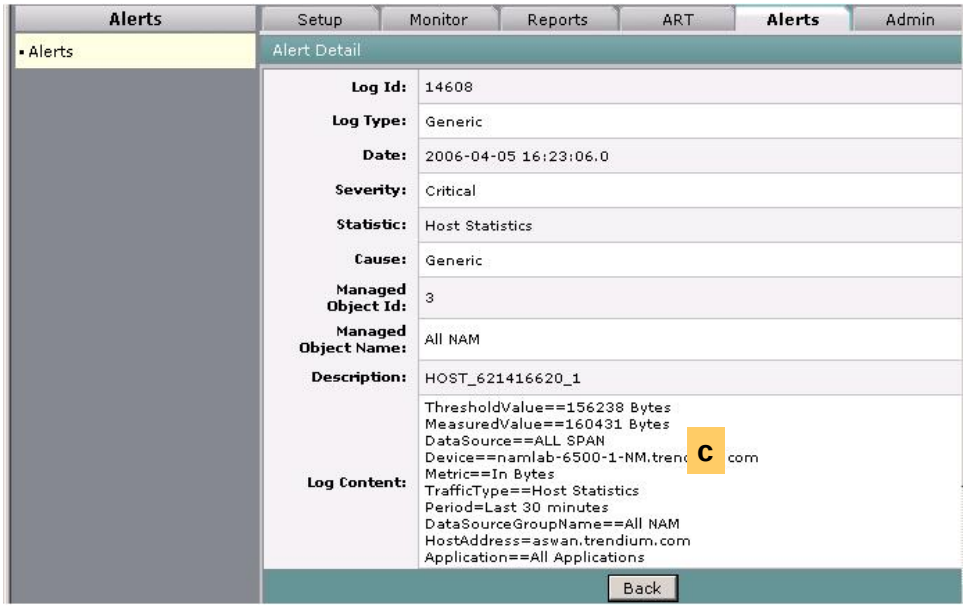
PVM will now start base–lining the Average Response time for that server. If the Thresholds are crossed, it issues an alert.

a. To view alerts, click on Alerts Tab.

b. To view a specific alert click on the severity hyperlink of the appropriate alert.

Scenario 2 – Proactive Monitoring

Cisco.com

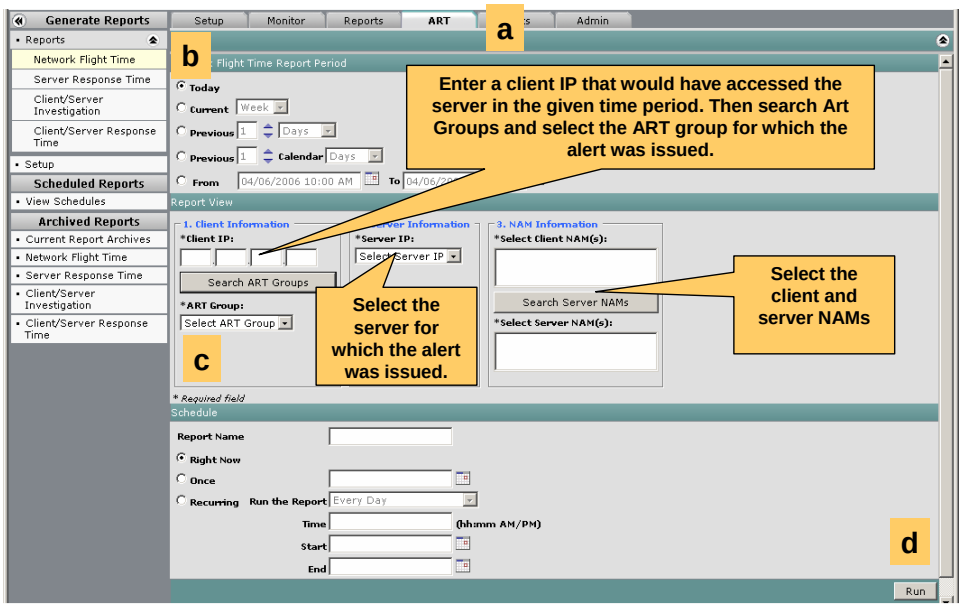


Step 3. (Contd.):

c. PVM displays the details of the Threshold violation.

Scenario 3 - Troubleshooting

Cisco.com



Scenario

You are base–lining your response times from the server farm. An alert is issued that a critical corporate server has a very high response time when compared to the baseline. You want to find out if the apparent slow response time is due to the network or the application. Once you find that the problem is indeed with the network, you want to know where the problem is and correlate the response time problem in context with other traffic in your network.

Step 1:

Run a Network Flight Time Report for the server and a client in the ART group for which the alert was issued.

a. Click on the ART tab.

b. Click on Reports –> Network Flight Time

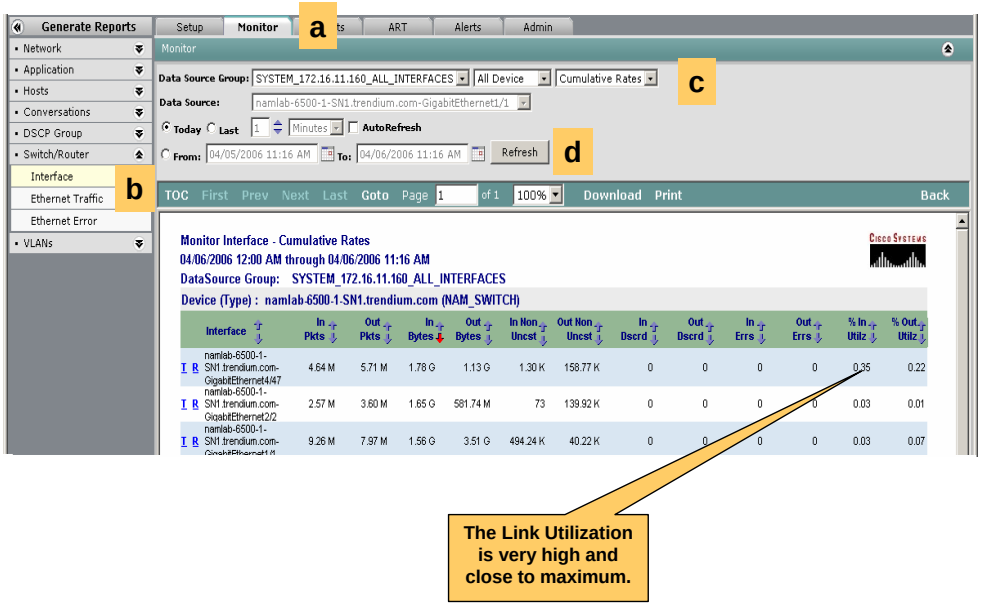
c. Enter the parameters.

d. Click on Run

Note: All ART Reports perform pre-filtering. That is, if Cisco PVM does not have any rerponse time information from an ART group for the selected time period and parameters, you will not see any ART groups in the drop-down list. In this event, try broadening the serach by changing the report period to a longer time frame, and also by changing the parameters like Client IP Address etc.

Scenario 3 - Troubleshooting

Cisco.com



Assume that the NFT indeed shows that the problem is with the network. To find out where the problem is, you check the Link Utilization of the client Branch Router.

Step 2:

Check the link utilization on the client Branch Router.

a. Click on the Monitor Tab

b. Click on Switch/Router –> Interface

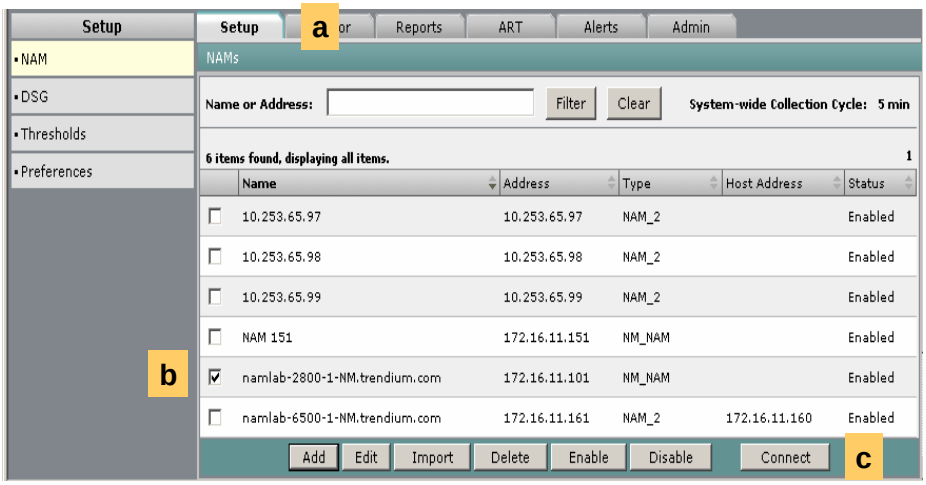
c. In the Parameters Pane, select the appropriate DSG and time period.

d. Click on Refresh

Note: You will see a report as soon as you click on Switch / Router → Interface. Click on the Down Arrow at the top right hand side to toggle the display of the Parameters pane and select the appropriate parameters.

Scenario 3 - Troubleshooting

Cisco.com



Knowing that some application is eating up bandwidth on the branch router, you use the Single Sign–On feature of PVM to logon to the NM–NAM on the branch router and check for the applications that are using that particular link.

Step 3:

Using the PVM Single Sign–On feature, logon to the Branch Router NM–NAM for further troubleshooting.

a. Click on the Setup Tab

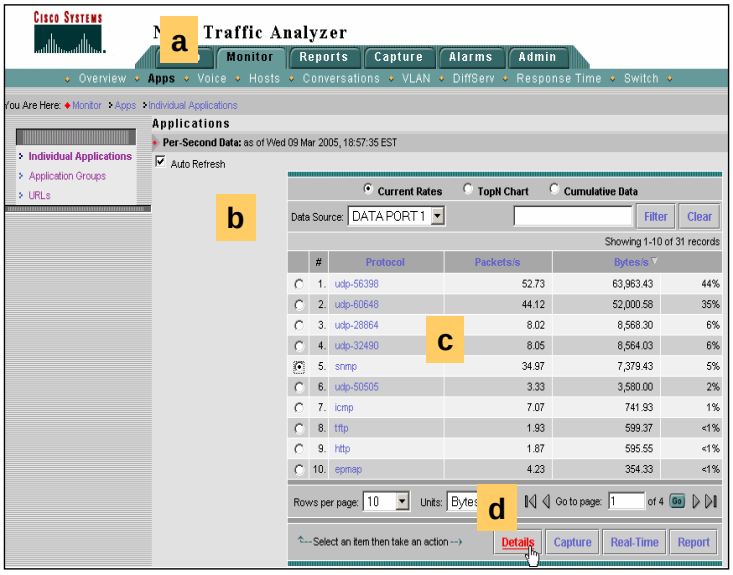
b. Check the appropriate NAM

c. Click on Connect

PVM takes you to the NAM Overview page.

Scenario 3 - Troubleshooting

Cisco.com



You find that a multi– GB FTP transfer was initiated by a host. You report this to the network planning group and close the ticket.

Step 4:

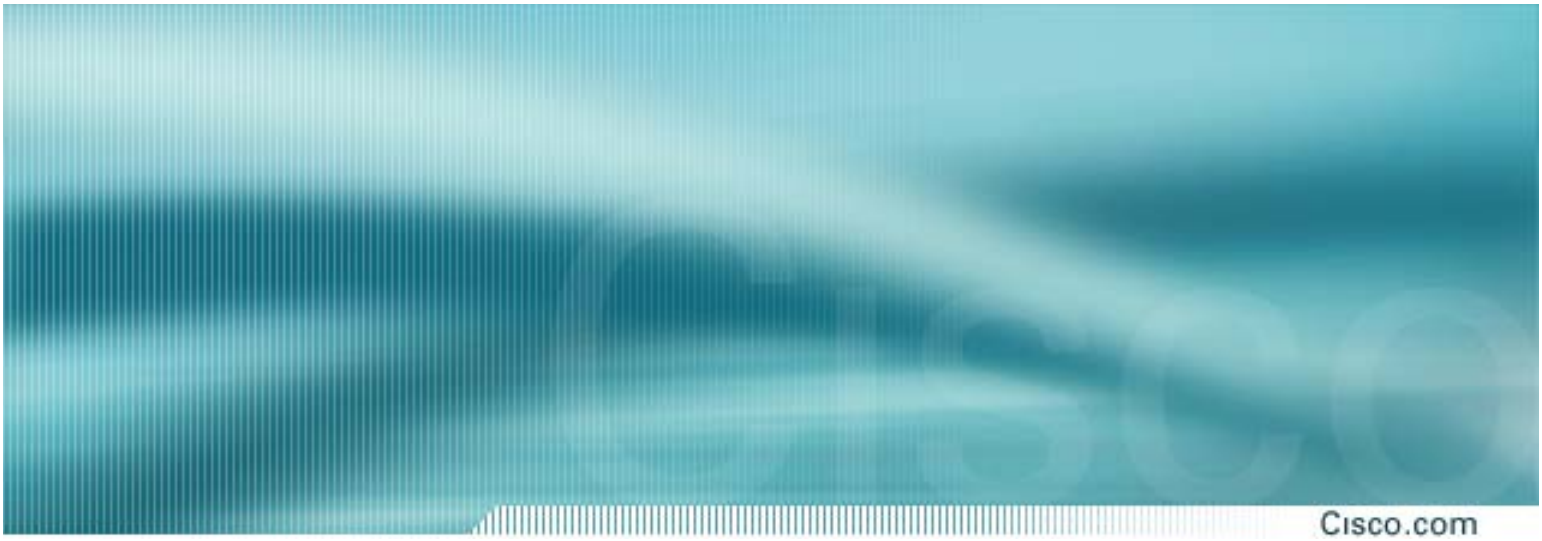
Using the PVM Single Sign–On feature, logon to the Branch Router NM–NAM for further troubleshooting.

a. Click on Monitor –> Apps

b. Select the appropriate data source

c. Top protocols are shown.

d. Select the FTP (For ex) protocol and click on details to view the hosts using that protocol.



Chapter 4

Administration & Maintenance

Cisco Performance Visibility Manager 1.0

Database Maintenance

Cisco.com

- **Overview**
- **Archiving & Purging**

Database Management Overview

PVM uses 2 database instances to store data:

OLTP Database – OLTP database is the application data store, where login information, configuration information etc. is stored, as well as the initial repository for collected traffic information. The raw traffic data is stored in the OLTP database until it is purged (in 2 days). The data for the Monitor charts comes from this database.

OLAP Database – The OLAP database is used as the long–term data store for traffic data. No configuration information is stored in this database. This database contains the aggregated information, based on the hourly, daily and yearly retention periods. The data for Historical Reports comes from this database.

Note: Raw traffic data is converted periodically from the OLTP database into an aggregated form in the OLAP database

Default DB Usernames, Roles, and SIDs

Cisco PVM uses the following instance ID's and username passwords for the oracle database instances

OLTP:

SID: CNAM User : cnam / cnam1 Role: USER

OLAP:

SID: SPDW User : tadw / tadw Role: USER

OLTP & OLAP: User : tadwop / tadwop Role: Operator

* It is recommended that the DBA change the passwords after installation.

Archiving

Cisco PVM provides a way to archive the data in the application data store. This archival feature is based on the oracle import/export utilities. The archive file is a oracle .dmp file that is compressed using the gzip utility. The following aspects need to be kept in mind when dealing with data archival:

- Archiving is disabled by default. When enabled, only data since the last archive is archived.
- What data can be archived? Configuration information from the OLTP database, and Traffic statistics from the OLTP and OLAP databases
- Archived data can be re–imported. Re–imported data will not be re–archived.
- Archives are run at 3:00 am when enabled (those without the –I switch).
- The archives are 7 day rolling archives
- Offline storage of archives is left to the user.

To schedule archiving, use the following command as pvmadm user:

$ archive -p <Operator password> -f <File location> -<flag> start

To stop archival use the following command as pvmadm user

$ archive –p <Operator password> stop

The following flags are available and can be used in any combination:

- I **- Perform archive immediately**
- H **- Consider historical data**
- T **- Consider non-historical data**
- C **- Archive configuration objects**

Import of Archives

Data that has been archived can be re-imported into PVM . To re-import the data, the follow these steps:

Unzip the archive file. An example of the command to use would be:

$gunzip –c <archive fine name>|cpio –icvB “*TC*”

Use the standard oracle import utility to import the data. Use the appropriate Oracle SID:

If you are importing configuration information or near-realtime data from the OLTP database use the CNAM SID.

If you are importing historical data from the OLAP database, use the SPDW SID:

$su – oracle

$imp file=<unzipped file name> userid=tadwop/tadwop@CNAM ignore=y

OR

$imp file=< unzipped file name> userid=tadwop/tadwop@SPDW ignore=y

Purging and Retention Periods

The data that is stored in the two instances of the database in Cisco PVM is periodically purged, so as to allow the user to better manage the data and provide speedy access to the relevant data. The data that is purged from the database depends on the retention periods for each type of data. Cisco PVM is programmed by default to retain information for a certain amount of time. For the raw traffic data in the OLTP database, the retention period is 2 days, and data more than 2 days old is automatically purged. For the historical data in the OLAP database, what is purged is based on the retention period for OLAP Aggregate Data. The default is 3 months for daily data, 1 year of daily data and 3 years of monthly data. The purge process is enabled by default.

You can configure the data retention periods:

- In the OLTP database, change the values of RETENTIONPERIOD in the TA_RETENTION table.
- In the OLAP database, change the values of RETENTIONPERIOD in the RETENTION table (you need to log in as dw/password in order to access this table).

Troubleshooting

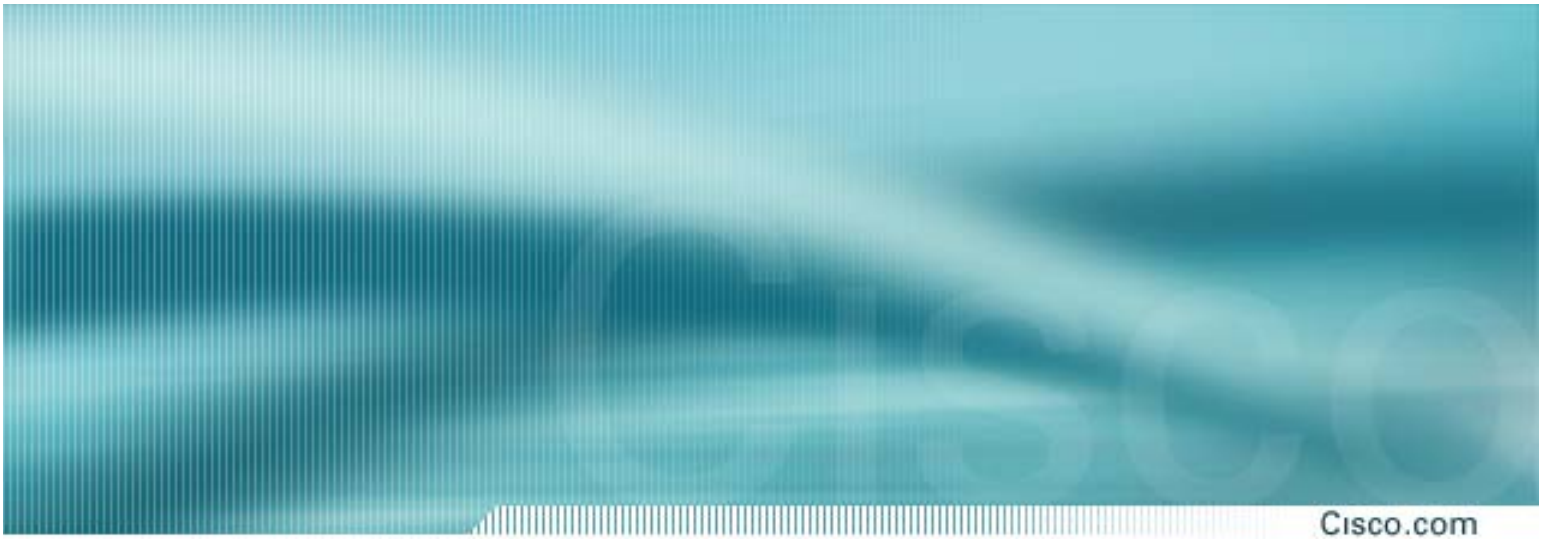
Cisco.com

Go to:
http://www.cisco.com/en/US/products/ps6768/prod_troubleshooting_guide_book09186a008063d44c.html

The Cisco PVM Troubleshooting Guide is available online at Cisco.com. You can download and print the guide using Adobe Reader through your Web browser, or you can order a copy of the guide (P/N OL–8619–01).

The guide provides the following PVM information:

- Deployment FAQs & Troubleshooting
- Setup FAQs & Troubleshooting
- Monitor and Reports FAQs & Troubleshooting
- ART FAQs & Troubleshooting
- General FAQs & Troubleshooting
- Trace Files



Chapter 5

References

Cisco Performance Visibility Manager 1.0

Reference Materials

Below are links to documents and Web pages that provide further details on Cisco Performance Visibility Manager and Network Analysis Modules (NAMs).

Cisco Performance Visibility Manager

Release Notes

http://www.cisco.com/en/US/products/ps6768/prod_release_note09186a0080640a00.html

Quick Start and Documentation Guide

http://www.cisco.com/en/US/products/ps6768/products_quick_start09186a00806409e9.html

User Guide

http://preview.cisco.com/en/US/products/ps6768/products_user_guide_book09186a008063d44f.html

Troubleshooting Guide

http://www.cisco.com/en/US/products/ps6768/prod_troubleshooting_guide_book09186a008063d44c.html

Installation Guide

http://www.cisco.com/en/US/products/ps6768/products_installation_guide_book09186a008063d41d.html

Cisco Catalyst 6500 and Cisco 7600 Series NAM (NAM-1, NAM-2)

Quick Start Guide

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps5401/prod_installation_guides_list.html

Product Literature (Data Sheets, Case Studies, Bulletins)

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html

Questions and Answers

http://www.cisco.com/en/US/partner/products/hw/modules/ps2706/products_qanda_item09186a00800a2c88.shtml

Cisco Branch Routers Series NAM (NM-NAM)

Quick Start Guide

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps5401/prod_installation_guides_list.html

Product Literature (Data Sheets, Case Studies, Bulletins)

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html

Questions and Answers

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5644/index.html

Cisco Network Analysis Module Software (Traffic Analyzer)

Release Notes

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps5401/prod_release_notes_list.html

User Guide

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps5401/products_user_guide_list.html

Online Bug Tracker

Search for known problems using the Cisco bug tracking system tool, called Bug Toolkit. To access Bug Toolkit, perform the following steps:

Go to URL: http://www.cisco.com/cgibin/Support/Bugtool/launch_bugtool.pl.

Log in to Cisco.com.

Click ***Launch Bug Toolkit***.

Locate the product in the list of Cisco Software Products.

Click ***Next***.