



## **Basic Dial NMS Implementation Guide**

Internetworking Solutions Guide  
August 2000

### **Corporate Headquarters**

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

Text Part Number: OL-0556-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED 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.

Access Registrar, AccessPath, Any to Any, Are You Ready, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, IQ Breakthrough, IQ Expertise, IQ FastTrack, IQ Readiness Scorecard, The IQ Logo, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMux, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, CollisionFree, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0005R)

*Basic Dial NMS Implementation Guide*  
Copyright © 2000, Cisco Systems, Inc.  
All rights reserved.



## **Preface   vii**

Purpose	vii
Audience	vii
Scope	vii
Conventions	viii
Related Documentation and Sites	ix
Cisco Connection Online	xi
Documentation CD-ROM	xii
Documentation Feedback	xii
Acknowledgements	xii

## **Overview of Basic SNMP Building Blocks   13**

About SNMP	13
What are the Basic Components of SNMP?	14
About Basic SNMP Message Types and Commands	15
What are SNMP MIBs?	16
What is SNMPv1?	18
What is SNMPv2?	19
About SNMP Management	20
About SNMP Security	21

## **Network Design for a Dial NMS Case Study   23**

Introduction to the Case Study	23
Benefits of a Dial NMS	24
Dial NMS Planning Questionnaire	25
Dial NMS Service Definition	27
Network Topology	30
Hardware Requirements	31
Software Requirements	32
Configuration Design Parameters	33
Implementation and Operation Tasks	35

<b>Dial MIBs and OIDs Used in the Case Study</b>	<b>37</b>
<b>Task 1—Enabling SNMP in a Cisco IOS Device</b>	<b>41</b>
About Enabling SNMP	41
Enabling SNMP	42
<b>Task 2— Exploring SNMP Capabilities by Using UCD-SNMP</b>	<b>45</b>
About Using UCD-SNMP	45
Installing UCD-SNMP and Downloading Cisco MIBs	46
Exploring SNMP MIBs for Dial Networks	46
About SNMP Commander	49
Setting Up SNMP Commander	49
<b>Task 3—Using MRTG to Monitor and Graph Traffic Loads</b>	<b>53</b>
About MRTG	53
About Selecting Dial OIDs	54
How to Inspect and Interpret Data	56
Creating and Editing a Configuration File	59
Sending MRTG Graphs to a Web Server	64
<b>Task 4—Using Syslog, NTP, and Modem Call Records to Isolate and Troubleshoot Fault s</b>	<b>67</b>
About Syslog	67
About NTP	69
About Modem Call Records	69
Enabling NTP on a Cisco IOS Device	71
Setting Up an NTP Client	72
Troubleshooting the NTP Client	74
Enabling Syslog and Modem Call Records in the Cisco IOS Software	74
Configuring the Syslog Daemon	76
Inspecting Syslog Messages in the Log File	78
<b>Task 5—Setting Up a Web Portal for the Dial NMS</b>	<b>81</b>
About a Web Portal	81
Building a Device Linker Web Page	83
Troubleshooting a Cisco 2511 Console Connection	85
About HTTP Access to the CLI	86

Using HTTP to Access CLI Commands	86
<b>Task 6—Managing IP Addresses by Using DNS</b>	<b>91</b>
About Managing IP Addresses	91
Using Cisco Network Registrar CLI Commands	92
Using a Batch File to Make Changes to a DNS Configuration	95
Creating a Primary Forward Zone	96
Creating an IP Tracker Web Page	96
How to Create a Reverse DNS Zone	99
<b>Task 7—Using HP OpenView to Create the SNMP Framework</b>	<b>101</b>
About HP OpenView	101
Verifying the SNMP Configuration	102
About SNMP Demand Polls	105
Performing an SNMP Demand Poll	105
Testing SNMP Get Requests	107
Troubleshooting SNMP and a Demand Poll	108
Verifying that SNMP Traps Are Received	108
Unmanaging the Dial Ports	110
Creating and Adjusting Maps	111
About Discovery Filters	112
Setting Up and Editing a Discovery Filter	113
Using the HPOV CLI to Enter a Device into the Database	115
<b>Task 8—Using CiscoWorks 2000 Resource Manager Essentials</b>	<b>117</b>
About CiscoWorks 2000 RME	117
Importing Devices from HPOV and Populating the Databases	118
Verifying that Device Polling is Turned On	120
Polling the Devices	121
Backing up Cisco IOS Configurations	123
Using CiscoView	124





# Preface

---

## Purpose

This Internetworking Solutions Guide (ISG) describes how to implement and operate a dial network management system (NMS) that provides management functions for a dial Internet access service (DIAS).

## Audience

This guide is intended for network engineers and operators who implement and operate dial NMS systems.

This guide assumes that you have the following level of knowledge and experience:

- An understanding of NMS protocols, such as Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), and syslog.
- Hands-on experience working with Cisco routers, IOS technologies, and UNIX.
- Success configuring a Cisco network access server (NAS) for basic IP modem services.
- A Cisco Certified Network Associate (CCNA) certificate or equivalent level of experience.

## Scope

This guide provides guidelines and a case study for:

- Designing a dial NMS.
- Collecting and using data-management streams to operate a dial access network.
- Managing important connection events and alarms for statistical analysis.
- Reporting on the performance of a DIAS.
- Addressing the perception problems that are commonly associated with dial access networks.

This guide describes the following network protocols, functions, and NMS applications:

- **Protocols**—SNMP and NTP.
- **Functions**—Syslog, modem call records, Cisco IOS command-line interface (CLI), Log File Rotator, Device Navigator, web-based management, and War Dialer.
- **NMS applications**—UCD-SNMP, Multi Router Traffic Grapher (MRTG), HP OpenView (HPOV), and CiscoWorks 2000 Resource Manager Essentials (CW2000 RME).

This guide *does not* provide the following information:

- Descriptions about the basics of network management.  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/index.htm)
- Windows NT-based management of Cisco routers.  
<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm>
- Detailed authentication, authorization, and accounting (AAA).  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/index.htm)
- Basic access server configurations.  
[http://www.cisco.com/cgi-bin/Support/PSP/index.pl?i=Products#Access\\_Products](http://www.cisco.com/cgi-bin/Support/PSP/index.pl?i=Products#Access_Products)
- Information about integrating high-end NMS systems in to a dial access environment.  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/index.htm>

## Conventions

Convention	Description
<b>bold</b>	Command or keyword that you must enter.
<i>italic</i>	File names, directory paths to files, user names, and arguments for which you supply values.
[x]	Optional keyword or argument that you enter.
{x   y   z}	Required keyword or argument that you must enter.
[x {y   z}]	Optional keyword or argument that you enter with a required keyword or argument.
string	Set of characters that you enter. Do not use quotation marks around the character string, or the string will include the quotation marks.
screen	Information that appears on the screen.
^ or Ctrl	Control key—for example, ^D means press the Control and the D keys simultaneously.
< >	Nonprinting characters, such as passwords.
!	Comment line at the beginning of a line of code.



### Caution

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss.



**Note**

Means reader take note. Notes contain helpful suggestions or reference to materials not contained in this manual.

**Timesaver**

Means the described action saves time. You can save time by performing the action described in the paragraph.

**Tips**

Means the information might help the reader solve a problem.

## Related Documentation and Sites

See the following related documentation and web sites for more information:

- Technical References and Support
- Internetworking Solutions Guides
- Freeware
- Cisco Product Documentation

## Technical References and Support

- Center of Excellence Internet Access Engineering—A site dedicated to developing lightweight tools and techniques for supporting the implementation and operation of Internet access services. This site is an educational endeavor of the University of Texas at Austin and Cisco Systems, Inc.  
<http://mccain.ots.utexas.edu/index.html>
- Wholesale Dial Resources—Provides links to technical documents related to wholesale dial Internet access services.  
<http://mccain.ots.utexas.edu/coe/wholesaledial/index.html>
- Technical Assistance Center—Provides technical support information about Cisco technologies. Locate your technology of interest from a list of available technology pages, which are continually updated by Cisco TAC engineers.  
<http://www.cisco.com/pcgi-bin/ibld/view.pl?i=support&m=GUEST>
- SNMP Technology Support Pages—Provides an overview of SNMP, network design tips, implementation and operation guidelines, and links to suggested reading.  
[http://www.cisco.com/pcgi-bin/Support/PSP/psp\\_view.pl?p=Internetworking:SNMP](http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:SNMP)  
<http://www.cisco.com/warp/public/535/3.html>  
<http://www.faqs.org/faqs/snmp-faq/>
- CiscoWorks 2000 TAC Support Page—Describes how to implement, operate, and troubleshoot Cisco Works 2000.  
[http://www.cisco.com/pcgi-bin/Support/PSP/psp\\_view.pl?p=Software:CiscoWorks2000](http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Software:CiscoWorks2000)

- Access Technology Software Center—Provides the firmware for modem upgrades.  
<http://www.cisco.com/kobayashi/sw-center/sw-access.shtml>
- Increasing Security on IP Networks—Addresses network-layer security issues.  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm>
- Carnegie Mellon CERT® Security Improvement Modules—Provides information about security management.  
<http://www.cert.org/security-improvement/>

## Internetworking Solutions Guides

- *Cisco AS5x00 Case Study for Basic IP Modem Services*—Describes how to configure, verify, and troubleshoot basic IP modem services.  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/as5xipmo/index.htm>
- *Cisco AAA Implementation Case Study*—Describes how to design, implement, and operate basic Cisco IOS AAA security and accounting functions.  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/aaaisg/index.htm>
- *Access VPN Solutions Using Tunneling Technology*—Describes how to configure, verify, and troubleshoot access VPN solutions. See also *Access VPDN Dial-in Using L2TP*.  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/index.htm>

## Freeware

- Sunfreeware.com—A repository of freeware programs and news for Solaris.  
<http://www.sunfreeware.com/>
- The UCD-SNMP Home Page—Provides an overview of UCD-SNMP, links to the FTP site, recent news, documentation, bug reports, mailing lists, and where to go for more information.  
<http://ucd-snmp.ucdavis.edu/>
- Multi Router Traffic Grapher (MRTG) Product Site—Provides an overview of MRTG, links to the FTP site, documentation, frequently asked questions, mailing lists, and contact information.  
<http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html>

## Cisco Product Documentation

- *Modem Router Connection Guide*—A starting point for understanding basic modem cabling and configuration. To view this guide, you must be a CCO member.  
<http://cio.cisco.com/warp/customer/76/9.html>
- *AT Command Sets and Register Summaries*—A list of AT commands for configuring and operating MICA and Microcom modems. Most modems function well with their default settings; however, AT commands are required for special features and troubleshooting modems.  
[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/5300/mod\\_info/at/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/mod_info/at/index.htm)

- *Managing Modems* (Cisco IOS 12.1)—Describes configuration and troubleshooting tasks for dial access environments.  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dialts\\_c/dtsprt2/dcdm odmg.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dialts_c/dtsprt2/dcdm odmg.htm)
- *Modem Management Commands* (Cisco IOS 12.1 and 12.0)—Provides two lists of Cisco IOS modem commands used for configuring and troubleshooting modems.  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dial\\_r/drdshom.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dial_r/drdshom.htm)  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/dial\\_r/drprt1/drmodmgt .htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/dial_r/drprt1/drmodmgt .htm)
- *CiscoWorks 2000 Documentation Set*—A collection of configuration guides and reference manuals.  
<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm>

## Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact [cco-help@cisco.com](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).



### Note

If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact the Cisco Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or [tac@cisco.com](mailto:tac@cisco.com). To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or [cs-rep@cisco.com](mailto:cs-rep@cisco.com).

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package that ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription.

You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select Documentation. After you complete the form, click **Submit** to send it to Cisco.

You can also submit feedback on Cisco documentation by sending an e-mail to [bug-doc@cisco.com](mailto:bug-doc@cisco.com) or sending a fax to (408) 527-8089. We appreciate your comments.

## Acknowledgements

This guide was created as a collaborative effort. The following Cisco team members participated: David Anderson, Oscar Bauer, Robert Brown, Drew Cupp, Katie Creegan, Barry Raveendran Greene, Jessica Janis, Andrew Kennedy, Jim Leonard, Robert Lewis, Lori Livingston, Greg McMillan, Roger Moises, Rizwan Mushtaq, Anjali Puri, Annie Shi, David Simms, Jim Thompson, Kris Thompson, Craig Tobias, Patrick Van Deynse, and Mario Villarreal.



# Overview of Basic SNMP Building Blocks

---

## About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that facilitates the exchange of management information between a network management system (NMS), agents, and managed devices. SNMP uses the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

There are three versions of SNMP:

- **SNMP Version 1 (SNMPv1)**—The initial implementation of the SNMP protocol, which is described in RFC 1157 (<http://www.ietf.org/rfc/rfc1157>).
- **SNMP Version 2 (SNMPv2)**—An improved version of SNMPv1 that includes additional protocol operations. For the SNMPv2 Structure of Management Information (SMI), see RFC 1902 (<http://www.ietf.org/rfc/rfc1902>).
- **SNMP Version 3 (SNMPv3)**—SNMPv3 has yet to be standardized.

The case study in this guide describes how to create a dial NMS environment. To successfully manage the environment, you must be familiar with the SNMP feature set. The following NMS applications use SNMP to help manage the network devices in the case study:

- UCD-SNMP
- Multi-Router Traffic Grapher (MRTG)
- HP OpenView (HPOV)
- Cisco Works 2000 Resource Manager Essentials (CW2000 RME)

**Table 1**     *Related SNMP Documentation and Sites*

Site Description	URL
<b>SNMP Technology TAC Page</b> —Network design tips, implementation and operation guidelines, which are continually updated by Cisco TAC engineers.	<a href="http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:SNMP">http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:SNMP</a>
<b>The SimpleWeb</b> —Public domain software packages, which are available on the Internet. Most of the software is a spin-off from SNMP related research.	<a href="http://penta.ufrgs.br/gereint/impl.htm">http://penta.ufrgs.br/gereint/impl.htm</a>
<b>SNMP FAQ</b> —Frequently asked questions about SNMP.	<a href="http://www.pantherdig.com/snmpfaq/">http://www.pantherdig.com/snmpfaq/</a> <a href="http://www.faqs.org/rfcs/rfc1382.html">http://www.faqs.org/rfcs/rfc1382.html</a>

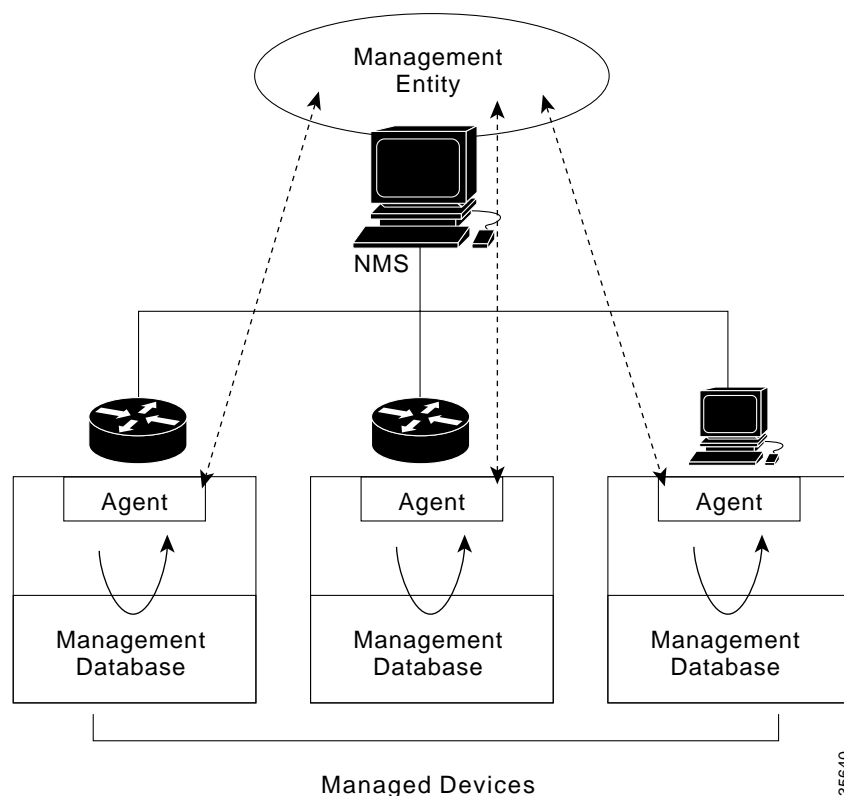
## What are the Basic Components of SNMP?

An SNMP-managed network consists of three key components: managed devices, agents, and network management systems (NMS).

- **Managed devices**
  - Contain an SNMP agent and reside on a managed network.
  - Collect and store management information and make it available to NMS by using SNMP.
  - Include routers, access servers, switches, bridges, hubs, hosts, or printers.
- **Agent**—A network-management software module, such as the Cisco IOS software, that resides in a managed device. An agent has local knowledge of management information and makes that information available by using SNMP.
- **Network Management Systems (NMS)**—Run applications that monitor and control managed devices. NMS provide resources required for network management. In the case study, the NMS applications are:
  - UCD-SNMP
  - MRTG
  - HPOV
  - CW2000 RME

Figure 1 illustrates the relationship between the managed devices, the agent, and the NMS.

**Figure 1** *An SNMP-Managed Network*



## About Basic SNMP Message Types and Commands

There are three basic SNMP message types:

- **Get**—NMS-initiated requests used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.
- **Set**—NMS-initiated commands used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.
- **Trap**—Agent-initiated messages sent from a managed device, which reports events to the NMS.

The Cisco IOS generates SNMP traps for many distinct network conditions. Through SNMP traps, the Network Operations Center (NOC) is notified of network events, such as:

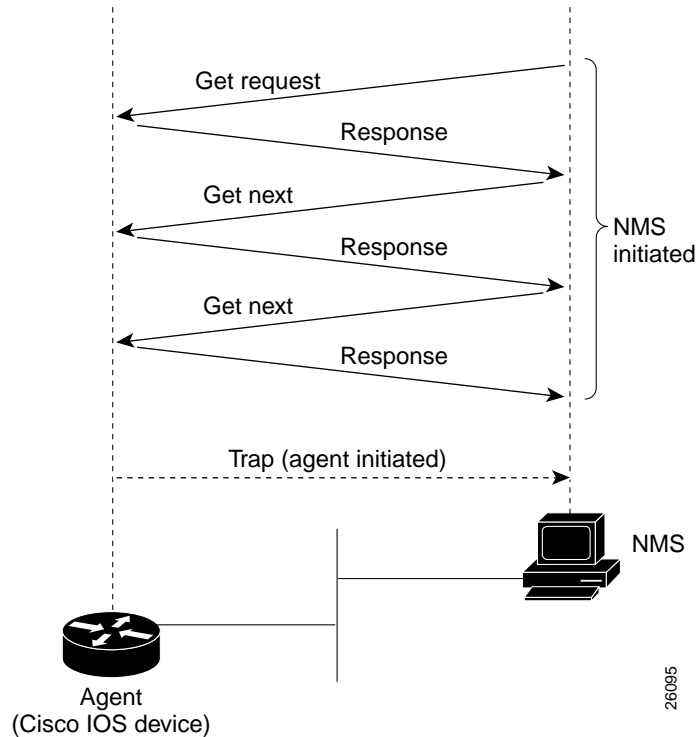
- Link up/down changes
- Configuration changes
- Temperature thresholds
- CPU overloads



**Note**

For a list of Cisco-supported SNMP traps, go to <http://www.cisco.com/public/mibs/traps/>

Figure 2 SNMP Event Interactions Between the NMS and the Agent



## What are SNMP MIBs?

A Management Information Base (MIB):

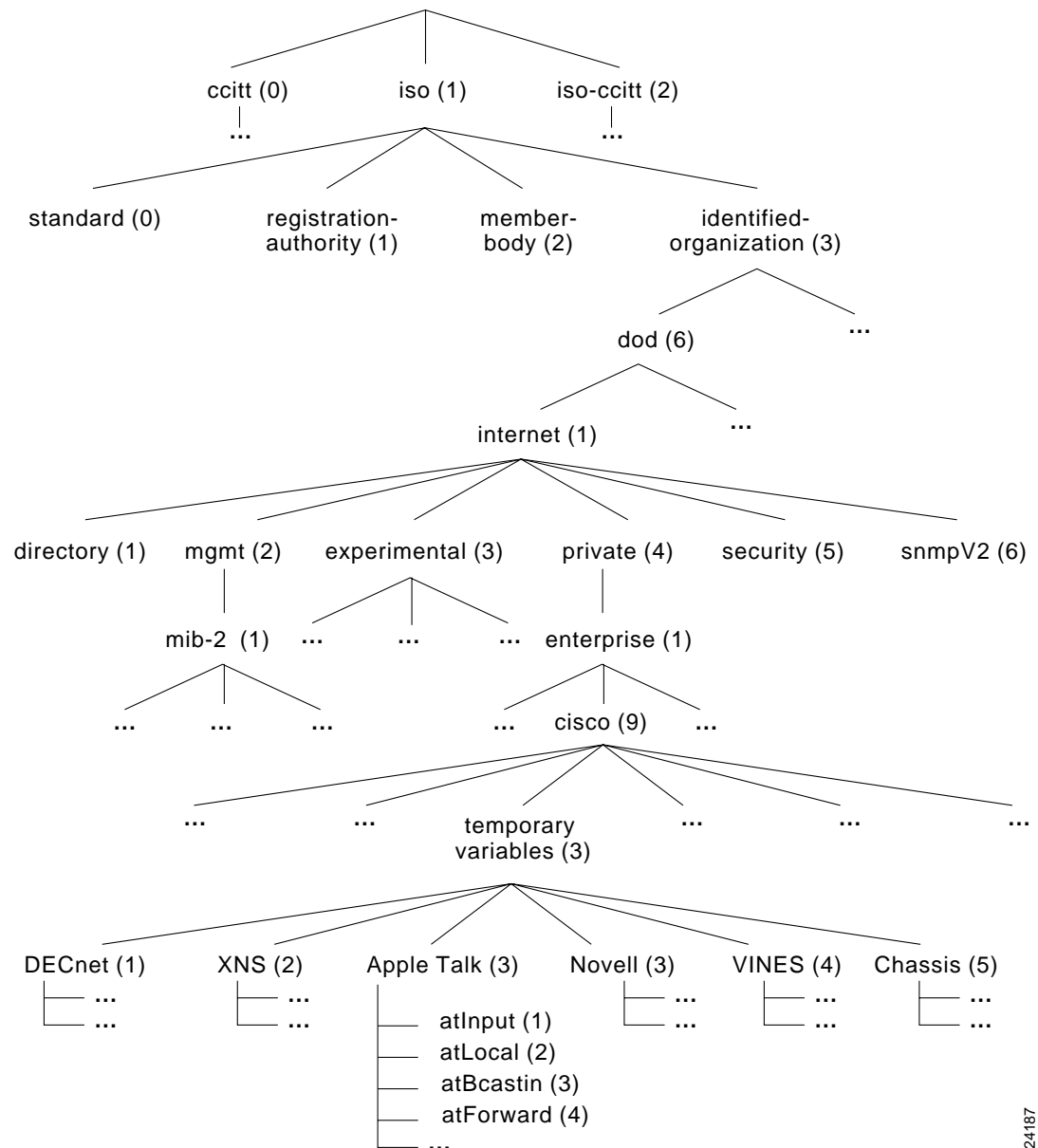
- Presents a collection of information that is organized hierarchically.
- Is accessed by using a network-management protocol, such as SNMP.
- References managed objects and object identifiers.

**Managed object**—A characteristic of a managed device. Managed objects reference one or more object instances (variables). Two types of managed objects exist:

- Scalar objects—Define a single object instance.
- Tabular objects—Define multiple-related object instances that are grouped together in MIB tables.

**Object identifier** (or object ID)—Identifies a managed object in the MIB hierarchy. The MIB hierarchy is depicted as a tree with a nameless root. The levels of the tree are assigned by different organizations and vendors.



**Figure 3** The MIB Tree and Its Various Hierarchies

24187

As shown in Figure 3, top-level MIB object IDs belong to different standards organizations while low-level object IDs are allocated by associated organizations. Vendors define private branches that include managed objects for products. Non standard MIBs are typically in the experimental branch.

A managed object has these unique identities:

- **The object name**—For example, iso.identified-organization.dod.internet.private.enterprise.cisco.  
temporary variables.AppleTalk.atInput  
or
- **The equivalent object descriptor**—For example, 1.3.6.1.4.1.9.3.3.1.

SNMP must account for and adjust to incompatibilities between managed devices. Different computers use different data-representation techniques, which can compromise the ability of SNMP to exchange information between managed devices.

## What is SNMPv1?

SNMPv1 is the initial implementation of the SNMP protocol and is described in RFC 1157 (<http://www.ietf.org/rfc/rfc1157>).

SNMPv1:

- Functions within the specifications of the Structure of Management Information (SMI).
- Operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX).
- Is the de facto network-management protocol in the Internet community.

The SMI defines the rules for describing management information by using Abstract Syntax Notation One (ASN.1). The SNMPv1 SMI is defined in RFC 1155 (<http://www.ietf.org/rfc/rfc1155>). The SMI makes three specifications:

- ASN.1 data types
- SMI-specific data types
- SNMP MIB tables

## SNMPv1 and ASN1 Data Types

The SNMPv1 SMI specifies that all managed objects must have a subset of associated ASN.1 data types. Three ASN.1 data types are required:

- **Name**—Serves as the object identifier (object ID).
- **Syntax**—Defines the data type of the object (for example, integer or string). The SMI uses a subset of the ASN.1 syntax definitions.
- **Encoding**—Describes how information associated with a managed object is formatted as a series of data items for transmission over the network.

## SNMPv1 and SMI-Specific Data Types

The SNMPv1 SMI specifies the use of many SMI-specific data types, which are divided into two categories:

- **Simple data types**—Including these three types:
  - Integers—A signed integer in the range of -2,147,483,648 to 2,147,483,647.
  - Octet strings—Ordered sequences of zero to 65,535 octets.
  - Object IDs—Come from the set of all object identifiers allocated according to the rules specified in ASN.1.

- **Application-wide data types**—Including these seven types:
  - Network addresses—Represent addresses from a protocol family. SNMPv1 supports only 32-bit IP addresses.
  - Counters—Nonnegative integers that increase until they reach a maximum value; then, the integers return to zero. In SNMPv1, a 32-bit counter size is specified.
  - Gauges—Nonnegative integers that can increase or decrease but retain the maximum value reached.
  - Time ticks—A hundredth of a second since some event.
  - Opaques—An arbitrary encoding that is used to pass arbitrary information strings that do not conform to the strict data typing used by the SMI.
  - Integers—Signed integer-valued information. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.
  - Unsigned integers—Unsigned integer-valued information that is useful when values are always nonnegative. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

The SNMPv1 SMI defines structured tables that are used to group the instances of a tabular object (an object that contains multiple variables). Tables contain zero or more rows that are indexed to allow SNMP to retrieve or alter an entire row with a single **Get**, **GetNext**, or **Set** command.

## SNMPv1 Protocol Operations

SNMP is a simple request-response protocol. The NMS issues a request, and managed devices return responses. This behavior is implemented by using one of four protocol operations:

- **Get**—Used by the NMS to retrieve the value of one or more object instances from an agent. If the agent responding to the Get operation cannot provide values for all the object instances in a list, the agent does not provide any values.
- **GetNext**—Used by the NMS to retrieve the value of the next object instance in a table or list within an agent.
- **Set**—Used by the NMS to set the values of object instances within an agent.
- **Trap**—Used by agents to asynchronously inform the NMS of a significant event.

## What is SNMPv2?

SNMPv2 is an improved version of SNMPv1. Originally, SNMPv2 was published as a set of proposed Internet standards in 1993; currently, it is a Draft Standard. As with SNMPv1, SNMPv2 functions within the specifications of the SMI. SNMPv2 offers many improvements to SNMPv1, including additional protocol operations.

## SNMPv2 and SMI

The SMI defines the rules for describing management information by using ASN.1.

RFC 1902 (<http://www.ietf.org/rfc/rfc1902>) describes the SNMPv2 SMI and enhances the SNMPv1 SMI-specific data types by including:

- **Bit strings**—Comprise zero or more named bits that specify a value.
- **Network addresses**—Represent an address from a protocol family. SNMPv1 supports 32-bit IP addresses, but SNMPv2 can support other types of addresses too.
- **Counters**—Non-negative integers that increase until they reach a maximum value; then, the integers return to zero. In SNMPv1, a 32-bit counter size is specified. In SNMPv2, 32-bit and 64-bit counters are defined.

## SMI Information Modules

The SNMPv2 SMI specifies information modules, which include a group of related definitions. Three types of SMI information modules exist:

- **MIB modules**—Contain definitions of interrelated managed objects.
- **Compliance statements**—Provide a systematic way to describe a group of managed objects that must conform to a standard.
- **Capability statements**—Used to indicate the precise level of support that an agent claims with respect to a MIB group. An NMS can adjust its behavior towards agents according to the capability statements associated with each agent.

## SNMPv2 Protocol Operations

The Get, GetNext, and Set operations used in SNMPv1 are exactly the same as those used in SNMPv2. SNMPv2, however, adds and enhances protocol operations. The SNMPv2 trap operation, for example, serves the same function as the one used in SNMPv1. However, a different message format is used.

SNMPv2 also defines two new protocol operations:

- **GetBulk**—Used by the NMS to efficiently retrieve large blocks of data, such as multiple rows in a table. GetBulk fills a response message with as much of the requested data as fits.
- **Inform**—Allows one NMS to send trap information to another NMS and receive a response. If the agent responding to GetBulk operations cannot provide values for all the variables in a list, the agent provides partial results.

## About SNMP Management

SNMP is a distributed-management protocol. A system can operate exclusively as an NMS or an agent, or a system can perform the functions of both.

When a system operates as both an NMS and an agent, another NMS can require the system to:

- Query managed devices and provide a summary of the information learned.
- Report locally stored management information.

# About SNMP Security

SNMP lacks authentication capabilities, which results in a variety of security threats:

- **Masquerading**—An unauthorized entity attempting to perform management operations by assuming the identity of an authorized management entity.
- **Modification of information**—An unauthorized entity attempting to alter a message generated by an authorized entity, so the message results in unauthorized accounting management or configuration management operations.
- **Message sequence and timing modifications**—Occurs when an unauthorized entity reorders, delays, or copies and later replays a message generated by an authorized entity.
- **Disclosure**—Results when an unauthorized entity extracts values stored in managed objects. The entity can also learn of notifiable events by monitoring exchanges between managers and agents.

**Note**

---

Because SNMP does not implement authentication, many vendors do not implement **Set** operations, which reduce SNMP to a monitoring facility.

---





# Network Design for a Dial NMS Case Study

## Introduction to the Case Study

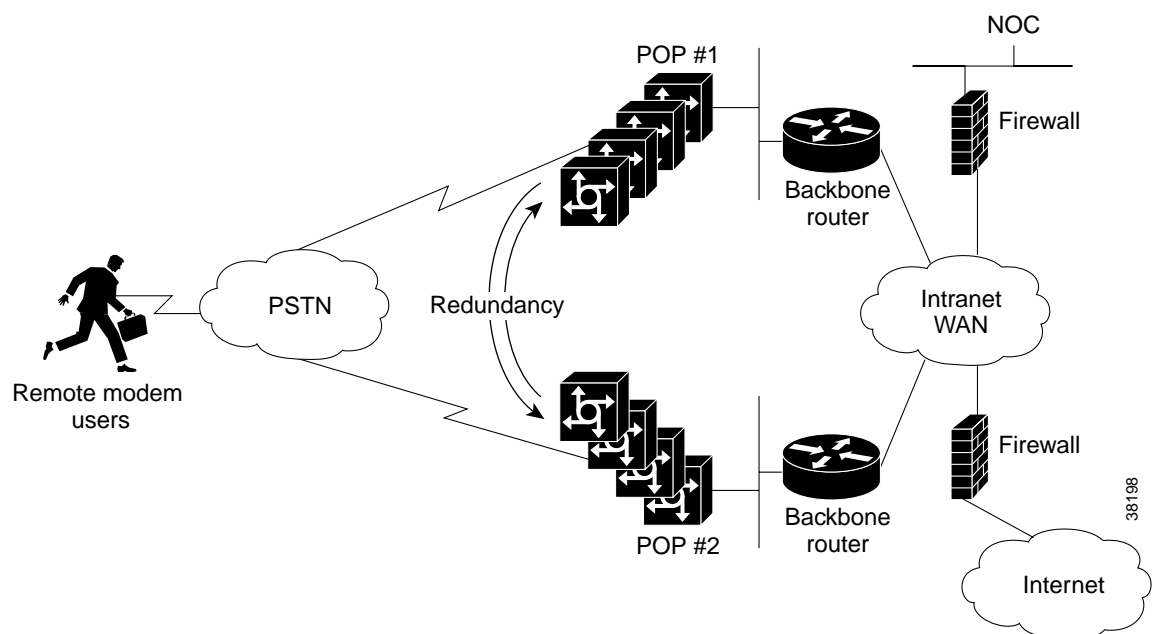
This case study describes:

- How one Internet service provider (ISP) designs, implements, and operates a dial network management system (NMS) for a dial Internet access service (DIAS).
- How to implement dial NMS protocols, applications, and other utilities.

THEnet is an ISP in Austin, Texas that wants to develop a dial NMS and integrate it with its existing Network Operations Center (NOC). THEnet has two dial point-of-presences (POPs) that provide dial-up services for the following types of customers:

- Residential subscribers
- Corporations who outsource their dial-up services and want to avoid the overhead of operating their own dial POP.

**Figure 4** *THEnet Operates Two POPs from One NOC*



- All remote modem users share a common pool of modem resources. Users can dial in to either POP.
- The dial POPs are redundant. If one POP loses service, traffic is re-routed to the other POP. Describing how traffic is re-routed is outside the scope of this case study, and the diagrams in the case study show simplified IP paths only.

THEnet uses this model to identify the different functional areas of the dial NMS:

**F** = Fault management

**C** = Configuration management

**A** = Accounting management

**P** = Performance management

**S** = Security management

A dial NMS provides the FCAPS management functions for a DIAS.

## Benefits of a Dial NMS

A dial NMS:

- Increases network availability
- Improves end-user satisfaction by improving service performance
- Provides fault-isolation capabilities, which improves fault-analysis information
- Reduces network support costs
- Enables capacity planning
- Enables security improvements
- Provides accounting (for example, billing and chargeback)
- Processes important connection events and alarms for statistical analysis
- Provides performance-reporting capabilities for a dial Internet access service
- Enables standardized software releases (for example, software versions and configuration files)
- Addresses the perception problems that are commonly associated with dial access networks



# Dial NMS Planning Questionnaire

This planning questionnaire describes information that is essential for creating a dial NMS service definition. A questionnaire helps network engineers make accurate design decisions and consider alternative solutions. The network engineers at THENet answered the design questions as shown in Table 2.

**Table 2**     *Network Design Questions and Answers*

Network Design Questions	THENet Answers
What types of services does your network provide?	Dial Internet access services (V.90 analog modem services)
How many dial POP sites are you managing?	Two sites in Austin, Texas
What types of network services will the DIAS support? (Network management is based on customer requirements.)	<ul style="list-style-type: none"> <li>• Residential subscriber services</li> <li>• Corporate-outsourcing services</li> </ul>
What is the user-growth projection for the next 5 years? 3 months = Current deployment requirement. 1 year = Current design plan requirement. 5 years = Future scalability plan requirement.	<ul style="list-style-type: none"> <li>• 3 months—50,000 users</li> <li>• 1 year—100,000 users</li> <li>• 5 years—1 million users</li> </ul>
What is the user-to-line ratio during busy hours?	10:1
What level of service must you guarantee to your customers?	Guaranteed up time
Do you have redundant connections to the Internet?	Yes
Do you have redundant connections to the NOC?	Yes
What existing servers do you have available in the NOC?	<ul style="list-style-type: none"> <li>• SNMP management server</li> <li>• Syslog server</li> <li>• AAA server</li> <li>• Database server</li> </ul>
What SNMP framework management system do you want to use?	HP OpenView (HPOV)
What element management system do you use for collecting and managing syslog?	CiscoWorks 2000 Resource Manager Essentials (CW2000 RME)
Do you have a preferred platform and operating system for monitoring the network?	Yes Sun Sparc, Solaris 2.6
What type of network access servers will you use?	Cisco AS5800s
Do you have a staff of UNIX experts?	Yes

**Table 2**     *Network Design Questions and Answers (continued)*

<b>Network Design Questions</b>	<b>THEnet Answers</b>
Do you provide reports for any service level commitments with your customers? If yes, what management systems will you use?	Yes <ul style="list-style-type: none"> <li>• Multi Router Traffic Grapher (MRTG)</li> <li>• Custom-based AAA accounting tools and database query tools</li> </ul>
Identify the types of users who require network management reports.	<ul style="list-style-type: none"> <li>• Network managers</li> <li>• Network operators</li> <li>• Network engineers</li> <li>• Help desk operators</li> <li>• Corporations who outsource their dial-up service</li> <li>• End users</li> </ul>
What types of reports do you provide?	<ul style="list-style-type: none"> <li>• Periodic performance reports</li> <li>• Billing reports</li> <li>• Security reports</li> <li>• Router operations reports</li> <li>• High-priority syslog reports</li> </ul>
What format do the managers want to view the reports in?	HTML web pages and online graphs
Who will monitor the management systems?	The network operations staff
How will network operators be notified of network problems?	By sending e-mail to their pagers
For fault and performance management purposes, do you need to provide call detail records?	Yes Disconnect cause codes and retrain counters must be inspected.
What security protocols do you use for authentication, authorization, and accounting (AAA)?	<ul style="list-style-type: none"> <li>• RADIUS for the remote modem users</li> <li>• TACACS+ for the router administrators in the NOC</li> </ul>
What dial NMS freeware do you plan to use?	MRTG, UCD-SNMP, Linux, and Apache
What software tools do you plan to develop internally?	<ul style="list-style-type: none"> <li>• Log File Rotator</li> <li>• Device Navigator</li> <li>• Modem Call Record Viewer</li> <li>• Web-based management</li> <li>• War Dialer for performance testing (optional)</li> </ul>
Do you plan to build and maintain customized scripts?	Yes

# Dial NMS Service Definition

A service definition is a statement that describes required services for a network design.

The dial NMS service definition determined for THEnet is based on:

- The answers provided in Table 2
- The FCAPS model
  - Fault management
  - Configuration management
  - Accounting management
  - Performance management
  - Security management

**Table 3** *Dial NMS Service Definition for THEnet*

<b>FCAPS Function</b>	<b>Service Requirements and Ways to Collect Management Data</b>
Fault management	<ul style="list-style-type: none"> <li>• SNMP—Use UCD-SNMP and HPOV to explore the SNMP Management Information Bases (MIBs) and create the SNMP framework for the dial NMS.</li> <li>• The Cisco IOS command-line interface (CLI)—Troubleshoot network connectivity problems by collecting robust network statistics. For example, use the following commands:               <ul style="list-style-type: none"> <li>– <b>show controller t1</b></li> <li>– <b>show isdn status</b></li> <li>– <b>debug ppp negotiation</b></li> <li>– <b>show isdn service</b></li> <li>– <b>debug ppp error</b></li> <li>– <b>debug isdn events</b></li> <li>– <b>debug isdn q921</b></li> <li>– <b>debug isdn q931</b></li> </ul> </li> <li>• Syslog—Troubleshoot and isolate faults in the network by collecting syslog data and modem call records. Important syslog messages will be e-mailed daily to the operations staff.</li> <li>• Log file management—Collect and archive syslog data from network access servers.</li> <li>• Web-based management—Navigate devices and enable HTTP access to the CLI.</li> <li>• AAA—Collect accounting disconnect cause codes and view authentication and authorization failures.</li> </ul>

**Table 3** *Dial NMS Service Definition for THEnet (continued)*

<b>FCAPS Function</b>	<b>Service Requirements and Ways to Collect Management Data</b>
Configuration management	<ul style="list-style-type: none"> <li>• <b>SNMP</b>—Use CW2000 RME to archive configuration files, manage Cisco IOS images, determine how much memory is installed, and discover which boot ROMs are present.</li> <li>• <b>CLI</b>—Inspect and modify Cisco IOS configuration files and images. For example, use the following commands: <ul style="list-style-type: none"> <li>– <b>show version</b></li> <li>– <b>show running</b></li> <li>– <b>show modem version</b></li> </ul> </li> <li>• <b>AAA authentication</b>—Control access to the routers.</li> <li>• <b>AAA authorization</b>—Limit CLI command access to router administrators on a per group basis. Authorization is also used for limiting network service assignments, such as static IP addresses and access lists.</li> <li>• <b>AAA accounting</b>—Monitor which configuration changes are made to the routers and identify who is making the changes. Authenticated usernames also appear in syslog.</li> <li>• <b>Effective IP address management</b>—Manage all assigned IP subnets by using a DNS server and the application Cisco Network Registrar.</li> <li>• <b>Web-based management</b>—Navigate devices and enable HTTP access to the CLI.</li> </ul>
Accounting management	<ul style="list-style-type: none"> <li>• <b>Send accounting information to a database that is accessible by Standard Query Language (SQL).</b> Archive user-accounting data for billing and auditing purposes.</li> <li>• <b>Syslog</b>—Collect basic accounting information by using modem call records.</li> <li>• <b>CLI</b>—Collect accounting statistics. For example, use the following commands: <ul style="list-style-type: none"> <li>– <b>show interface accounting</b></li> <li>– <b>show isdn history</b></li> <li>– <b>show controller t1 call-counters</b></li> <li>– <b>show modem log</b></li> <li>– <b>show modem summary</b></li> <li>– <b>show modem call-stats</b></li> </ul> </li> </ul>

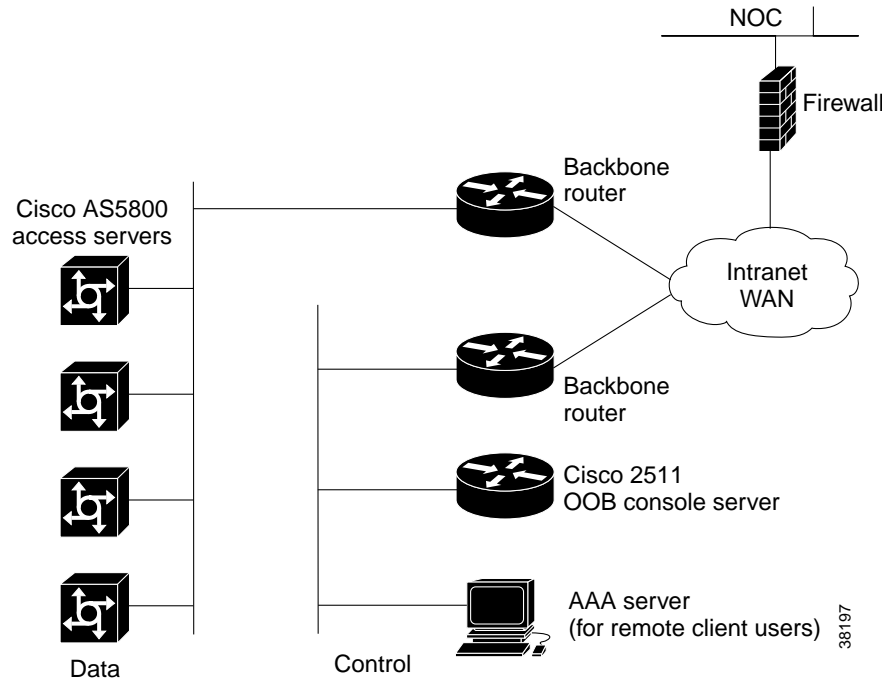
**Table 3** *Dial NMS Service Definition for THEnet (continued)*

<b>FCAPS Function</b>	<b>Service Requirements and Ways to Collect Management Data</b>
Performance management	<ul style="list-style-type: none"> <li>• <b>SNMP</b>—For the initial installation, use MRTG to monitor key Object Identifications (OIDs) in the device MIBs. In the future, use commercial software applications that collect mass scale management data streams for large numbers of access servers.</li> <li>• <b>CLI</b>—Monitor the performance of the access servers. For example, use the following commands: <ul style="list-style-type: none"> <li>– <b>show modem operational-status</b></li> <li>– <b>show modem connect-speeds</b></li> <li>– <b>show modem summary</b></li> <li>– <b>show modem call-stats</b></li> </ul> </li> <li>• <b>Web-based management</b>—Navigate devices and enable HTTP access to the CLI.</li> <li>• <b>War Dialer</b>—Test remote client PCs by using a free client simulator.</li> </ul>
Security management	<ul style="list-style-type: none"> <li>• <b>Authenticate, authorize, and account for dial access clients (modem users) in each POP by using RADIUS.</b></li> <li>• <b>Authenticate, authorize, and account for router administrators in the NOC by using TACACS+.</b></li> <li>• <b>Review the AAA service security logs.</b></li> <li>• <b>Review the AAA server database by using SQL queries.</b></li> <li>• <b>CLI</b>—Inspect security information. For example, use the following commands: <ul style="list-style-type: none"> <li>– <b>show snmp group</b></li> <li>– <b>show access-lists</b></li> <li>– <b>show location</b></li> <li>– <b>show tacacs</b></li> <li>– <b>show radius statistics</b></li> <li>– <b>show logging</b></li> </ul> </li> <li>• <b>Web-based management</b>—Navigate devices and enable HTTP access to the CLI.</li> </ul>

# Network Topology

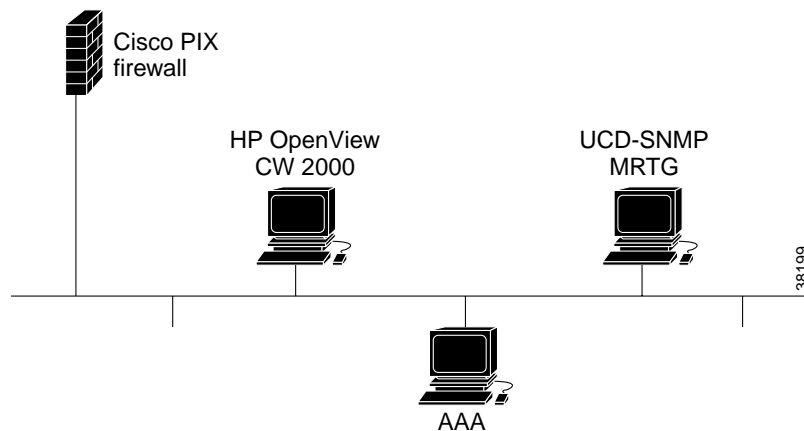
Based on the dial NMS service definition in Table 3, the network engineers at THENet defined the network topology for the POPs and NOC.

**Figure 5** *Network Topology for One POP*



An intranet WAN connects the two POPs together and routes traffic to the Internet. The NOC collects management data from both POPs.

**Figure 6** *Network Topology for the NOC*



An important design issue to consider is where to send syslog data. If syslog data is sent back to a central site NOC, the syslog data must travel across WAN links. Estimate and monitor how much syslog data is generated by each POP and the impact on the WAN links. Modem call records can add a significant amount of traffic to syslog data.

In this case study, THENet initially sends syslog data across WAN links to the NOC. The WAN links are designed to support a large network capacity in a metropolitan area. Collecting syslog locally in each POP is a future design consideration.

## Hardware Requirements

To design the dial NMS for the two POPs and the NOC, the network engineers at THENet defined these hardware requirements:

**Table 4** *Hardware Description for Two POPs and the NOC*

Hardware	Purpose
4 Cisco AS5800 access servers	Two access servers in each POP to provide access in to the Internet from the PSTN. Cisco IOS Release 12.0(7)T is installed in each access server.
2 backbone gateways	Enables management data streams to enter the NOC. Routes traffic to the intranet WAN and the Internet.
2 Cisco 2511 OOB console servers	Accesses the console ports in the Cisco AS5800s by using out-of-band (OOB) management lines.
3 AAA servers	One server in each POP to authenticate, authorize, and account for dial access clients by using RADIUS. One server in the NOC to authenticate, authorize, and account for router administrators by using TACACS+.
1 Cisco PIX firewall	Protects the NOC by filtering the devices that can access management services, such as TACACS+, RADIUS, syslog, and SNMP.
3 Sun Ultra 10 workstations	Operates the dial NMS inside the NOC. Solaris version 2.6 is used.

The following capacity-planning calculations were made to determine the number of required lines and Cisco AS5800s for the next five years.

Basic parameters:

- There are 23 available bearer channels per PRI line
- There are 28 PRI lines per T3 card (644 channels)
- Each Cisco AS5800 has two T3 cards
- There are 1288 available bearer channels per dual T3 Cisco AS5800

**Table 5** *Capacity-Planning Matrix for the Line and Chassis Requirements*

Time	Busy Hour Ratio	Users Required	Lines Required	Chassis Calculation	AS5800s Required
3 months	10:1	50,000	5000	5000 lines / 1288 = 3.88 chassis	4 AS5800s
1 year	10:1	100,000	10,000	10,000 lines / 1288 = 7.76 chassis	8 AS5800s
5 years	10:1	1,000,000	100,000	100,000 lines / 1288 = 77.64 chassis	78 AS5800s

These calculations in Table 5 are based on a PRI system integration—not a system signalling 7 (SS7) integration.

For each POP site, also plan for the following elements:

- Power, space, and cooling for each Cisco AS5800
- Required number of AAA servers
- Required number of Cisco 2511s (OOB ports)
- WAN link capacity

## Software Requirements

To design the dial NMS inside the NOC, the network engineers at THENet identified these software and management system requirements:

**Table 6** *Dial NMS Software and Management System Requirements*

Software and Management Systems	Purpose
UCD-SNMP	Uses CLI-based SNMP freeware to explore the SNMP MIBs and OIDs that are useful for operating a dial network.
Multi Router Traffic Grapher (MRTG), version 2.8.12	Monitors and graphs the traffic load on the network.
Web-based management	<p>Manages a network by using light-weight NMS tools (LWT). A LWT is light on:</p> <ul style="list-style-type: none"> <li>• Budget</li> <li>• Staff support</li> <li>• Course requirements</li> <li>• GUI requirements</li> </ul> <p>THENet requires the following LWTs:</p> <ul style="list-style-type: none"> <li>• Device Navigator—A web page that links network devices together.</li> <li>• Cisco IOS Command Center—A web page that provides HTTP access to the CLI.</li> <li>• Log File Rotator—A freeware script that archives, sorts, and deletes syslogs.</li> <li>• Modem Call Record Viewer—A tool that enables you to view modem records and syslogs on a web page.</li> </ul>
HP OpenView (HPOV) Network Node Manager Release 5.0	Creates the SNMP framework for the dial NMS and identifies what is breaking in the network.
CiscoWorks 2000, maintenance release 2 Resource Manager Essentials (RME), version 2.2	<p>Archives configuration files, upgrades the Cisco IOS, determines how much memory is installed, and discovers what boot ROMs are present.</p> <p>You can install HPOV and CW2000 RME on the same Sun workstation—without conflicts.</p>



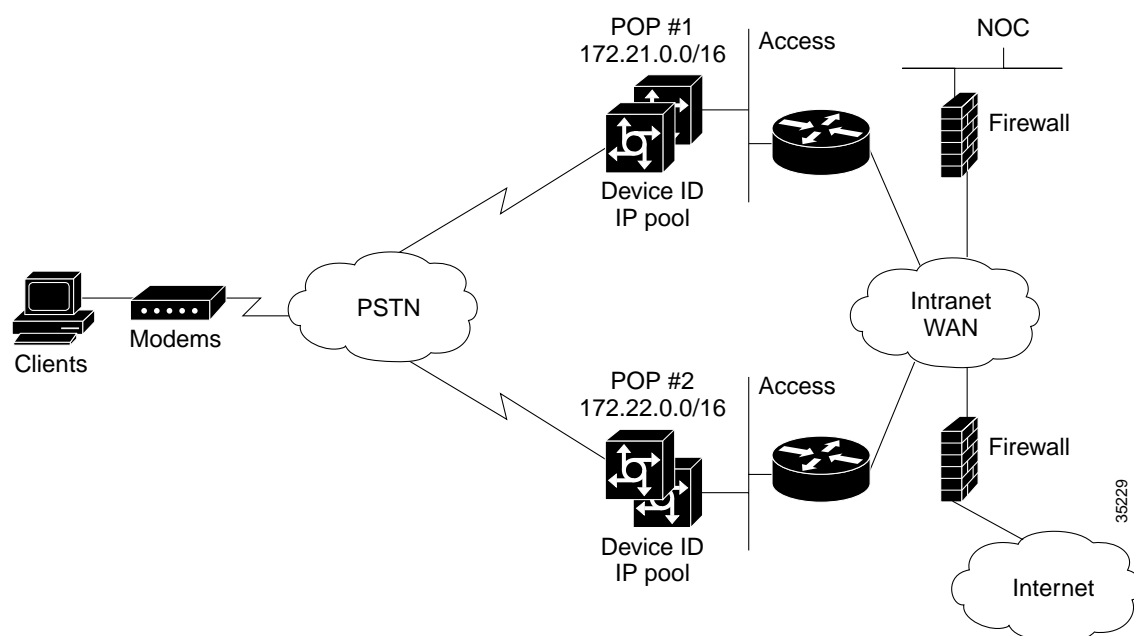
**Table 6** *Dial NMS Software and Management System Requirements (continued)*

Software and Management Systems	Purpose
CiscoSecure Unix, version 2.3(3)	<ul style="list-style-type: none"> <li>Authenticates, authorizes, and accounts for dial access clients in each POP by using RADIUS.</li> <li>Authenticates, authorizes, and accounts for router administrators in the NOC by using TACACS+.</li> <li>Uses AAA accounting records to collect performance data, fault data, and track router configuration changes.</li> </ul>
War Dialer	Runs performance tests by using a dial simulator and client PCs.

## Configuration Design Parameters

Before THENet can implement and operate the dial NMS, several design parameters must be defined by the network engineers and operators.

Each dial POP requires enough IP address space for the POP to grow to its maximum size. For THENet, each POP must support up to 50,000 lines. Therefore, an entire class B network is initially assigned to each POP.

**Figure 7** *IP Subnetting Diagram for the THENet*

To simplify IP address management, each POP uses a similar IP subnetting plan.

**Table 7** *IP Subnetting Plan for POP #1 and POP #2*

Network Name	Assigned IP Subnet	Description
POP #1	172.21.0.0/16	Class B IP subnet assigned to POP #1.
POP #2	172.22.0.0/16	Class B IP subnet assigned to POP #2.
NOC	172.23.10.0/24	Class C IP subnet assigned to the NOC.
Access	172.21.101.0/24 172.21.102.0/24 172.22.101.0/24 172.22.102.0/24	Primary and secondary class C access Ethernet subnets. All the access devices in each POP are directly connected to these subnets.
DeviceID	172.21.10.0/24 172.22.10.0/24	Identifies each Cisco IOS device with a unique, fixed, and stable loopback IP address for network management purposes.  One IP address is assigned to the loopback 0 interface of each Cisco IOS device.  One IP address block is used to simplify IP-security filtering at the NOC. This technique protects the NOC from devices that should not access management services, such as TACACS+, RADIUS, syslog, and SNMP.
IP pool	172.21.103.0/24 172.21.104.0/22  172.22.103.0/24 172.22.104.0/22	Hosts a pool of IP addresses for the dial access clients with modems.  This IP assignment provides 1280 IP addresses to each POP. The access servers create the IP routes to support the IP pools.  Few IP routes are summarized to the backbone instead of advertising 1280 host routes.

**Table 8** *SNMP Community Strings Used at THENet*

Community Strings	Purpose
5urf5h0p	Assigns a read-only (RO) community string to enable SNMP polling and SNMP get requests.
5crapmeta1	Assigns a read-write (RW) community string to enable router configuration changes.

**Caution**

Do not use “public” or “private” strings, which are well known in the industry, are common hardware defaults, and invite attacks from hackers—regardless if you use filters. To maximize security, choose community strings that are not associated with your personal life or company.

The information in Table 9 is posted and maintained on web-based management pages. Easy access to this information reduces network downtime.

**Table 9** *T1 Support Management Information at THEnet*

T1 Dial-in Number	Circuit ID	Support Contract	Contact Phone Number
512-111-2222	72ABCA047006-001PT	ABC	512-555-1212
512-333-4444	72ABCA047006-002PT	DEF	512-555-1212

## Implementation and Operation Tasks

THEnet implements and operates the dial NMS in two phases:

- **Phase A**—Exploring and setting up basic dial NMS functions by using free management software and light-weight NMS tools:
  - Task 1—Enabling SNMP in a Cisco IOS Device
  - Task 2— Exploring SNMP Capabilities by Using UCD-SNMP
  - Task 3—Using MRTG to Monitor and Graph Traffic Loads
  - Task 4—Using Syslog, NTP, and Modem Call Records to Isolate and Troubleshoot Faults
  - Task 5—Setting Up a Web Portal for the Dial NMS
- **Phase B**—Monitoring and maintaining basic dial NMS functions by using commercially available management systems:
  - Task 6—Managing IP Addresses by Using DNS
  - Task 7—Using HP OpenView to Create the SNMP Framework
  - Task 8—Using CiscoWorks 2000 Resource Manager Essentials



**Note** Providing information for integrating high-end management systems is beyond the scope of this case study.

The examples in this document are taken from a Sun Microsystems workstation running Solaris 2.6. Some commands and filenames may vary slightly on other Unix systems, such as Linux and HP UX.





## Dial MIBs and OIDs Used in the Case Study

This section describes the MIBs and OIDs used to manage the dial Internet access service in the case study.

See the following tables and choose the variables you want to use in your network. Explore the OIDs and determine whether to poll and graph the results on a regular basis.

- To explore the MIBs and OIDs, use UCD-SNMP. For more information, see the “Task 2— Exploring SNMP Capabilities by Using UCD-SNMP” section on page 45.
- To graph the trending statistics for a specific OID, use Multi Router Traffic Grapher (MRTG). For more information, see the “Task 3—Using MRTG to Monitor and Graph Traffic Loads” section on page 53.



### Caution

Be cautious when polling network elements. Polling OIDs that retrieve large amounts of data can cause CPU problems on a Cisco IOS device. For example, do not get the ARP table, walk large portions of a MIB tree, poll the wrong OID too frequently, or get statistics that have an entry for every interface. For example, a Cisco 7200 may have 10 interfaces; whereas, a Cisco AS5800 may have 3,000 interfaces.

**Table 10** MIBs to Consider Using for the Dial NMS

Dial Related	System Management	MIB II / Interfaces
CISCO-POP-MGMT-MIB <sup>1</sup>	OLD-CISCO-CHASSIS	RFC1213-MIB
CISCO-MODEM-MGMT-MIB	CISCO-MEMORY-POOL-MIB	IF-MIB
CISCO-VPDN-MGMT-MIB	CISCO-SYSTEM-MIB	CISCO-CAS-IF-MIB
CISCO-AAA-SESSION-MIB	CISCO-FLASH-MIB	CISCO-ISDN-MIB
CISCO-AAA-SERVER-MIB	CISCO-CONFIG-MAN-MIB	
CISCO-CALL-HISTORY-MIB	CISCO-PROCESS-MIB	
CISCO-DIAL-CONTROL-MIB		
CISCO-CALL-RESOURCE-POOL-MIB		

1. This MIB was enhanced in Cisco IOS Release 12.1(2)XH and later releases.

- For a complete list of available Cisco MIBs, go to <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>
- For a list of Cisco-supported traps, go to <http://www.cisco.com/public/mibs/traps>

- For more information about other NMS enhancements for dial, see *Call Tracker plus ISDN and AAA Enhancements for the Cisco AS5300 and Cisco AS5800* at [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xh/121xh\\_2/dt\\_cltrk.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xh/121xh_2/dt_cltrk.htm)

**Note**

To protect a network access server from over polling, use the SNMP get bulk feature. It's available in SNMP v2 in CISCO-BULK-FILE-MIB.

Table 11 and Table 12 identify useful OIDs and variables within selected MIBs from Table 10. Equivalent Cisco IOS commands are shown wherever applicable. Sometimes data is more clearly inspected by using OIDs and a graphing tool instead of CLI commands.

To see the complete structure of the CISCO-POP-MGMT-MIB and CISCO-MODEM-MGMT-MIB, go to the following URLs:

- CISCO-POP-MGMT-MIB  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/popmgt.txt>
- CISCO-MODEM-MGMT-MIB  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/modemmgt.txt>

**Table 11**    *Description of CISCO-POP-MGMT-MIB*

Description	OID	Equivalent Cisco IOS Command
Number of analog calls connected	cpmISDNCFgBChanInUseForAnalog .1.3.6.1.4.1.9.10.19.1.1.2	<b>show modem summary</b>
Number of active DS0s in use	cpmActiveDS0s .1.3.6.1.4.1.9.10.19.1.1.4	<b>show controllers t1 call-counters</b>  <b>show isdn memory</b> (See the number of call control blocks, CCBs, in the command output.)
Total call count per DS0	cpmCallCount .1.3.6.1.4.1.9.10.19.1.1.1.7	<b>show controllers t1 call-counters</b>
Total time in use for each DS0	cpmTimeInUse .1.3.6.1.4.1.9.10.19.1.1.1.8	<b>show controllers t1 call-counters</b>
Total octets received on a DS0	cpmInOctets .1.3.6.1.4.1.9.10.19.1.1.1.9	None available
Total octets transmitted on a DS0	cpmOutOctets .1.3.6.1.4.1.9.10.19.1.1.1.10	None available
Total packets received on a DS0	cpmInPackets .1.3.6.1.4.1.9.10.19.1.1.1.11	None available

**Table 11** Description of CISCO-POP-MGMT-MIB (continued)

Description	OID	Equivalent Cisco IOS Command
Total packets transmitted on a DS0	cpmOutPackets .1.3.6.1.4.1.9.10.19.1.1.1.12	None available
Number of active PPP calls	cpmPPPCalls .1.3.6.1.4.1.9.10.19.1.1.5	None available
Number of active V120 calls	cpmV120Calls .1.3.6.1.4.1.9.10.19.1.1.6	None available
Number of active V110 calls	cpmV110Calls .1.3.6.1.4.1.9.10.19.1.1.7	None available
Maximum number of DS0s used simultaneously	cpmActiveDS0sHighWaterMark .1.3.6.1.4.1.9.10.19.1.1.8	<b>show controllers t1 call-counters</b>
Type of call currently connected to each DS0	cpmDS0CallType .1.3.6.1.4.1.9.10.19.1.1.1.5	None available

**Table 12** Description of CISCO-MODEM-MGMT-MIB

Variable Description	OID	Equivalent Cisco IOS Command
Modems available to take calls	cmSystemModemsAvailable .1.3.6.1.4.1.9.9.47.1.1.7	<b>show modem summary</b>
Average call duration for each modem	cmCallDuration .1.3.6.1.4.1.9.9.47.1.3.1.1.9	<b>show modem</b>
Number of times each modem failed to answer	cmRingNoAnswers .1.3.6.1.4.1.9.9.47.1.3.3.1.1	<b>show modem</b>
Number of times each modem failed to train up successfully	cmIncomingConnectionFailures .1.3.6.1.4.1.9.9.47.1.3.3.1.2	<b>show modem</b>
Number of times each modem successfully trained up	cmIncomingConnectionCompletions .1.3.6.1.4.1.9.9.47.1.3.3.1.3	<b>show modem</b>
Current TX speed for all the modems	cmTXRate .1.3.6.1.4.1.9.9.47.1.3.1.1.14	<b>show modem connect-speeds</b>
Current RX speed for all the modems	cmRXRate .1.3.6.1.4.1.9.9.47.1.3.1.1.15	<b>show modem connect-speeds</b>
List of users currently connected and authenticated	cpmActiveUserID .1.3.6.1.4.1.9.10.19.1.3.1.1.3	<b>show caller</b>
Call durations for currently connected and authenticated users	cpmActiveCallDuration .1.3.6.1.4.1.9.10.19.1.3.1.1.8	<b>show caller</b>

**Table 12** *Description of CISCO-MODEM-MGMT-MIB (continued)*

<b>Variable Description</b>	<b>OID</b>	<b>Equivalent Cisco IOS Command</b>
List of user CLIDs	cpmActiveRemotePhoneNumber .1.3.6.1.4.1.9.10.19.1.3.1.1.2	<b>show caller ip</b> <b>show isdn history</b>
List of called DNIS phone numbers	cpmActiveLocalPhoneNumber .1.3.6.1.4.1.9.10.19.1.3.1.1.13	<b>show caller ip</b>
List of TTY interfaces in use	cpmActiveTTYNumber .1.3.6.1.4.1.9.10.19.1.3.1.1.14	<b>show caller ip</b>
List of which user is using which modem slot	cpmActiveModemSlot .1.3.6.1.4.1.9.10.19.1.3.1.1.6	<b>show caller user</b>
List of which user is using which modem port	cpmActiveModemPort .1.3.6.1.4.1.9.10.19.1.3.1.1.7	<b>show caller user</b>
List of which IP addresses are currently in use	cpmActiveUserIpAddr .1.3.6.1.4.1.9.10.19.1.3.1.1.4	<b>show caller ip</b>





## Task 1—Enabling SNMP in a Cisco IOS Device

---

### About Enabling SNMP

In this case study:

- Each Cisco IOS device is identified by a fixed and stable loopback IP address for network management purposes. The IP address functions as an device ID.

One block of loopback IP addresses is used to simplify IP-security filtering at the NOC. This technique protects the NOC from devices that should not access management services, such as TACACS+, RADIUS, syslog, and SNMP.

- The dial NMS environment interfaces with SNMP through these applications:
  - UCD-SNMP
  - SNMP Commander
  - Multi-Router Traffic Grapher (MRTG)
  - HP OpenView (HPOV)
  - Cisco Works 2000 Resource Manager Essentials (CW2000 RME)



#### Caution

---

Avoid using well-known community strings, such as “public,” “private,” or “cisco.” These strings are easily guessed and leave your device open to malicious attacks or inadvertent access. To further enhance SNMP security, apply access lists to the community strings.

---

# Enabling SNMP

To enable SNMP on a Cisco IOS device in the network, follow these steps.



**Note** In some software releases, the commands **snmp-server engineID local** and **snmp-server packetsize** are enabled by default.

**Step 1** To use Loopback0 for device management and set SNMP traps to use that IP address, enter the following commands. This configuration also eliminates the need to change IP addresses if a different interface is used to send traps.

```
!  
interface Loopback0  
  ip address 172.21.10.1 255.255.255.255  
!  
  
!  
snmp-server trap-source Loopback0  
!
```

**Step 2** To enable a basic SNMP configuration, enter the following commands. See Table 13 for descriptions of each command.

```
snmp-server community Surf5h0p RO  
snmp-server community Scrapmetal RW  
snmp-server location Lake Travis (Austin) Dial POP  
snmp-server contact net-admin@aurora.the.net  
snmp-server enable traps  
snmp host 172.23.10.1 traps SNMPv1
```

Table 13 SNMP Command Descriptions

Command	Purpose
snmp-server community Surf5h0p RO	Assigns a read only (RO) community string. Only get requests (queries) can be performed.  The RO community string in this example (Surf5h0p) allows Get requests but no Set operations. The NMS and the managed device must reference the same community string.
snmp-server community Scrapmetal RW	Assigns a read write (RW) community string. SNMP applications require RW access for Set operations.  The RW community string in this example (Scrapmetal) enables write access to OID values. For example, you can shut down an interface, download a configuration file, or change a password.
snmp-server location Lake Travis (Austin) Dial POP	Specifies the location of the device for administrative purposes.
snmp-server contact admin net-admin@aurora.the.net	Specifies a contact name to notify whenever a MIB problem occurs.

**Table 13** *SNMP Command Descriptions (continued)*

Command	Purpose
<code>snmp-server enable traps</code>	<p>Enables traps for unsolicited notifications for configuration changes, environmental variables, and critical device conditions.</p> <p>This command enables 14+ other commands for distinct types of SNMP traps. Edit this command list to include only the traps that are used by your network environment.</p>
<code>snmp host 172.23.10.1 traps SNMPv1</code>	Identifies the host destination for the traps. Traps are sent in the SNMP v1 format in this case study.





## Task 2— Exploring SNMP Capabilities by Using UCD-SNMP

---

### About Using UCD-SNMP

Researching and identifying which functions are available in SNMP are part of building a dial NMS environment. In this case study, UCD-SNMP, an opensource freeware application that allows access to SNMP functions from a command line interface (CLI), is used to explore the capabilities of SNMP.

There are many benefits to using UCD-SNMP.

You can:

- Gain a fundamental understanding of how SNMP functions and protocols work in a dial access environment. This knowledge provides a solid foundation for using automated and GUI-based SNMP applications.
- Learn how to use a low-level troubleshooting capability in the event that other SNMP applications produce questionable results.
- Poll any OID and verify SNMP agent responses.
- Use stable and reliable CLI commands. UCD-SNMP is unobstructed by GUI functionality.
- Explore and research MIB content.
- Discover what functions are available to manage a Cisco IOS device.
- Create customized scripts and tools.

For this case study, the dial engineers at THENet created a tool called SNMP Commander. The tool aided the MIB research task by enabling dial engineers to build web-based object identification (OIDs) bookmarks, which they could go to without using a keyboard.

By using UCD-SNMP and SNMP Commander, the dial engineers at THENet identified which items the commercial NMS applications would monitor within the network operations center (NOC).

## Installing UCD-SNMP and Downloading Cisco MIBs

To install UCD-SNMP and download MIBs from the Cisco FTP site, follow these steps.



**Note** You can also download individual MIBs from <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

- 
- Step 1** Go to <http://ucd-snmp.ucdavis.edu>
- Step 2** Download, compile, and install UCD-SNMP. In this case study, the UCD-SNMP commands are installed in the `/usr/local/bin` directory.
- Step 3** From the Cisco FTP site, download the MIBs into the `/usr/local/share/snmp/mibs` directory on your Solaris workstation. By using the following Unix commands, you can copy the entire bundled v1 MIB tar file from [ftp.cisco.com](http://ftp.cisco.com).

```
cd /usr/local/share/snmp/mibs
ftp ftp.cisco.com
cd /pub/mibs/v1
bin
get v1.tar.gz
exit
```

- Step 4** Decompress and untar the files in the `/usr/local/share/snmp/mibs` directory:

```
gzip -d v1.tar.gz
tar -xvf v1.tar
```



**Note** There are many MIBs in the tar file that you may not use. Regardless, Cisco recommends you keep all the MIBs on file to support your evolving network needs.

## Exploring SNMP MIBs for Dial Networks

To explore the MIBs for a Cisco IOS device by using SNMP CLI commands, follow the steps in this section. Poll OID variables by using the commands **snmpget**, **snmpwalk**, and **snmptable**.



**Note** This section assumes you already have a basic understanding of UCD-SNMP and know how to use its CLI commands.

- 
- Step 1** To determine the last restart reason for the router, enter the **snmpget** command and the relevant OID. In the following example, the restart reason is “reload.”

```
onionring:~$ snmpget travis-nas-01.the.net 5urf5h0p .1.3.6.1.4.1.9.2.1.2.0
Counter32 (is a reserved word): At line 6 in /usr/local/share/snmp/mibs/SNMPv2-S
MI-V1SMI.my
Gauge32 (is a reserved word): At line 7 in /usr/local/share/snmp/mibs/SNMPv2-SMI
-V1SMI.my
Integer32 (is a reserved word): At line 8 in /usr/local/share/snmp/mibs/SNMPv2-S
MI-V1SMI.my
Did not find 'mib-2' in module RFC1213-MIB (/usr/local/share/snmp/mibs/IANAifTyp
e-MIB-V1SMI.my)
```

```
enterprises.9.2.1.2.0 = "reload"
```

If SNMP-parsing errors are generated, suppress them by appending **2>/dev/null** to the end of the command. Standard output is tagged as 1. Error output is tagged as 2.

```
onionring:~$ snmpget travis-nas-01.the.net Surf5h0p .1.3.6.1.4.1.9.2.1.2.0 2> /dev/null
enterprises.9.2.1.2.0 = "reload"
onionring:~$
```



**Note** If no response is returned by the SNMP agent, allow error messages to print to the screen by removing the **2>/dev/null** argument.

**Step 2** Check the system up time by entering the **snmpget** command and sysUpTime OID:

```
onionring:~$ snmpget travis-nas-01.the.net Surf5h0p .1.3.6.1.2.1.system.sysUpTime.0 2> /dev/null
system.sysUpTime.0 = Timeticks: (45450609) 5 days, 6:15:06.09
onionring:~$
```

**Step 3** To gather basic configuration management information about the Cisco IOS device, enter the **snmpwalk** command and the system OID.

```
onionring:~$ snmpwalk travis-nas-01.the.net Surf5h0p system 2> /dev/null
system.sysDescr.0 = "Cisco Internetwork Operating System Software ..IOS (tm) 5800
Software (C5800-P4-M), Version 12.1(2a)T1, RELEASE SOFTWARE (fc2)..Copyright
(c) 1986-2000 by cisco Systems, Inc...Compiled Mon 12-Jun-00 23:13 by ccai"
system.sysObjectID.0 = OID: enterprises.9.1.188
system.sysUpTime.0 = Timeticks: (45492606) 5 days, 6:22:06.06
system.sysContact.0 = "net-admin@aurora.the.net"
system.sysName.0 = "travis-nas-01.the.net"
system.sysLocation.0 = "Lake Travis (Austin) Dial POP"
system.sysServices.0 = 78
system.8.0 = Timeticks: (0) 0:00:00.00
onionring:~$
```

**Step 4** Change the OID environmental prefix by entering the commands **prefix** and **export prefix**. This step reduces the number of key strokes you must enter at the command line.

```
onionring:~$ snmpget travis-nas-01.the.net Surf5h0p .1.3.6.1.4.1.9.2.1.2.0 2> /dev/null
enterprises.9.2.1.2.0 = "reload"
onionring:~$ PREFIX=.1.3.6.1.4.1.9
onionring:~$ export PREFIX
onionring:~$ snmpget travis-nas-01.the.net Surf5h0p 2.1.2.0 2> /dev/null
enterprises.9.2.1.2.0 = "reload"
onionring:~$
```

The UCD-SNMP application attaches a prefix to the requested variable unless it is fully qualified (for example, unless the variable starts with a period “.”). By default, the prefix points to the MIB-II node .1.3.6.1.2.1 location. The Cisco enterprises prefix points to .1.3.6.1.4.1.9

**Step 5** Inspect the IP address entry table by entering the **snmptable** command and ipAddrTable OID:

```
onionring:~$ snmptable travis-nas-01.the.net Surf5h0p ip.ipAddrTable 2> /dev/null
SNMP table: ip.ipAddrTable.ipAddrEntry
ipAdEntAddr ipAdEntIfIndex ipAdEntNetMask ipAdEntBcastAddr ipAdEntReasmMaxSize
172.21.10.1          351    255.255.255.255          1          18024
172.21.101.20       289    255.255.255.0           1          18024
onionring:~$
```

- Step 6** Poll the interfaces table and redirect the output to a text file by entering the **snmptable** command and ifTable OID:

```
onionring:~$ snmptable travis-nas-01.the.net 5urf5h0p interfaces.ifTable
> /export/home/www/travis-nas-01_ifTable.txt
onionring:~$
```



**Note** Do not forget the space between > and /export

- Step 7** Inspect the contents of the interfaces table by entering the **cat** command. In the following Cisco AS5800 example, notice the interface descriptions (ifDescr) and types (ifType). There is one PPP and DS0 entry for each serial interface.

```
onionring:~$ cat /export/home/www/travis-nas-01_ifTable.txt
SNMP table: interfaces.ifTable.ifEntry
```

ifIndex	ifDescr	ifType	ifMtu	ifSpeed	.....
1	"Async1/2/00"	other	1500	9000	
2	"Async1/2/01"	other	1500	9000	
3	"Async1/2/02"	other	1500	9000	
.					
.					
.					
.					
289	"FastEthernet0/0/0"	ethernetCsmacd	1500	100000000	
290	"Null0"	other	1500	4294967295	
291	"T1 1/0/0"	ds1	?	?	
292	"T1 1/0/1"	ds1	?	?	
.					
.					
.					
301	"T1 1/0/10"	ds1	?	?	
302	"T1 1/0/11"	ds1	?	?	
303	"Serial1/0/0:0"	propPointToPointSerial	1500	64000	
304	"Serial1/0/0:1"	propPointToPointSerial	1500	64000	
.					
.					
.					
326	"Serial1/0/0:23"	lapd	1500	64000	
327	"Serial1/0/0:23-Signaling"	isdn	1500	64000	
328	"Serial1/0/0:0-Bearer Channel"	ds0	?	?	
329	"Serial1/0/0:1-Bearer Channel"	ds0	?	?	
.					
.					
.					
350	"Serial1/0/0:22-Bearer Channel"	ds0	?	?	
351	"Loopback0"	softwareLoopback	15144294967295		

To view the complete, unabridged output for this example, go to  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/iftable.txt>



## About SNMP Commander

The dial engineers at THENet created a tool called SNMP Commander that:

- Provides web-based access to UCD-SNMP CLI commands.
- Builds web-based OID bookmarks, which enable you to go to OIDs without using a keyboard.
- Aids the MIB exploration and NMS design tasks.

By using SNMP Commander and a web browser, you can:

- Create URL links for the network staff and help desk.
- Identify target OIDs you want to graph by using MRTG.
- Inspect thresholds and events to monitor by using other NMS systems.

The following two components work together to create SNMP Commander:

- **snmpcmds.dat**—A comma separated variables file, which includes a list of SNMP CLI commands. This file is read by the snmpcmds.pl script.

For the source code, go to

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/snmpdat.txt>

- **snmpcmds.pl**—A script that loads and reads a data file. You can use additional data files by creating multiple instances of the original script and altering the data file descriptor.

For the source code, go to

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/snmppl.txt>

## Setting Up SNMP Commander

To set up SNMP Commander, follow these steps:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | From CCO, download snmpcmds.dat and snmpcmds.pl   |
| <b>Step 2</b> | Customize the files for your environment. When you find useful OIDs, enter them in the snmpcmds.dat file and use the web-based form of the script to research the MIBs. The web tool functions like an SNMP OID bookmark.   |
| <b>Step 3</b> | Test SNMP Commander by using a web browser: <ul style="list-style-type: none"><li>a. Select an SNMP command and OID.</li><li>b. Select an SNMP agent (Cisco IOS device).</li><li>c. Click <b>Submit</b>.</li><li>d. Inspect the program and query messages.</li></ul> |

Figure 8 SNMP Commander Tool

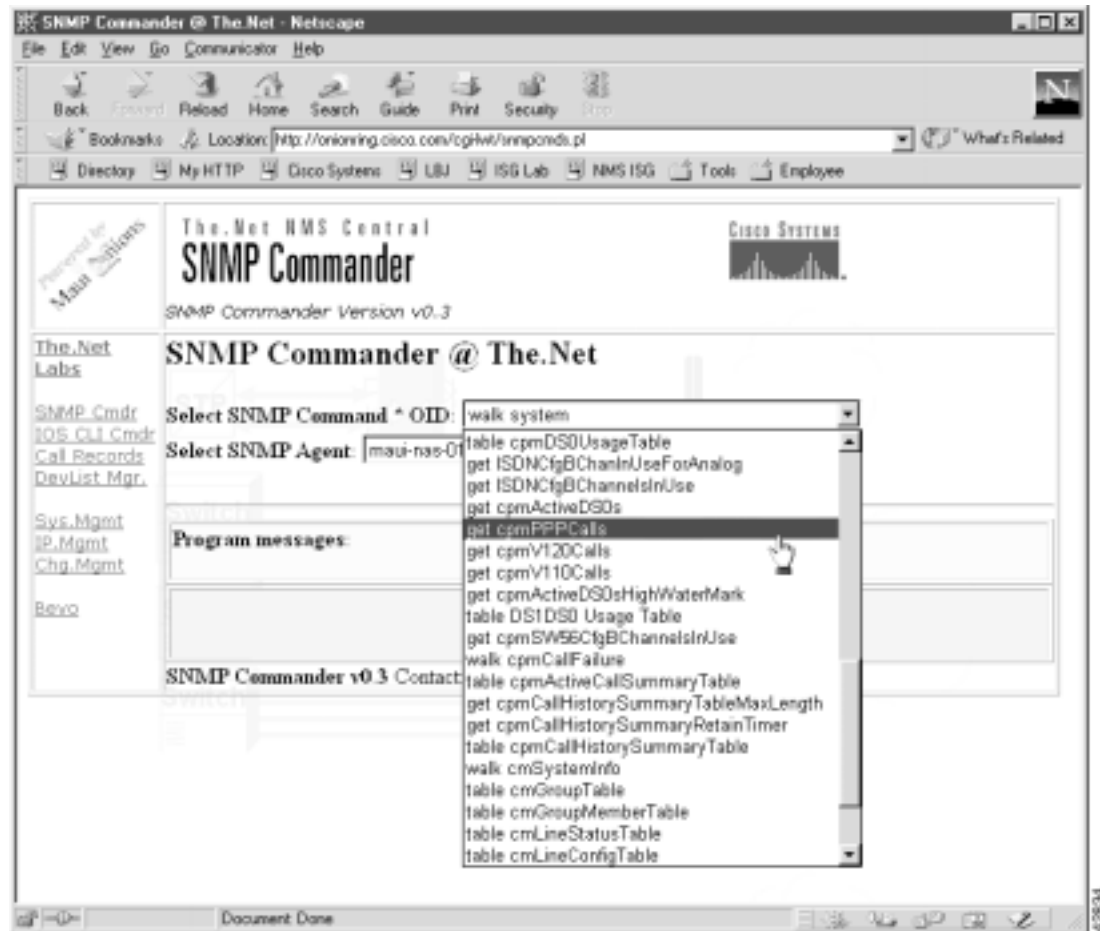


Figure 9 Polling Results from the table `cpmActiveCallSummaryTable` Command

The screenshot shows the SNMP Commander web interface in a Netscape browser window. The page title is "The.Net NMS Central SNMP Commander". The version is "SNMP Commander Version v0.3". The interface includes a navigation bar with links like Back, Forward, Reload, Home, Search, Guide, Print, and Security. The main content area displays the "SNMP Commander @ The.Net" logo and a form to select an SNMP command and agent. The selected command is "table cpmActiveCallSummaryTable" and the agent is "maui-nas-01". Below the form, the "Program messages" section shows the requested command and device. The "Query was:" section displays the command used to retrieve the data. The "SNMP table:" section shows the table name and its contents, which are displayed in a table format.

**Program messages:**

```
Requested Cmd: table cpmActiveCallSummaryTable
Requested Device: maui-nas-01
MIB: CISCO-POP-MGMT-MIB
OID: Numeric = .1.3.6.1.4.1.9.10.19.1.3.1, Symbolic = cpmActiveCallSummaryTable
```

**Query was:** `snmpget -ib -m all maui-nas-01 comm-string .1.3.6.1.4.1.9.10.19.1.3.1 2>/dev/null`

**SNMP table:** enterprises.cisco.ciscoExperiment.ciscoPopMgmtMIB.ciscoPopMgmtMIBObjects.cpmActiveCallSummary.cpmActiveCallSummaryTable

index	CallStartTimeIndex	CallSummaryIndex	UserID	UserIPAddr	CallType	NodeSlot	NodePort	CallID
20244644.0	?	?	"rbrown-isdn"	0.0.0.0	digital	-1	-1	0:1:5
20247644.0	?	?	"rbrown-isdn"	0.0.0.0	digital	-1	-1	0:1:5
20786302.0	?	?	"dieyard-isdn"	0.0.0.0	digital	-1	-1	0:0:2





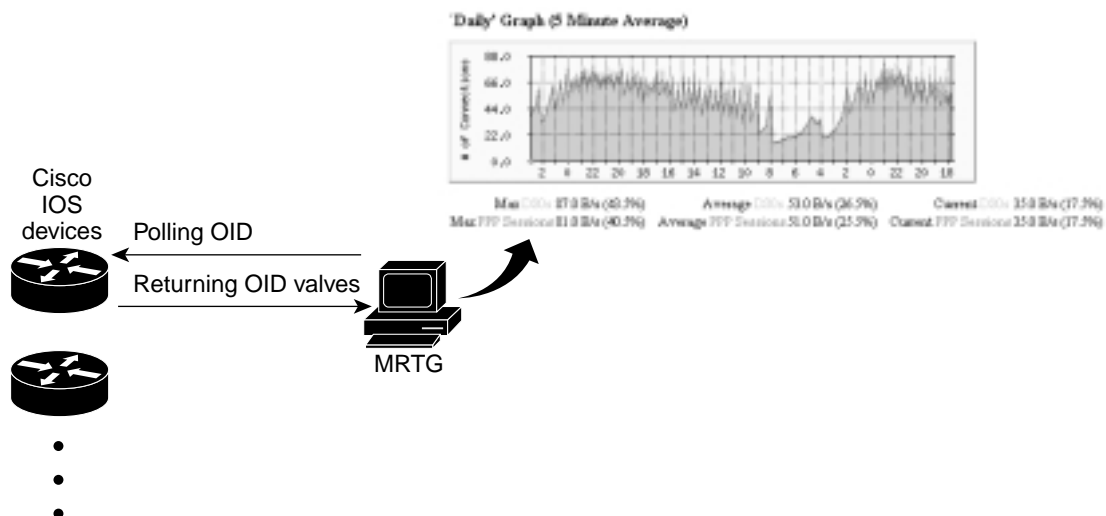
## Task 3—Using MRTG to Monitor and Graph Traffic Loads

### About MRTG

Multi Router Traffic Grapher (MRTG) is a free performance management application for Unix that monitors SNMP statistics from any SNMP capable device on your network and performs the following functions:

- Captures, stores, and graphically presents SNMP data. By default, a web page with four graphs per MIB object (OID) is created by MRTG. The graphs show the variation of MIB data over time.
- Runs from the crontab. Every five minutes, a cron job runs MRTG to query a user-configured list of OIDs and network devices. After each data collection cycle, the MRTG perl script posts updated graphs to a web page.
- Efficiently compresses and archives data samples to create graphs.
- Enables you to determine if trending data is useful for monitoring your environment before you invest in costly network performance software. If trending data is critical to manage your network, it may be necessary to purchase a commercial network performance package, such as Concord Network Health. However, you may find that MRTG is all you need.

**Figure 10** MRTG Polls for OIDs; OID Values that Are Returned to MRTG



35193

For each OID referenced in the configuration file, MRTG creates the following graphs:

- **Daily graph**—5 minute average data points with approximately 33 hours of data presented.
- **Weekly graph**—30 minute average data points with approximately 8 days of data presented.
- **Monthly graph**—2 hour average data points with approximately 5 weeks of data presented.
- **Yearly graph**—1 day average data points with approximately 1 year of data presented.

To quickly create images by using the GD graphics library, go to <http://www.boutell.com/gd>

## About Selecting Dial OIDs

To select which dial OIDs to query when monitoring dial-up activity, see the OIDs listed in the following tables:

- Circuit utilization OIDs (Table 14)
- Modem information OIDs (Table 15)
- User information OIDs (Table 16)



### Caution

Be cautious when polling network elements. Polling OIDs that retrieve large amounts of data can cause CPU problems on a Cisco IOS device. For example, do not get the ARP table, walk large portions of a MIB tree, poll the wrong OID too frequently, or get statistics that have an entry for every interface. For example, a Cisco 7200 may have 10 interfaces; whereas, a Cisco AS5800 may have 3,000 interfaces.

In this case study, the tools UCD-SNMP and SNMP Commander were used to inspect and understand the MIBs. Based on this research, the network engineers at THEnet identified the OIDs in the following tables to program in to MRTG.

To see the complete structure of the CISCO-POP-MGMT-MIB and CISCO-MODEM-MGMT-MIB, go to the following URLs:

- CISCO-POP-MGMT-MIB  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/popmgt.txt>
- CISCO-MODEM-MGMT-MIB  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/modemmgt.txt>

**Table 14**    *Circuit Utilization OIDs*

Variable	Base MIB and OID	Description
Analog calls	CISCO-POP-MGMT-MIB 1.3.6.1.4.1.9.10.19.1.1.2	The number of analog calls connected.
Active DS0s	CISCO-POP-MGMT-MIB 1.3.6.1.4.1.9.10.19.1.1.4	The total number of calls connected.
Call count	CISCO-POP-MGMT-MIB 1.3.6.1.4.1.9.10.19.1.1.1.1.7	The number of calls that have occupied a specific DS0.

**Table 14** *Circuit Utilization OIDs (continued)*

<b>Variable</b>	<b>Base MIB and OID</b>	<b>Description</b>
Time in use	CISCO-POP-MGMT-MIB 1.3.6.1.4.1.9.10.19.1.1.1.8	The time for each DS0.
PPP calls	CISCO-POP-MGMT-MIB 1.3.6.1.4.1.9.10.19.1.1.5	The number of active PPP calls.
DS0 high water mark	CISCO-POP-MGMT-MIB 1.3.6.1.4.1.9.10.19.1.1.8	The maximum number of DS0s ever used simultaneously.

**Table 15** *Modem Information OIDs*

<b>Variable</b>	<b>Base MIB and OID</b>	<b>Description</b>
Modems available	CISCO-MODEM-MGMT-MIB 1.3.6.1.4.1.9.9.47.1.1.7	The number of modems currently available to take calls.
Average call duration	CISCO-MODEM-MGMT-MIB 1.3.6.1.4.1.9.9.47.1.3.1.1.9	The average call duration for each modem in the NAS.
No answers	CISCO-MODEM-MGMT-MIB 1.3.6.1.4.1.9.9.47.1.3.3.1.1	The number of calls not answered by a modem.
Failed Train	CISCO-MODEM-MGMT-MIB 1.3.6.1.4.1.9.9.47.1.3.3.1.2	The number of modem calls that failed to train up.  It's normal behavior for most modems to not have a 100 percent success rate.
Successful train	CISCO-MODEM-MGMT-MIB 1.3.6.1.4.1.9.9.47.1.3.3.1.3	The number of modem calls that successfully trained up.  It's normal for most modems to not have a 100 percent success rate.
TX speed	CISCO-MODEM-MGMT-MIB 1.3.6.1.4.1.9.9.47.1.3.1.1.14	The current transmit speed (TX) of all the modems in the NAS.  If a modem does not have an active call, zero is returned.
RX speed	CISCO-MODEM-MGMT-MIB 1.3.6.1.4.1.9.9.47.1.3.1.1.15	The current receive speed (RX) of all the modems in the NAS.  If a modem does not have an active call, zero is returned.

**Table 16** User Information OIDs

<b>Variable</b>	<b>Base MIB and OID</b>	<b>Description</b>
Active user ID	CISCO-MODEM-MGMT-MIB .1.3.6.1.4.1.9.10.19.1.3.1.1.3	List of users currently connected and authenticated.
Active call duration	CISCO-MODEM-MGMT-MIB .1.3.6.1.4.1.9.10.19.1.3.1.1.8	Call durations for currently connected and authenticated users.
User CLID	CISCO-MODEM-MGMT-MIB .1.3.6.1.4.1.9.10.19.1.3.1.1.2	List of user Caller IDs (CLID).
DNIS phone number	CISCO-MODEM-MGMT-MIB .1.3.6.1.4.1.9.10.19.1.3.1.1.13	List of called Dialed Number Information Service (DNIS) phone numbers.
Active TTY	CISCO-MODEM-MGMT-MIB .1.3.6.1.4.1.9.10.19.1.3.1.1.14	List of asynchronous terminal lines (TTY) in use.
Active modem slot	CISCO-MODEM-MGMT-MIB .1.3.6.1.4.1.9.10.19.1.3.1.1.6	List of which user is using which modem slot.
Active modem port	CISCO-MODEM-MGMT-MIB .1.3.6.1.4.1.9.10.19.1.3.1.1.7	List of which user is using which modem port.
Active user IP	CISCO-MODEM-MGMT-MIB .1.3.6.1.4.1.9.10.19.1.3.1.1.4	List of which IP addresses are currently in use.

## How to Inspect and Interpret Data

Internet users spend approximately 80 percent of their time reading information—not downloading data. Modem traffic is very limited on a per user basis. People cannot read as fast as modems can download. Therefore, watch for the following types of trends and performance data on the access servers:

- PPP sessions in use.
- DS0s in use.
- Modem calls that have been rejected.
- The number of calls coming in to the access server and at what time.
- Spikes or dips in total calls connected outside the normal call pattern.
- Long-term trends that may mean that you need to upgrade components in your network.
- Throughput that has been reduced to unacceptable levels (potential bottlenecks).
- For disaster recovery purposes, when fail over events and routing swaps occur, look for drops in the primary data path and jumps in the backup path.
- The utilization of the IP backbone, such as a Frame Relay link or Ethernet campus.



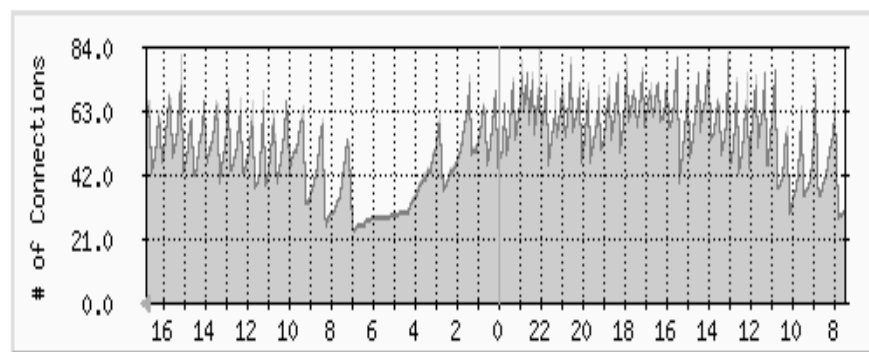
The Connection Success Rate (CSR) is an important metric for tracking and measuring the stability of a dial service. The CSR is defined by the number of modems that successfully train up and go in to connected state. In addition to the CSR, you must track and analyze additional areas. For example, SNMP MIBs can be used to measure the success rate for items such as PPP, AAA, and IP negotiation.

To collect the CSR service level counters, inspect the connection success and failure rate by using modem OIDs or the **show modem** Cisco IOS command. SNMP, rather than the Cisco IOS CLI, is the preferred method to collect these counters. SNMP can scale to support large numbers of access servers.

The following graphs show the DS0s and PPP sessions in use for 70,000 modem users calling in to a dial-up service at a large university. The graphs are taken from one Cisco AS5300 in a large dial-up modem pool.

**Figure 11** Daily Graph: DS0s and PPP Sessions in Use

**'Daily' Graph (5 Minute Average)**

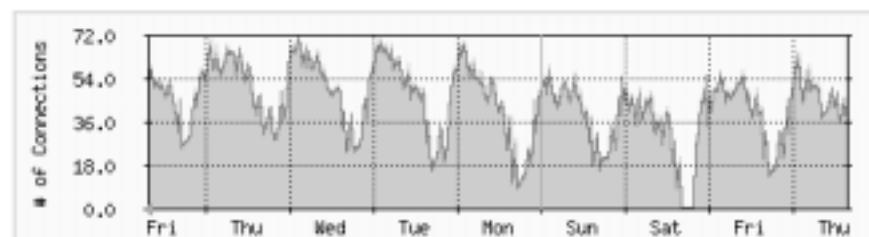


Max DS0s 84.0 B/s (42.0%)      Average DS0s 52.0 B/s (26.0%)      Current DS0s 59.0 B/s (29.5%)  
 Max PPP Sessions 80.0 B/s (40.0%)      Average PPP Sessions 51.0 B/s (25.5%)      Current PPP Sessions 58.0 B/s (29.0%)

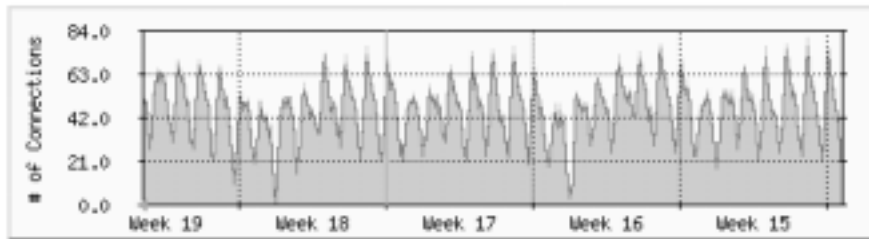
The jagged saw-tooth pattern at the top of the graph indicates a telephone-switch hunt group for the dial lines passing by the access servers. A “jump up” occurs each time the hunt group passes by a different T1 line. For a hunt group that rotates in a round-robin fashion, a jagged saw-tooth pattern is normal.

**Figure 12** Weekly Graph: DS0s and PPP Sessions in Use

**'Weekly' Graph (30 Minute Average)**

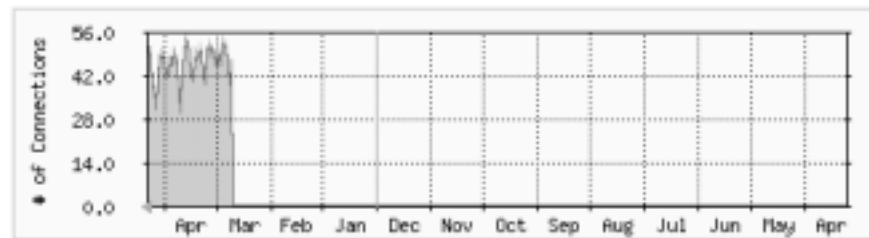


Max DS0s 72.0 B/s (36.0%)      Average DS0s 45.0 B/s (22.5%)      Current DS0s 53.0 B/s (26.5%)  
 Max PPP Sessions 70.0 B/s (35.0%)      Average PPP Sessions 44.0 B/s (22.0%)      Current PPP Sessions 51.0 B/s (25.5%)

**Figure 13 Monthly Graph: DS0s and PPP Sessions in Use****'Monthly' Graph (2 Hour Average)**

Max DS0s 81.0 B/s (40.5%)      Average DS0s 47.0 B/s (23.5%)      Current DS0s 53.0 B/s (26.5%)  
 Max PPP Sessions 76.0 B/s (38.0%)      Average PPP Sessions 45.0 B/s (22.5%)      Current PPP Sessions 51.0 B/s (25.5%)

MRTG efficiently compresses and archives data to create graphs. For example, you can keep information for an entire year on a server without using much disk space.

**Figure 14 Yearly Graph: DS0s and PPP Sessions in Use****'Yearly' Graph (1 Day Average)**

Max DS0s 56.0 B/s (28.0%)      Average DS0s 48.0 B/s (24.0%)      Current DS0s 53.0 B/s (26.5%)  
 Max PPP Sessions 54.0 B/s (27.0%)      Average PPP Sessions 46.0 B/s (23.0%)      Current PPP Sessions 52.0 B/s (26.0%)

The configuration file used to create these graphs is posted at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/mrtg53.txt>

Note the numeric OIDs in the configuration file.

## Creating and Editing a Configuration File

Because dial interfaces normally go up and down as calls connect and disconnect, monitor counters such as:

- PPP sessions in use
- DS0s in use
- Modem calls that have been rejected

Depending on how the dial interfaces are used on a access server, different types of counters may not be valuable to monitor, such as byte-packet counters on the interfaces in Table 17.

**Table 17** *Dial Interface Types on a Cisco AS5800*

Interface Type	Syntax Example
Asynchronous	Async1/2/00
B-channel serial	Serial1/0/0:1
D-channel serial	Serial1/0/0:23
Group asynchronous	Group-Async0
T1/E1 controllers	T1 1/0/0

To enable MRTG to locate a device and poll it for network statistics, follow these steps:

- 
- Step 1** Collect the hostnames, IP address, and read only (RO) SNMP community strings for the devices to be monitored.
- Step 2** Download, compile, and install MRTG on to a Solaris workstation:
- For the source code, go to <http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/pub/>
  - For the documentation, see the section “Getting and Installing MRTG on a UNIX System” at <http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html>
- Step 3** Create a configuration file.

There are two basic ways to create the file:

- Manually create it by using the MRTG files `config.text` and `sample-mrtg.config`. These files are in the `/mrtg/doc` directory.
- or
- Use the configuration maker (`cfgmaker`) in the `/mrtg/run` directory. MRTG creates a basic configuration file for you. The default configuration file made with `cfgmaker` automatically polls for a standard set of MIBs and pre-defined values.

Generic command syntax:

```
./cfgmaker communitystring@hostname-or-ipaddress >> outputfilename.cfg
```

```
./cfgmaker 5urf5h0p@travis-nas-01 >> travis-nas-01.cfg
```

`5urf5h0p` is the SNMP community string.

`travis-nas-01` is the hostname of the managed device.

`travis-nas-01.cfg` is the configuration file that MRTG reads each time it starts up.



**Note** If the domain name server (DNS) is not working, MRTG cannot use a hostname. You must use an IP address instead.

The following definitions are used in the example:

- The RO community string is 5urf5h0p
- The work directory is WorkDir: /export/home/www/mrtg/travis-nas-01/dial
- The device name is travis-nas-01

An electronic copy of this template is available at  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/dialmrtg.txt>

```

WorkDir: /export/home/www/mrtg/travis-nas-01/dial
# set defaults
Options[_]: growright
# make legends reflect these are call counters
YLegend[_]: Active Calls
ShortLegend[_]: calls
LegendI[_]: &nbsp;   calls:
LegendO[_]: &nbsp;   calls:

#####
#-----
# purpose: DS0s and PPP Sessions.
#-----
-----
Target[travis-nas-01_DS0PPP]:
1.3.6.1.4.1.9.10.19.1.1.4.0&1.3.6.1.4.1.9.10.19.1.1.5.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_DS0PPP]: 200
MaxBytes2[travis-nas-01_DS0PPP]: 200
Title[travis-nas-01_DS0PPP]: DS0s and PPP sessions in Use
PageTop[travis-nas-01_DS0PPP]: <H2>DS0s and PPP sessions in Use</H2>
<TABLE>
  <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>
  <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
</TABLE>
Options[travis-nas-01_DS0PPP]: gauge

```

```

#-----
# purpose: DS0s and Analog
#-----
Target[travis-nas-01_DS0ANALOG]:
1.3.6.1.4.1.9.10.19.1.1.4.0&1.3.6.1.4.1.9.10.19.1.1.2.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_DS0ANALOG]: 200
MaxBytes2[travis-nas-01_DS0ANALOG]: 200
Title[travis-nas-01_DS0ANALOG]: DS0s and Analog in Use
PageTop[travis-nas-01_DS0ANALOG]: <H2>DS0s and Analog in Use</H2>
<TABLE>
  <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>
  <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
</TABLE>
Options[travis-nas-01_DS0ANALOG]: gauge

#-----
#-----
# purpose: DS0s and SerialX:Y
#-----
#-----
Target[travis-nas-01_DS0SERIAL]:
1.3.6.1.4.1.9.10.19.1.1.4.0&1.3.6.1.4.1.9.10.19.1.1.3.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_DS0SERIAL]: 200
MaxBytes2[travis-nas-01_DS0SERIAL]: 200
Title[travis-nas-01_DS0SERIAL]: DS0s and SerialX:Y in Use
PageTop[travis-nas-01_DS0SERIAL]: <H2>DS0s and SerialX:Y in Use</H2>
<TABLE>
  <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>
  <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
</TABLE>
Options[travis-nas-01_DS0SERIAL]: gauge

#-----
#-----
# purpose: DS0s and Sw56
#-----
#-----
Target[travis-nas-01_DS0Sw56]:
1.3.6.1.4.1.9.10.19.1.1.4.0&1.3.6.1.4.1.9.10.19.1.1.10.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_DS0Sw56]: 200
MaxBytes2[travis-nas-01_DS0Sw56]: 200
Title[travis-nas-01_DS0Sw56]: DS0s and Sw56 in Use
PageTop[travis-nas-01_DS0Sw56]: <H2>DS0s and Sw56 in Use</H2>
<TABLE>
  <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>
  <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
</TABLE>
Options[travis-nas-01_DS0Sw56]: gauge

#-----
#-----
# purpose: cpmISDNCallsRejected and cpmModemCallsRejected
#-----
#-----
Target[travis-nas-01_callrejects]:
1.3.6.1.4.1.9.10.19.1.2.1.0&1.3.6.1.4.1.9.10.19.1.2.2.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_callrejects]: 200
MaxBytes2[travis-nas-01_callrejects]: 200
Title[travis-nas-01_callrejects]: travis-nas-01 cpmISDNCallsRejected and
cpmModemCallsRejected
PageTop[travis-nas-01_callrejects]: <H2>cpmISDNCallsRejected and
cpmModemCallsRejected</H2>
<TABLE>
  <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>

```

```

        <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
    </TABLE>

#-----
#
# purpose: cpmISDNCallsClearedAbnormally and cpmModemCallsClearedAbnormally
#-----
#
#-----
Target[travis-nas-01_clearAbnormal]:
1.3.6.1.4.1.9.10.19.1.2.3.0&1.3.6.1.4.1.9.10.19.1.2.4.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_clearAbnormal]: 200
MaxBytes2[travis-nas-01_clearAbnormal]: 200
Title[travis-nas-01_clearAbnormal]: travis-nas-01 cpmISDNCallsClearedAbnormally and
cpmModemCallsClearedAbnormally
PageTop[travis-nas-01_clearAbnormal]: <H2>cpmISDNCallsClearedAbnormally and
cpmModemCallsClearedAbnormally</H2>
<TABLE>
    <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>
    <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
</TABLE>

#-----
#
# purpose: cpmISDNNoResource and cpmModemNoResource
#-----
#
#-----
Target[travis-nas-01_callNoResource]:
1.3.6.1.4.1.9.10.19.1.2.5.0&1.3.6.1.4.1.9.10.19.1.2.6.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_callNoResource]: 200
MaxBytes2[travis-nas-01_callNoResource]: 200
Title[travis-nas-01_callNoResource]: travis-nas-01 cpmISDNNoResource and
cpmModemNoResource
PageTop[travis-nas-01_callNoResource]: <H2>cpmISDNNoResource and cpmModemNoResource</H2>
<TABLE>
    <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>
    <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
</TABLE>

#-----
#
# purpose: cmSystemModemsInUse and cmSystemModemsAvailable
#-----
#
#-----
Target[travis-nas-01_modemcount]:
1.3.6.1.4.1.9.9.47.1.1.6.0&1.3.6.1.4.1.9.9.47.1.1.7.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_modemcount]: 200
MaxBytes2[travis-nas-01_modemcount]: 200
Title[travis-nas-01_modemcount]: cmSystemModemsInUse and cmSystemModemsAvailable
PageTop[travis-nas-01_modemcount]: <H2>cmSystemModemsInUse and
cmSystemModemsAvailable</H2>
<TABLE>
    <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>
    <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
</TABLE>
Options[travis-nas-01_modemcount]: gauge

#-----
#
# purpose: cvpdpnTunnelTotal and cvpdpnDeniedUsersTotal
#-----
#
#-----
Target[travis-nas-01_vpdn_tunnelanddenied]:
1.3.6.1.4.1.9.10.24.1.1.1.0&1.3.6.1.4.1.9.10.24.1.1.3.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_vpdn_tunnelanddenied]: 200

```

```

MaxBytes2[travis-nas-01_vpdn_tunnelanddenied]: 200
Title[travis-nas-01_vpdn_tunnelanddenied]: cvpdnTunnelTotal and cvpdnDeniedUsersTotal
PageTop[travis-nas-01_vpdn_tunnelanddenied]: <H2>cvpdnTunnelTotal and
cvpdnDeniedUsersTotal</H2>
<TABLE>
  <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>
  <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
</TABLE>
Options[travis-nas-01_vpdn_tunnelanddenied]: gauge

#-----
#
# purpose: activeDS0s and cvpdnSessionTotal
#-----
#
#-----
Target[travis-nas-01_activeDS0vpdnSession]:
1.3.6.1.4.1.9.10.19.1.1.4.0&1.3.6.1.4.1.9.10.24.1.1.2.0:5urf5h0p@travis-nas-01
MaxBytes1[travis-nas-01_activeDS0vpdnSession]: 200
MaxBytes2[travis-nas-01_activeDS0vpdnSession]: 200
Title[travis-nas-01_activeDS0vpdnSession]: activeDS0s and cvpdnSessionTotal
PageTop[travis-nas-01_activeDS0vpdnSession]: <H2>activeDS0s and cvpdnSessionTotal</H2>
<TABLE>
  <TR><TD>Device:</TD><TD>travis-nas-01</TD></TR>
  <TR><TD><a href="/mrtg/mrtg.html">HOME</a></TD></TR>
</TABLE>
Options[travis-nas-01_activeDS0vpdnSession]: gauge

```

- Step 5** Open the crontab file in your system by entering **crontab -e**. The **-e** enables edit mode. You can run crontab from any directory.

```

igloo:/ ->crontab -e
"/tmp/crontabmMaqZd" 14 lines, 610 characters
#ident  "@(#)root      1.19    98/07/06 SMI"    /* SVr4.0 1.1.3.1    */
#
# The root crontab should be used to perform accounting data collection.
#
# The rtc command is run to adjust the real time clock if and when
# daylight savings time changes.
#
10 3 * * 0,4 /etc/cron.d/logchecker
10 3 * * 0   /usr/lib/newsyslog
15 3 * * 0   /usr/lib/fs/nfs/nfsfind
1 2 * * * [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
30 3 * * * [ -x /usr/lib/gss/gsscred_clean ] && /usr/lib/gss/gsscred_clean

```

**Caution**

Although the crontab file is a flat text file, do not manually edit it by using **vi crontab**. **vi** can corrupt the crontab, which causes all cron jobs to stop working. You must use the **crontab -e** command, which synchronizes and updates all the crontab daemons accordingly.

- Step 6** Insert the directory path for the MRTG configuration file (.cfg) you created. At the bottom of the file, enter a line similar to this one:

```

0,5,10,15,20,25,30,35,40,45,50,55 * * * * /opt/mrtg/run/mrtg
/opt/mrtg/run/conf/travis-nas-01.cfg

```

**Note**

Do not forget to include a space between **/mrtg** and **/opt**

```

/tmp/crontabmMaqZd" 14 lines, 610 characters
#ident "@(#)root 1.19 98/07/06 SMI" /* SVr4.0 1.1.3.1 */
#
# The root crontab should be used to perform accounting data collection.
#
# The rtc command is run to adjust the real time clock if and when
# daylight savings time changes.
#
10 3 * * 0,4 /etc/cron.d/logchecker
10 3 * * 0 /usr/lib/newsyslog
15 3 * * 0 /usr/lib/fs/nfs/nfsfind
1 2 * * * [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
30 3 * * * [ -x /usr/lib/gss/gsscred_clean ] && /usr/lib/gss/gsscred_clean
0,5,10,15,20,25,30,35,40,45,50,55 * * * * /opt/downloads/mrtg/mrtg-2.8.8/run/mrtg
/opt/downloads/mrtg/mrtg-2.8.8/run/travis-nas-01.cfg

```

On a 5-minute time interval, MRTG will start up, read the configuration file, and re-generate performance graphs.

## Sending MRTG Graphs to a Web Server

MRTG builds all the graphs and web pages.

To browse and view the graphs produced by MRTG, make sure the web server is running. For information on how to set up a web server, go to <http://www.apache.org/>

To send MRTG graphs to a web server, follow these steps:

- Step 1** Verify that the configuration file points to the correct working directory (WorkDir:) on your web server by entering the **more** command. See WorkDir: in the following example.

```

igloo:/opt/downloads/mrtg/mrtg-2.8.8/run ->more travis-nas-01.cfg
WorkDir: /export/home/www/mrtg/travis-nas-01/dial
# set defaults
Options[_]: growright
# make legends reflect these are call counters
YLegend[_]: Active Calls
ShortLegend[_]: calls
LegendI[_]: &nbsp;  calls:
LegendO[_]: &nbsp;  calls:
.
.
.

```

- Step 2** To send the web pages and graphs to the web-server directory, enter the following command:

```

igloo:/opt/downloads/mrtg/mrtg-2.8.8/run ->./mrtg travis-nas-01.cfg
igloo:/opt/downloads/mrtg/mrtg-2.8.8/run ->

```

Now, the crontab will automatically perform this function every five minutes.

Ignore any Rateup WARNING errors, which means that crontab is working in the background.

```

Rateup WARNING: ../rateup The backup log file for 172.21.101.20.178 was invalidl
Rateup WARNING: ../rateup Can't remove 172.21.101.20.178.old updating log file
Rateup WARNING: ../rateup Can't rename 172.21.101.20.178.log to 172.21.101.20.1e
Rateup WARNING: ../rateup could not read the primary log file for 172.21.101.209

```

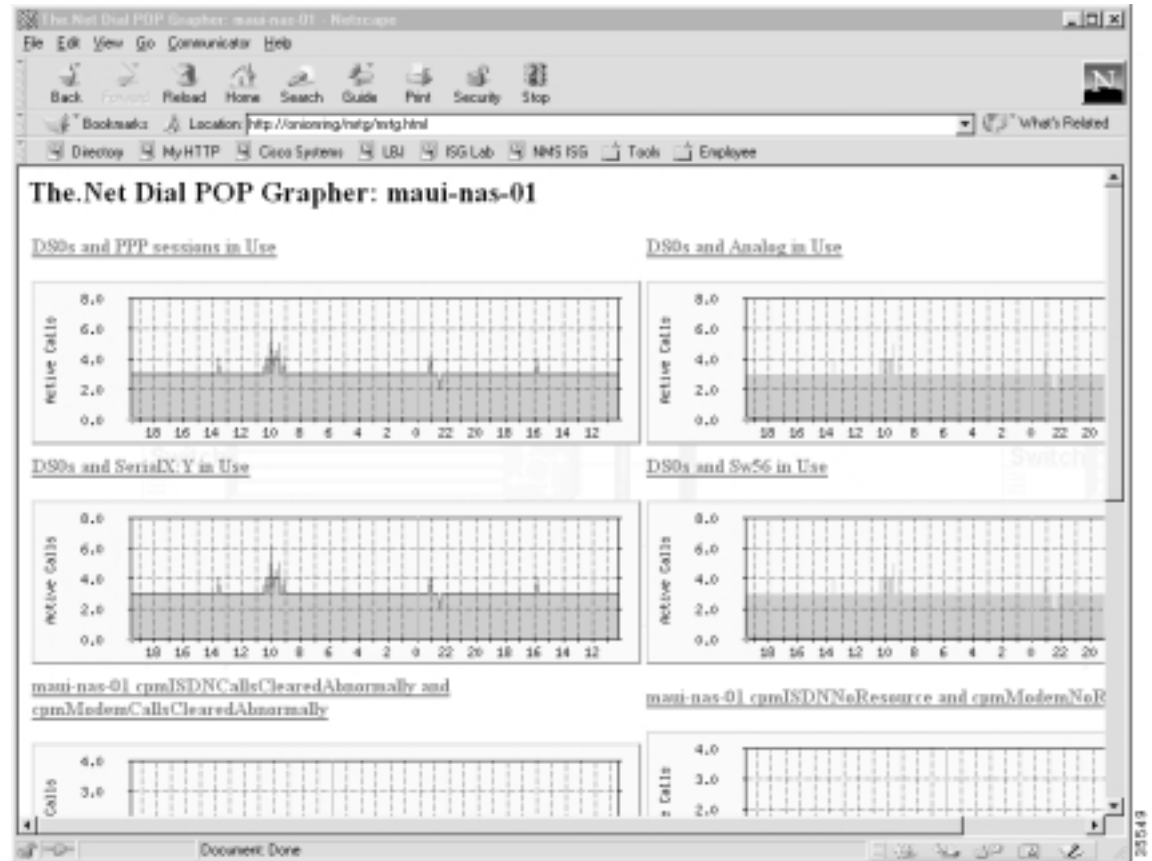


**Step 3** Use a web browser to view the MRTG output files in the web page directory.



**Note** If the domain name server (DNS) is not working, a hostname cannot be used by MRTG. Use the IP address instead.

**Figure 15** MRTG Graphs Viewed by Using a Web Browser







## Task 4—Using Syslog, NTP, and Modem Call Records to Isolate and Troubleshoot Faults

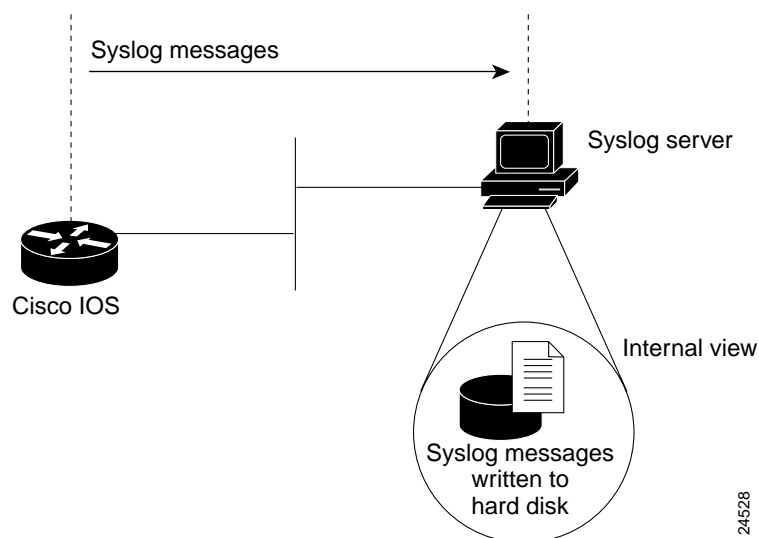
### About Syslog

Syslog, Network Time Protocol (NTP), and modem call records work together to isolate and troubleshoot faults in a dial access network.

Syslog enables you to:

- Centrally log and analyze configuration events and system error messages, such as router configuration changes, interface up and down status, modem events, security alerts, environmental conditions, trace backs, and CPU process overloads.
- Capture client debug output sessions in a real-time scenario.
- Reserve telnet sessions for making configurations changes and using **show** commands. Telnet sessions that are cluttered with debug output interfere with troubleshooting procedures.
- Reduce network downtime by knowing when the network has quality problems.

**Figure 16** Cisco IOS Sending Syslog Messages to a Syslog Server



You can enable syslog in any Cisco IOS device and send syslog messages to many different destinations (host, buffer, console, history, and monitor).

By using the **logging ?** command, you can see the log settings for distinct destinations:

```
travis-nas-01(config)#logging ?
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  console              Set console logging level
  facility              Facility parameter for syslog messages
  history              Configure syslog history table
  monitor              Set terminal line (monitor) logging level
  on                   Enable logging to all supported destinations
  rate-limit           Set messages per second limit
  source-interface     Specify interface for source address in logging
                      transactions
  trap                 Set syslog server logging level
```

There are eight levels of syslog information in the Cisco IOS software. Monitor and manage logs according to the severity level of the syslog message. By using the **logging trap ?** command, you can see the logging severity levels:

```
travis-nas-01(config)#logging trap ?
<0-7>             Logging severity level
alerts             Immediate action needed          (severity=1)
critical           Critical conditions                (severity=2)
debugging          Debugging messages                (severity=7)
emergencies        System is unusable                (severity=0)
errors             Error conditions                  (severity=3)
informational       Informational messages            (severity=6)
notifications      Normal but significant conditions (severity=5)
warnings           Warning conditions                 (severity=4)
<cr>
```

**Table 18** Logging Trap Severity Definitions

Message Type	Description	Syslog Message	Severity Level
emergencies	System unusable	LOG_EMERG	0
alerts	Immediate action needed	LOG_ALERT	1
critical	Critical conditions	LOG_CRIT	2
errors	Error conditions	LOG_ERR	3
warnings	Warning conditions	LOG_WARNING	4
notifications	Normal but significant condition	LOG_NOTICE	5
informational	Informational messages only	LOG_INFO	6
debugging	Debugging messages	LOG_DEBUG	7

In this case study, syslog is enabled on all Cisco access servers and backbone routers. Each device sends syslog messages to the same log file on the same syslog server.

The terminology in the syslog messages can vary between different versions of Cisco IOS software. To effectively manage syslog messages, ensure that wherever possible, the same version of Cisco IOS software is running on all routers.



**Note**

For background information on syslog, go to <http://www.cert.org/security-improvement/practices/p041.html>

## About NTP

The Network Time Protocol (NTP):

- Provides a synchronized time base for networked routers, servers, and other devices.
- Coordinates the time of network events, which helps you understand and troubleshoot the time sequence of network events. For example, call records for specific users can be correlated within one millisecond.
- Enables you to compare time logs from different networks, which is essential for:
  - Tracking security incidents
  - Analyzing faults
  - Troubleshooting

Without precise time synchronization between all the various logging, debug output, management, and AAA functions in the network, you cannot make time comparisons.

For a list of NTP clients, go to <http://www.eecis.udel.edu/~ntp/software.html>

## About Modem Call Records

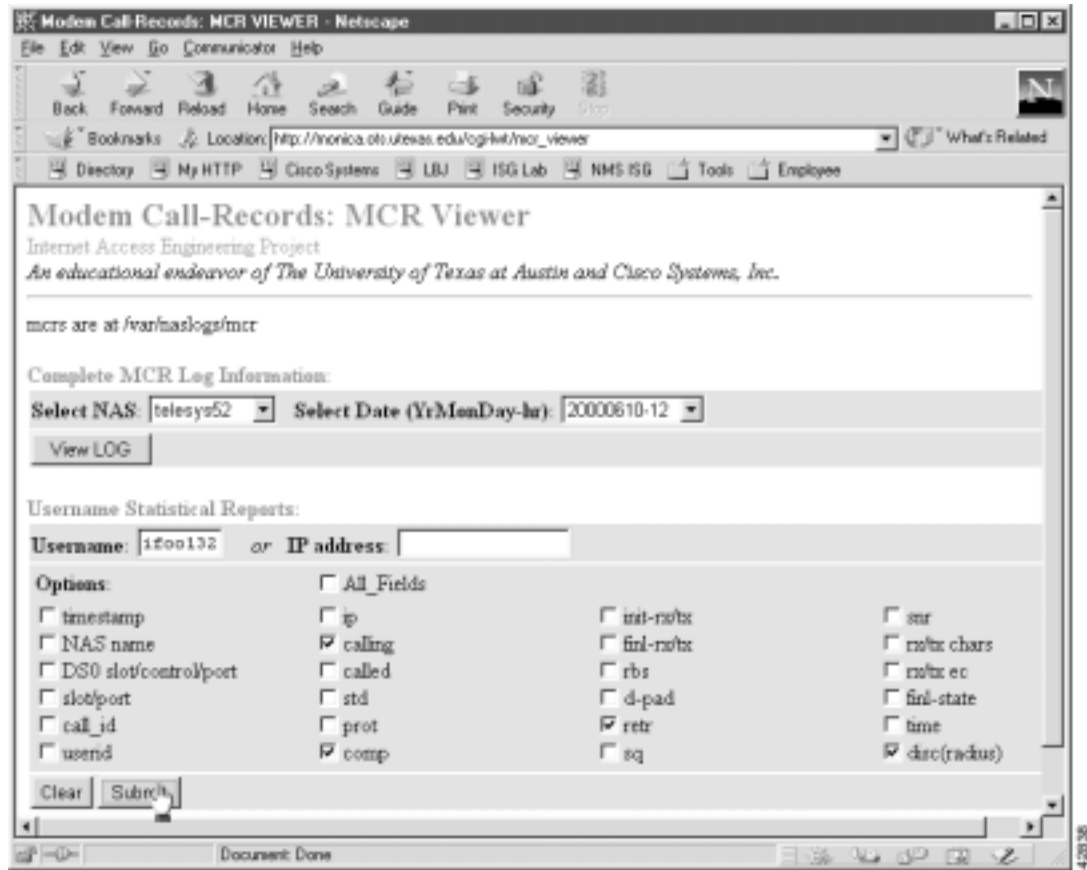
A modem call record (MCR) is a type of syslog message that is:

- Created when a user dials in and hangs up, but it is not generated until the end of the call.
- Used to gather statistics and modem-performance logs on a per-call basis, such as:
  - Modulation trends (V.90 versus V.34).
  - Call time durations (consistent short connection times on a modem, regular Lost Carrier counts).
  - Unavailable user IDs.
  - PPP negotiation or authentication failures.

In this case study, the engineers filter modem call records out of syslog and store them into flat files on a Unix host. The records are sorted by using cron jobs and perl scripts. A web-based MCR viewer facility is used to:

- Search the call records.
- Extract historical and statistical information about individual users and access servers.

Figure 17 Web-Based MCR Viewer



You can view entire log files or portions of logs in the MCR viewer. In addition, you can parse for specific users and other call attributes for a modem call (for example, modulation, error correction, compression, disconnect causes, and retrains).



**Note** Modem call records are available in syslog starting with Cisco IOS Releases 11.3AA and 12.0T.

## Enabling NTP on a Cisco IOS Device

To enable NTP and related clocking services, follow these steps.

- Step 1** From the Cisco IOS device, enter the following commands. Enable debug timestamps and include the date, time, and milliseconds relative to the local time zone:

```
!
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
```

- Step 2** Identify the local timezone and enable recurring time adjustments for daylight savings time by entering the following commands:

```
!
clock timezone CST -6
clock summer-time CST recurring
!
```

- Step 3** Locate an NTP server that can be reached by the Cisco IOS device.

- Step 4** Specify the IP address for the NTP server and enable automatic-calendar updates by entering the following commands:

```
!
ntp update-calendar
ntp server 172.22.255.1
!
```



**Note** By default, the **ntp clock-period** command is enabled in some Cisco IOS releases. The Cisco IOS software appends an arbitrary number to the end of the command.

- Step 5** Verify that the clock is synchronized with the NTP server by entering the following command:

```
travis-nas-01>show ntp status
Clock is synchronized, stratum 9, reference is 172.22.255.1
nominal freq is 250.0000 Hz, actual freq is 249.9987 Hz, precision is 2**24
reference time is BD123336.28CCF0C4 (18:09:42.159 CST Sat Jul 8 2000)
clock offset is 0.1183 msec, root delay is 61.84 msec
root dispersion is 0.93 msec, peer dispersion is 0.79 msec
travis-nas-01>
```

Inspect the status and time association. Clock sources are identified by their stratum levels. The previous display shows a stratum level nine clock.



**Note** If the NTP synchronization does not take place, reload the router.

- Step 6** Verify that the router is receiving NTP packets from the NTP server by entering the following command:

```
travis-nas-01>show ntp association

      address      ref clock      st  when  poll reach  delay  offset  disp
*~172.22.255.1    127.127.7.1      8   984  1024  377    60.3   -0.89   0.8
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
travis-nas-01>
```

The tilde (~) next to the IP address of the NTP server means the NTP service is configured. The asterisk (\*) indicates successful synchronization with the master clock.

## Setting Up an NTP Client

To set up an NTP client on a Solaris v2.6 workstation, follow these steps.



**Note** Additional software is not required to set up NTP on the workstation if it is running Solaris v2.6 (or later).

- Step 1** Locate an NTP server that can be reached by the workstation. There are many available NTP servers on the Internet. If your workstation cannot reach the Internet, locate an NTP server within your network.



**Note** A common practice is to configure an area border router as an NTP server for a particular subnet. The area border router then points to an external NTP server. Other equipment on that subnet uses the loopback 0 IP address on the area border router as an NTP server.

- Step 2** Go to the /etc/inet directory and inspect the template file called ntp.client:

```
onionring:~$ cd /etc/inet
onionring:/etc/inet$ more ntp.client
# @(#)ntp.client      1.2      96/11/06 SMI
#
# /etc/inet/ntp.client
#
# An example file that could be copied over to /etc/inet/ntp.conf; it
# provides a configuration for a host that passively waits for a server
# to provide NTP packets on the ntp multicast net.
#

multicastclient 224.0.1.1
```

- Step 3** Copy ntp.client and create the ntp.conf configuration file in the /etc/inet default directory:

```
onionring:/etc/inet$ cp ntp.client ntp.conf
onionring:/etc/inet$
```

The NTP daemon reads ntp.conf at startup to locate the NTP server.



**Note** You must have root-level permissions to edit or copy any files in the /etc/inet/ directory.



- Step 4** Edit the `ntp.conf` file by changing *multicastclient* to **server** followed by the IP address of the target NTP server:

```
# @(#)ntp.client      1.2      96/11/06 SMI
#
# /etc/inet/ntp.client
#
# An example file that could be copied over to /etc/inet/ntp.conf; it
# provides a configuration for a host that passively waits for a server
# to provide NTP packets on the ntp multicast net.
#

server 172.22.255.1
```

- Step 5** Go to the directory `/usr/lib/inet/` and start the NTP daemon by entering the **xntpd** command. The daemon sets and maintains the time-of-day of the operating system in agreement with the master time server.

```
onionring:/etc/inet$ cd /usr/lib/inet/
onionring:/usr/lib/inet$ ls
in.dhcpd  xntpd
onionring:/usr/lib/inet$ xntpd
onionring:/usr/lib/inet$
```

- Step 6** Verify that the NTP daemon is running by entering the **ntpq -p** command:

```
onionring:/usr/lib/inet$ ntpq -p
      remote           refid      st t when poll reach  delay  offset   disp
=====
*maui-rtr-01.mau CHU(1)         8 u  49   64  377    1.08  -0.131   0.08
onionring:/usr/lib/inet$
```

The following information appears:

- The remote NTP server to which the workstation is connected.
- The reference ID.
- The stratum level of the server.
- The type of NTP packet that was received by the client (local, unicast, multicast, or broadcast).
- The polling interval in seconds.
- The reachability register in octal.
- The current delay of the server in seconds.
- The current offset of the server in seconds and the dispersion of the server in seconds.
- The delay, offset, and displacement between the client and the server in seconds.

When the daemon starts, most of the time values will be zeros until there is a sufficient number of queries taken by the daemon to determine the correct offset.

## Troubleshooting the NTP Client

**Table 19** NTP Problems and Solutions

Problem	Solution
The ntp.client file or the xntpd daemon cannot be found in the directories shown in the examples.	<p>Verify that the workstation is running Solaris v2.6 or a later version of Solaris. Enter the <b>uname -a</b> command to see the version.</p> <p>Versions earlier than Solaris v2.6 do not support NTP and must be supplemented with additional NTP software available from <a href="http://www.sunfreeware.com/">http://www.sunfreeware.com/</a></p>
The error message “No Associations IDs Returned” when you enter the <b>ntpq -p</b> command.	<p>There are three possible solutions:</p> <ul style="list-style-type: none"> <li>• The network traffic is slow, and the workstation has not had time to poll the NTP server. Allow the workstation enough time to issue the poll (a few seconds); then, enter the <b>ntpq -p</b> command.</li> <li>• The multicastclient line in the ntp.conf file was not replaced with the server line.</li> <li>• The NTP server you have chosen is down, or it is not configured correctly.</li> </ul>

## Enabling Syslog and Modem Call Records in the Cisco IOS Software

To enable syslog messages in the Cisco IOS software and send them to a syslog server, follow these steps:

**Step 1** Inspect the current logging status by entering the following command:

```
travis-nas-01#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 42 messages logged
  Monitor logging: level debugging, 93 messages logged
  Buffer logging: level debugging, 3 messages logged
  Trap logging: level informational, 121 message lines logged


Log Buffer (8192 bytes):
travis-nas-01#
```

**Step 2** Set up a basic syslog configuration by entering the following commands. See Table 20 for command descriptions.

```
!
logging buffered 10000 debugging
no logging console guaranteed
logging console informational
!

!
logging trap debugging
logging facility local0
logging 172.21.100.100
!
```

**Table 20** Logging Command Descriptions

Command	Purpose
<code>logging buffered 10000 debugging</code>	<p>Sets the internal log buffer to 10000 bytes for debug output. New messages overwrite old messages.</p> <p>You can tune buffered-logging parameters for collecting logs on a NAS when you are at a remote location. For example, turn on debugs and start logging them in the history buffer. Make your test call; then, re-connect in shell mode and inspect the debugs.</p>
<code>logging console informational</code> <code>no logging console guaranteed</code>	<p>Sends the most urgent informational logs to the console port in the event the IP network or syslog server fails. Alternatively, send messages to the console by using the commands <b>logging console errors</b> or <b>logging console warnings</b>.</p> <div style="display: flex; align-items: center; justify-content: center;">  <div style="margin-left: 10px;"> <p><b>Caution</b></p> <p>Logging console can cause the router to intermittently freeze up as soon as the console port overloads with log messages. Debugs and modem call records sent to the console port are potentially destructive to the Cisco IOS software.</p> </div> </div>
<code>logging trap debugging</code>	Enables logging up to the debug level (all eight levels).
<code>logging 172.21.100.100</code>	Specifies the IP address of the syslog server.
<code>logging facility local0</code>	<p>Assigns a logging-facility tag (local0) to the syslog messages for this device. The tag must match the facility number configured in the syslog.conf file on the Unix host. See Step 1 in “Configuring the Syslog Daemon” section on page 76.</p> <p>In this case study, each device sends syslog messages to the same log file on the same syslog server.</p>

**Step 3** Enable modem call records in the Cisco IOS by entering the following command:

```
!
modem call-record terse
!
```

A modem call record, which is a syslog message, looks like this:

```
May 26 22:04:23.346 CST: %CALLRECORD-3-MICA_TERSE_CALL_REC: DS0 slot/contr/chan=
0/0/0, slot/port=2/14, call_id=26, userid=(n/a), ip=0.0.0.0, calling=4082322078,
called=3241933, std=V.34+, prot=LAP-M, comp=V.42bis both, init-rx/tx b-rate=264
00/24000, finl-rx/tx b-rate=28800/24000, rbs=0, d-pad=None, retr=1, sq=4, snr=27
, rx/tx chars=136/6470, bad=2, rx/tx ec=134/184, bad=0, time=594, finl-state=Ste
ady, disc(radius)=(n/a)/(n/a), disc(modem)=DF03 Tx (host to line) data flushing
- OK/Requested by host/DTR dropped
```

- Step 4** (Optional) To disable syslog messages and SNMP traps when dial interfaces go up and down, use the commands **no logging event link-status** and **no snmp trap link-status**. Although up and down events are legitimate events on dial interfaces, these events should not cause alarms as LAN and WAN interfaces would.

```
!
interface Serial1/0/0:4:23
  no logging event link-status
  no snmp trap link-status
!
interface Group-Async0
  no logging event link-status
  no snmp trap link-status
!
```

In this example, only the fourth T1 of a T3 card is shown.



**Note** In some Cisco IOS images, the **logging event link-status** command is disabled by default.

## Configuring the Syslog Daemon

In this case study, all the syslog messages from the access servers are sent to a single log file. The syslog messages from the backbone routers are sent to a different log file.

To configure the syslog daemon on a Solaris syslog server, follow these steps:

- Step 1** On the syslog server, edit the file `syslog.conf` in the `/etc/` directory by using a text editor. To get syslog working, you must add the following line to the file:

```
|
local0.debug      /var/log/router.log
|
```

- The local facility number is `local0.debug`. It must match the facility number configured in the Cisco IOS device. See the **logging facility** command in Table 20.
- The log file path name is `/var/log/router.log`
- One tab exists between the facility number and the path name. Spaces are not permitted. You can define any directory location/path for the `.txt` log file.

In the following example, the new line is in **bold**:

```
"syslog.conf" 53 lines, 1861 characters
#ident  "@(#)syslog.conf      1.3      93/12/09 SMI"      /* SunOS 5.0 */
#
# Copyright (c) 1991-1993, by Sun Microsystems, Inc.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words. Also, within ifdef's, arguments
# containing commas must be quoted.
#
#
#
```

```
#Following is the new line. It adds a logging facility number and direcorey path for the
#log file (router.log).
local0.debug    /var/log/router.log
```



**Note** The previous syslog.conf example has been abbreviated to fit this document. The actual file size is much larger than the example. Add the new line to the end of the file.

**Step 2** Create the log file and check the read/write privileges by entering the following commands:

```
aurora:/etc ->touch /var/log/router.log
aurora:/etc ->ls -l /var/log/router.log
-rw-r--r--  1 root    other      27110 Jul  8 19:56 /var/log/router.log
aurora:/etc ->
```

**Step 3** Verify the syslog daemon is running by entering the **ps -elf | grep syslog** command from the /etc directory. If the daemon is running, a process ID is returned by the system (for example, 169). If the daemon is not running, no ID is returned.

```
aurora:/etc ->ps -elf | grep syslog
 8 S      root   169      1  0  41 20 60756cc8      187 604e3156   Jun 19 ?          d
aurora:/etc ->
```

**Step 4** Activate the configuration changes you made in syslog.conf by restarting the syslog daemon. Enter the start/stop S74syslog scripts from the /etc/rc2.d directory.

```
aurora:/etc ->rc2.d/S74syslog stop
Stopping the syslog service.
aurora:/etc ->rc2.d/S74syslog start
syslog service starting.
aurora:/etc ->ps -elf | grep syslog
 8 S      root  4405      1  0  44 20 6042d320      187 604e3156 09:16:35 ?          d
aurora:/etc ->
```

Confirm that a new syslog process ID was assigned (for example, 4405) after the start/stop process.



**Note** You must have root-level permissions to run system scripts, such as the files in /etc/rc2.d

## Inspecting Syslog Messages in the Log File

To inspect syslog messages by using Cisco IOS commands, Unix commands, FTP, and a web browser, follow these steps:

- Step 1** From the Cisco IOS device, create basic syslog messages by entering these commands:

```
travis-nas-01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
travis-nas-01(config)#^Z
travis-nas-01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
travis-nas-01(config)#^Z
travis-nas-01#
```

- Step 2** From the syslog server, verify that the syslog messages went in to the log file. Enter the **tail -f** command to monitor the last 10 lines of an active log file. To exit tail -f mode, press **Ctrl-C**.

```
aurora:/etc ->tail -f /var/log/router.log
May 26 17:43:12 [172.21.101.20.6.122] 629: May 26 20:35:23.551 CST: %SYS-5-CONFIG_I:
Configured from console by vty0 (172.22.61.200)
May 26 17:51:15 [172.21.101.20.6.122] 630: May 26 20:43:27.068 CST: %SYS-5-CONFIG_I:
Configured from console by console
May 26 17:51:19 [172.21.101.20.6.122] 631: May 26 20:43:30.932 CST: %SYS-5-CONFIG_I:
Configured from console by console
May 26 17:54:38 [172.21.101.20.6.122] 632: May 26 20:46:50.344 CST: %SYS-5-CONFIG_I:
Configured from console by vty0 (172.22.61.200)
^C
aurora:/etc ->
```

- Step 3** View the syslog messages in a web browser. Notice the wide horizontal scroll bar, which is helpful for viewing debug messages and modem call records.

**Figure 18** Syslog Messages that Appear by Using FTP and a Web Browser

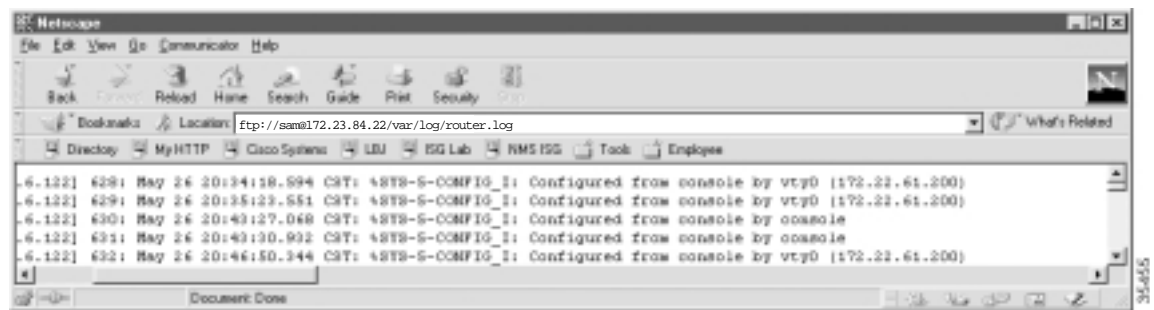


Table 21 shows the generic URL syntax to use. Be sure to replace the variables with your own information. The FTP server automatically prompts you for a login password.

**Table 21** URL Syntax Descriptions and Examples

Generic URL Syntax	Description	Example
<code>ftp://username@host/directory-path</code>	Uses FTP to view logs from a remote location.	<code>ftp://sam@172.23.84.22/var/log/router.log</code>
<code>file://directory-path</code>	Views logs on a local host.	<code>file://var/log/router.log</code>







## Task 5—Setting Up a Web Portal for the Dial NMS

### About a Web Portal

A web portal for the dial NMS is a combination of CGI scripts and HTML links used to support a dial Internet access service.

As the number of devices and applications in a network increase, the operations support team may become inundated with a myriad of management products. To support a dial service, a web portal provides easy access to:

- Product manuals, design guides, white papers, and troubleshooting guides.
- Light-weight tools and scripts.
- Network policies, procedures, and reports.
- Periodic and just-in-time reporting.
  - The help desk can access operational information (for example, current connected caller status).
  - The operations staff can report on current service levels.



#### Tips

For more information on building a management intranet, go to [http://www.cisco.com/warp/public/cc/serv/mkt/nmps/ent/tech/bmi\\_wi.htm](http://www.cisco.com/warp/public/cc/serv/mkt/nmps/ent/tech/bmi_wi.htm)

**Table 22** Utilities Provided by the Web Portal for the Dial NMS

Utility	Function
Documentation Center	A web server used as an online-documentation hub to share network operations information.
Device Linker	A web page used for bookmarking URLs for quick device telnet and out of band (console) access. See the “Building a Device Linker Web Page” section on page 83.

**Table 22** *Utilities Provided by the Web Portal for the Dial NMS (continued)*

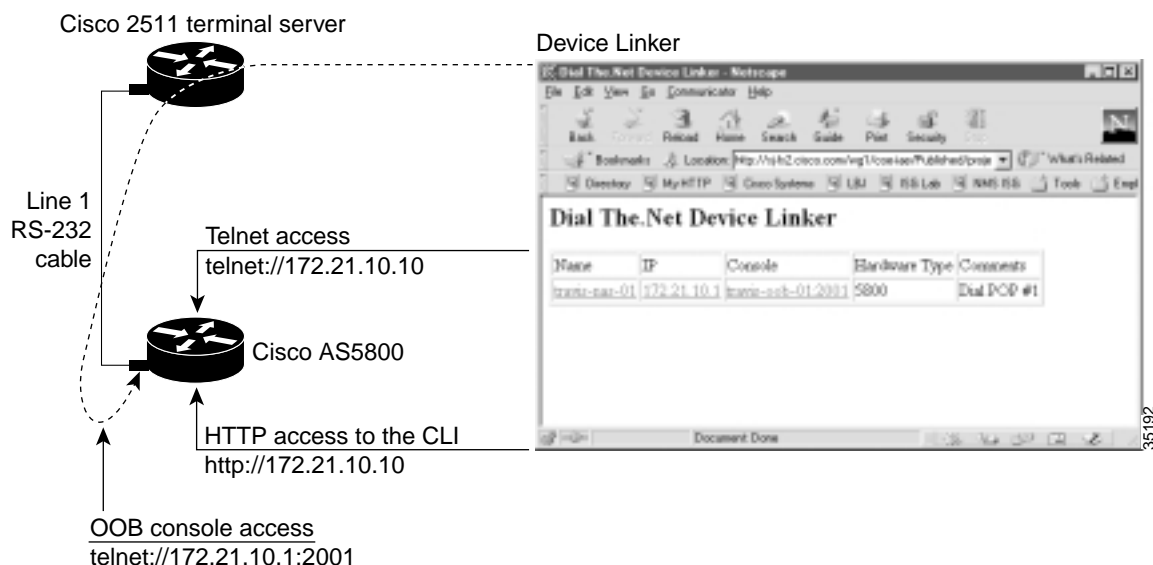
Utility	Function
Cisco IOS CLI Command Center	<p>A web page that provides HTTP access to frequently used Cisco IOS CLI commands. The operations team and help desk can use this utility to troubleshoot connectivity problems.</p> <p>See the “Using HTTP to Access CLI Commands” section on page 86.</p>
IP Tracker	<p>A web page that uses two scripts to keep track of IP address block assignments by using DNS reverse lookup zones.</p> <p>See the “Creating an IP Tracker Web Page” section on page 96.</p>
SNMP Commander	<p>A script that aids the MIB research task by enabling engineers to build web-based object identification (OIDs) bookmarks. You can poll for network statistics by using OID bookmarks and a web browser. No keyboard is required.</p> <p>See the “About SNMP Commander” section on page 49.</p>
Syslog Viewer	<p>A utility that uses FTP to access a syslog server and a web browser to view syslog messages. Migration to HTTP is straightforward after security issues are addressed. The use of non-wrapping text is useful when viewing debug messages and modem call records.</p> <p>See the “Inspecting Syslog Messages in the Log File” section on page 78.</p>
Modem Call Record Viewer	<p>Light-weight scripts used to parse and view modem call records.</p> <p>See the “About Syslog” section on page 67.</p>
CiscoWorks 2000 Resource Manager Essentials	<p>A utility used to remotely monitor and maintain devices through a web-based browser interface.</p> <p>See the “Task 8—Using CiscoWorks 2000 Resource Manager Essentials” section on page 117.</p>

## Building a Device Linker Web Page

A device linker web page:

- Simplifies access to the many device-management interfaces in the network.
- Provides links to the telnet, console, and HTTP ports of Cisco IOS devices.

**Figure 19** Device Linker Used to Access Devices



By using a Cisco terminal server for out-of-band console access, such as a Cisco 2511, the consoles are available at TCP port 20xx on a terminal server. The target line number replaces xx. For example to get to line 1, telnet to port 2001. The equivalent URL is telnet://172.21.101.250:2001

To build a device linker web page, follow these steps:

- Step 1** Collect the IP addresses for the Cisco IOS devices.
- Step 2** Collect the device console out-of-band (OOB) paths for the terminal server and the lines connected to Cisco IOS devices.
- Step 3** Create a basic HTML table and enter the information for each device. The telnet and HTTP information is in bold in the following HTML code fragment. Step 4 shows what the table looks like in a web browser.

```
<html>
<head>
<title>Dial The.Net Device Linker</title>
</head>
<body>
<h2>Dial The.Net Device Linker</h2>
<table border="1">
  <tr>
    <td>Name</td>
    <td>IP</td>
    <td>Console</td>
    <td>Hardware Type</td>
    <td>Comments</td>
  </tr>
  <tr>
    <td>Dial POP #1</td>
    <td>172.21.10.1</td>
    <td>telnet-ash-01.2001</td>
    <td>5800</td>
    <td>Dial POP #1</td>
  </tr>
</table>
```

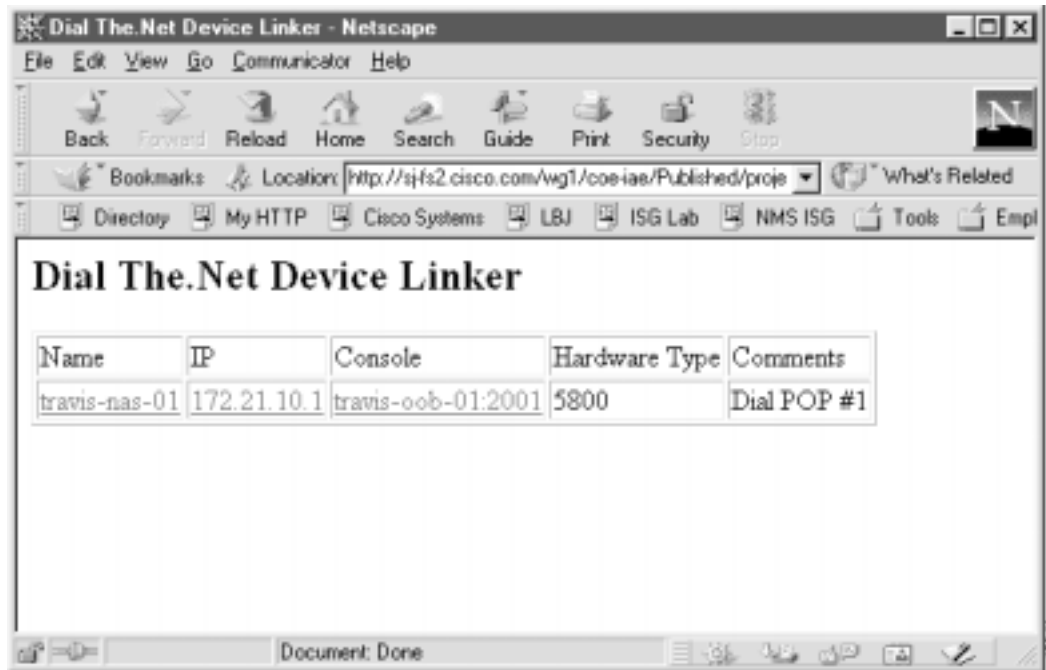
```
<td><a href="http://172.21.10.1">travis-nas-01</a></td>
<td><a href="telnet://172.21.10.1">172.21.10.1</a></td>
<td><a href="telnet://172.21.101.250:2001">travis-oob-01:2001</a></td>
<td>5800</td>
<td>Dial POP #1</td>
</tr>
</table>
</body>
</html>
```

**Table 23** Functions and Parameters for Designing a Device Linker Web Page

Function	Formula	Example
OOB console access	telnet://termserver-ip:20XX	telnet://172.21.101.250:2001
Basic IP access	telnet://ip-address	telnet://172.21.10.1
IOS HTTP access	http://ip-address	http://172.21.10.1

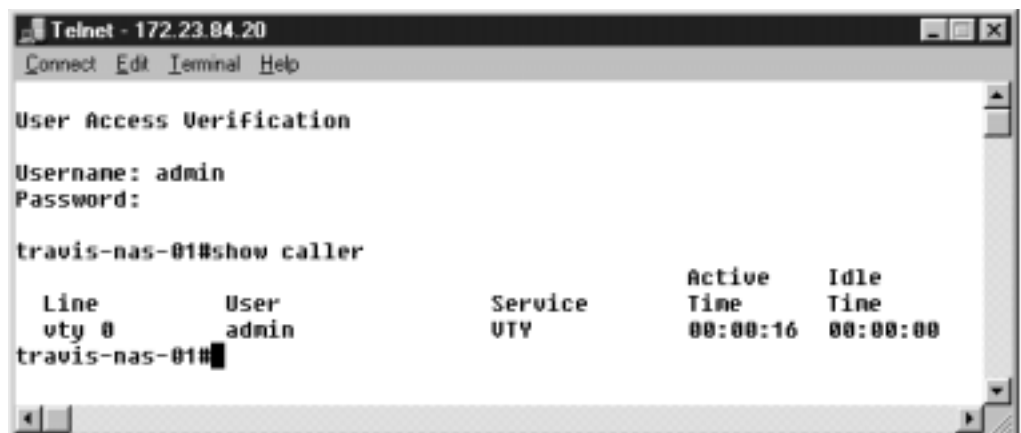
**Step 4** Post the device linker web page to a WWW server in the NOC.

**Figure 20** A Device Linker Management Page



- Step 5** Click on an active device link. After a telnet session opens, log in.

**Figure 21 Console Port Login**



## Troubleshooting a Cisco 2511 Console Connection

If you cannot access the console of a device, follow these steps:

- Step 1** Verify that the configuration on the terminal server is correct. Telnet is the only service that must be supported to access the lines. The following configuration fragment shows you how to configure 16 TTY lines on a Cisco 2511 terminal server.

```
!
line 1 16
no exec
transport input telnet
!
```

- Step 2** If the console port is blocked, you may need to telnet to the terminal server and clear the line. Enter the **show users EXEC** command followed by the **clear line type number** command.

```
c2511-oob#show users
```

Line	User	Host(s)	Idle	Location
0 con 0	admin	idle		
4 tty 4	admin	incoming		0 dhcp-172-71-218-198.guessme.com
* 10 vty 0	admin	incoming		0 dhcp-172-71-218-198.guessme.com

```
c2511-oob#clear line tty 4
[confirm]
[OK]
c2511-oob#show users
```

Line	User	Host(s)	Idle	Location
0 con 0	admin	idle		
* 10 vty 0	admin	incoming		0 dhcp-172-71-218-198.guessme.com

**Step 3** (Optional) Sometimes administrators inadvertently leave lines in use. To make idle telnet sessions end after 30 minutes, enter the **exec-timeout 30 0** command on all the lines.

```
!
line 1 16
no exec
exec-timeout 30 0
transport input telnet
!
```

# About HTTP Access to the CLI

Using web-based access to the CLI reduces the need for telnet sessions to monitor or verify network operations. Telnet sessions can be reserved for actions such as making configuration changes. Additionally, sending syslog to a syslog server prevents telnet sessions from becoming cluttered with debug output.

HTTP access to the CLI is:

- Very difficult to secure. One way of securing a router is to use access-control lists on all VTY lines. Enable only devices in the NOC to access the VTY lines.
- Not recommended for service providers. If used, you should weigh the perceived ease of use versus the additional security issues involved with HTTP access to a network device.

The Cisco IOS CLI Command Center is a web page utility that provides HTTP access to CLI commands on a router. HTTP access to the CLI simplifies the troubleshooting tasks for a help desk.

# Using HTTP to Access CLI Commands

To manage a dial Internet access service by using HTTP access to CLI commands, follow these steps:

**Step 1** Enable HTTP services on the Cisco IOS device by entering the following commands:

```
!
ip http server
ip http authentication aaa
!
```

**Table 24** Command Descriptions

Command	Purpose
ip http server	Enables the router to function as an HTTP server.
ip http authentication aaa	Uses the AAA facility as an authentication method for HTTP server users.

- Step 2** Create a table in an HTML web page and enter your list of frequently used Cisco IOS CLI commands.



**Note** To create the link for a CLI command, specify the IP address of the Cisco IOS device followed by the command. Remember to include the forward slashes (/) between each command mode and key word.

**Table 25** *Formula and Example for Linking a CLI Command*

Formula	Example
<code>http://ip-address/exec/ios-key-word/.../cr</code>	<code>http://172.23.84.20/exec/sh/caller/cr</code>

The web page can include many types of commands useful for managing a dial Internet access service, including:

- System commands (Table 26)
- Interface commands (Table 27)
- Call state commands (Table 28)
- Debug commands (Table 29)

**Table 26** *System Commands*

<b>show running configuration</b>	<b>show file systems</b>	<b>show ip route</b>
<b>show version</b>	<b>dir</b>	<b>show ip route static</b>
<b>show modem version</b>	<b>show flash</b>	<b>show ip route connected</b>

**Table 27** *Interface Commands*

<b>show controller t1</b>	<b>show ip interface brief</b>	<b>show interface Fast Ethernet0/0/0</b>
<b>show isdn service</b>	<b>show interface</b>	<b>show line</b>
<b>show isdn status</b>		

**Table 28**    *Call State Commands*

<b>show modem</b>	<b>show caller</b>	<b>show users</b>
<b>show modem call-stats</b>	<b>show caller ip</b>	<b>show dialer</b>
<b>show modem ?</b>	<b>show caller timeout</b>	<b>show dialer map</b>
	<b>show caller ?</b>	

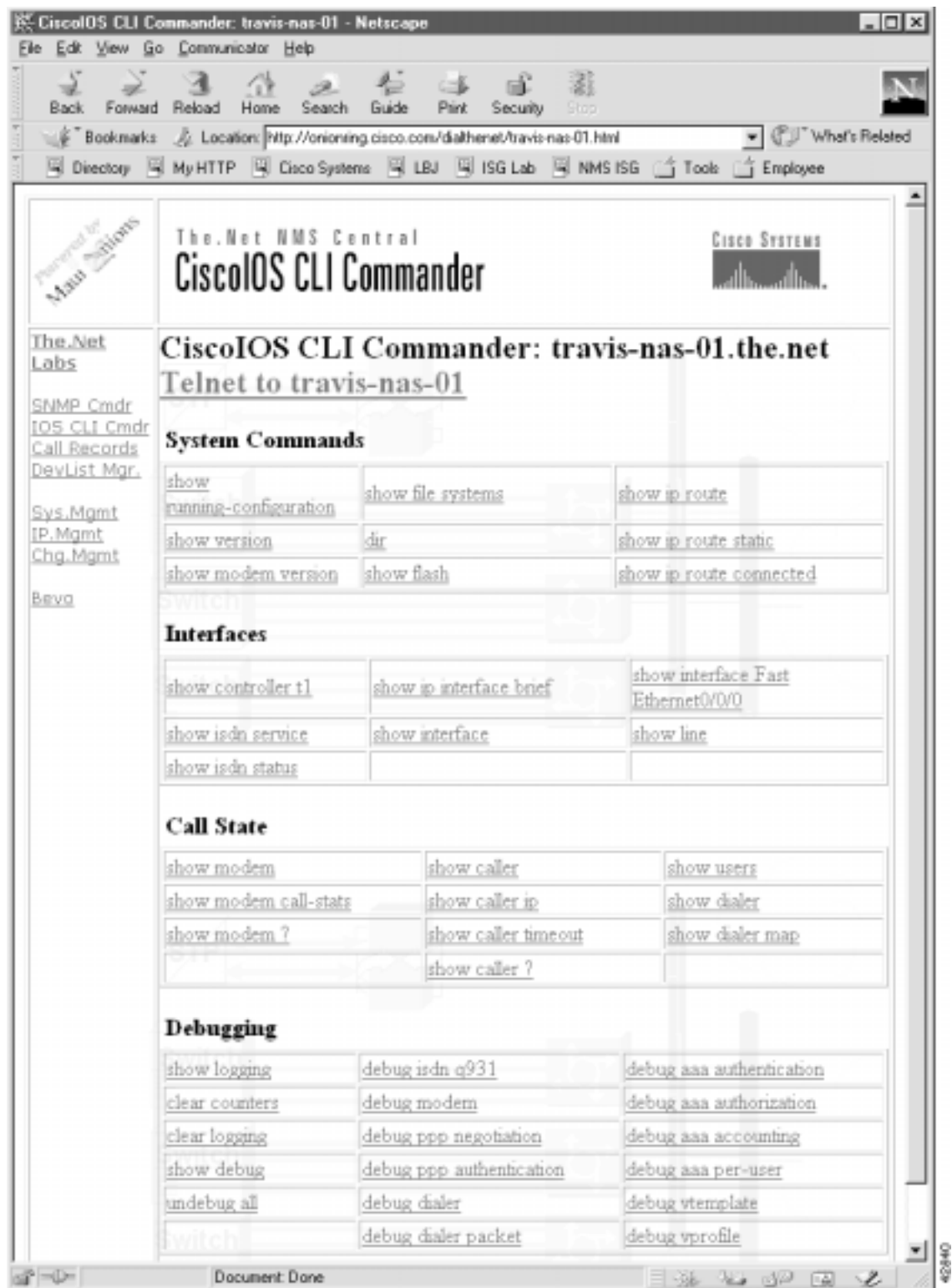
**Table 29**    *Debugging Commands*

<b>show logging</b>	<b>debug isdn q931</b>	<b>debug aaa authentication</b>
<b>clear counters</b>	<b>debug modem</b>	<b>debug aaa authorization</b>
<b>clear logging</b>	<b>debug ppp negotiation</b>	<b>debug aaa accounting</b>
<b>show debug</b>	<b>debug ppp authentication</b>	<b>debug aaa per-user</b>
<b>undebug all</b>	<b>debug dialer</b>	<b>debug vtemplate</b>
	<b>debug dialerpacket</b>	<b>debug vprofile</b>

**Step 3**    Post the HTML page that you created in Step 2 to a web server.



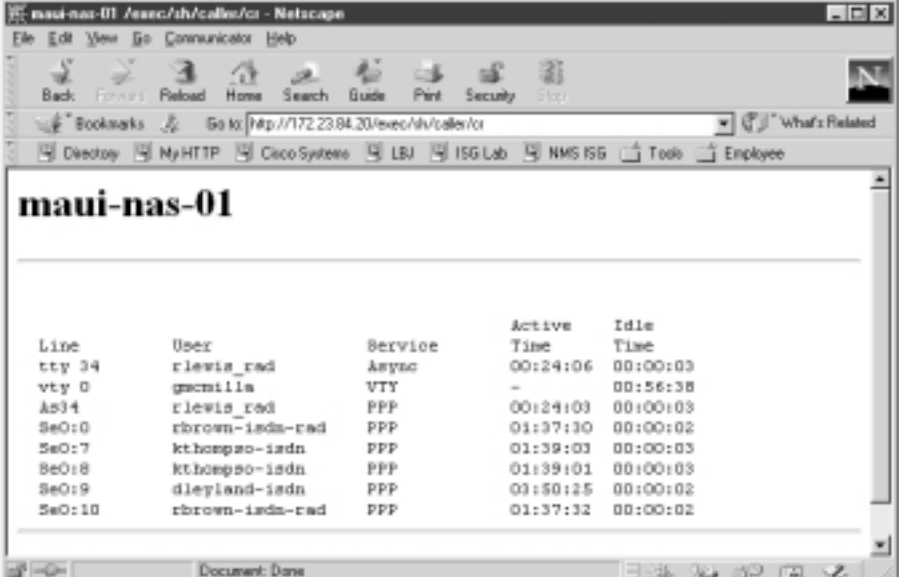
Figure 22 Cisco IOS CLI Commander



For the source code that created the Cisco IOS CLI Commander in Figure 22, go to <http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/httpcli.txt>

**Step 4** Click on a CLI command and view the command output in a web page.

**Figure 23** Output for the Show Caller Command



maui-nas-01

Line	User	Service	Active Time	Idle Time
tty 34	rlewis_rad	Async	00:24:06	00:00:03
vty 0	gacmilla	VTY	-	00:56:38
As34	rlewis_rad	PPP	00:24:03	00:00:03
Se0:0	rbrown-isdn-rad	PPP	01:37:30	00:00:02
Se0:7	kthompson-isdn	PPP	01:39:03	00:00:03
Se0:8	kthompson-isdn	PPP	01:39:01	00:00:03
Se0:9	dleyland-isdn	PPP	03:50:25	00:00:02
Se0:10	rbrown-isdn-rad	PPP	01:37:32	00:00:02



## Task 6—Managing IP Addresses by Using DNS

### About Managing IP Addresses

Managing IP addresses is a primary network administration function. Assigning and removing IP addresses can be tedious and error prone. Regardless—you must manage IP addresses to avoid duplicate IP subnets and addresses.

Domain Name System (DNS) servers provide two kinds of fundamental lookup services:

- **Forward lookups**—Used for looking up the IP address of a provided device name. This is the most common kind of lookup performed.
- **Reverse lookups**—Used for looking up a device name of a provided IP address. Administratively, reverse-lookup zones are important tools used for tracking IP address assignments.

In this case study, the dial engineers at THENet:

- Have received a block of IP addresses from the NOC with DNS administrative rights and instructions for setting up IP address space.
- Track IP address assignments by using DNS reverse lookup zones within the existing DNS service.
- Use the application Cisco Network Registrar (CNR) and its CLI to manage the IP address database. CNR is a full-featured IP address management solution for both enterprise and service provider networks. It includes advanced DNS and Dynamic Host Configuration Protocol (DHCP) servers.



**Note**

This section assumes you are familiar with the basics of DNS. For more information about DNS, see *DNS and Bind*, Third Edition, by Paul Albitz and Cricket Liu. The ISBN number is 1565925122.

**Table 30**    *Related References and Documents*

Reference	URL
<i>Internet Software Consortium for BIND</i> (Berkeley Internet Name Daemon)—Describes the DNS protocols.	<a href="http://www.isc.org/products/BIND/">http://www.isc.org/products/BIND/</a>
<i>Cisco Network Registrar</i> —A collection of DNS/DHCP user guides and reference manuals.	<a href="http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/index.htm</a>

## Using Cisco Network Registrar CLI Commands

Database locking prevents multiple users from writing to the same database records concurrently. However, an administrator may occasionally not exit a session properly, and the database may be left locked. To release the lock on the database, use the **force-lock** network registrar command.

Network registrar commands sent from the Unix shell lock the database only while commands are running.

The name for a reverse zone is the inverse of your Internet network number, added to the special domain in-addr.arpa. For example if the network number is 1.2.3.0, the reverse zone name is 3.2.1.in-addr.arpa. A second example is the network number 1.2.0.0 with the reverse zone of 2.1.in-addr.arpa.

For a description of the network registrar CLI commands, go to <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/nr30t/cliref/cli01.htm#68483>

To quickly perform administrative tasks by using CNR CLI commands, follow these steps:

- Step 1** Log in to the Cisco Network Registrar application by entering the following directory path:

```
/opt/nwreg2/usrbin/nrcmd
nrcmd>
```

After logging in, the command mode is accessed and the prompt “nrcmd>” appears.

- Step 2** To create an account for an administrator, enter the **admin** command and an associated password:

```
nrcmd> admin bob create password=xyz
```

In this example, the administrator name is **bob**. The password is **xyz**.

- Step 3** To see a list of existing administrators, enter the **admin list** command:

```
nrcmd> admin list
bob: password=*****;
omar: password=*****;
padma: password=*****;
```



**Note** The **admin list** command is a read-only command.

- Step 4** Inspect a reverse zone by entering the **zone** command and **listRR** option:

```
nrcmd> zone 101.21.172.in-addr.arpa. listRR

100 Ok
Static Resource Records
@                IN      SOA      onionring.the.net. netadmin.the.net 1997121601
3600 1800 86400 86400
@                IN      NS       onionring.the.net.com.
205              IN      PTR      unused-205.the.net.
203              IN      PTR      unused-203.the.net.
210              IN      PTR      unused-210.the.net.
204              IN      PTR      unused-204.the.net.
1                IN      PTR      unused-1.the.net.
10               IN      PTR      unused-10.the.net.
101              IN      PTR      unused-101.the.net.
102              IN      PTR      unused-102.the.net.
103              IN      PTR      unused-103.the.net.
104              IN      PTR      unused-104.the.net.
(truncated for brevity)
```

- Step 5** When working with a reverse zone, you can map an IP address to a router by entering the **zone** command and the **addRR** resource record (RR) option:

```
nrcmd> zone 101.21.172.in-addr.arpa. addRR 7 PTR bobslake-nas-01.the.net
```

- Step 6** Remove a resource record by entering the **zone** command and **removeRR** option:

```
nrcmd> zone 101.21.172.in-addr.arpa. removeRR 7 PTR unused-07.the.net
```

- Step 7** To minimize the lock-time on the database, enter the following CNR command from the Unix command line. Use quotations (“ ”) to contain the command and pass it to the shell.

```
/opt/nwreg2/usrbin/nrcmd "zone 101.21.172.in-addr.arpa. listRR"
```



**Note** The NRCMD command mode is not used.

- Step 8** Sort the records and parse the output by entering the following CNR command from the Unix command line:

```
/opt/nwreg2/usrbin/nrcmd "zone 101.21.172.in-addr.arpa. listRR" | sort -n | more
username: password:
0                IN      PTR      broadcast-0.the.net.
@                IN      NS       onionring.the.net.
@                IN      SOA      onionring.the.net. netadmin.the.net.101.
21.172.in-addr.arpa. 1997121606 3600 1800 86400 86400
Dynamic Resource Records
Static Resource Records
1                IN      PTR      unused-1.the.net.
2                IN      PTR      unused-2.the.net.
3                IN      PTR      unused-3.the.net.
4                IN      PTR      unused-4.the.net.
5                IN      PTR      unused-5.the.net.
6                IN      PTR      unused-6.the.net.
7                IN      PTR      unused-7.the.net.
8                IN      PTR      unused-8.the.net.
9                IN      PTR      unused-9.the.net.
10               IN      PTR      unused-10.the.net.
(truncated for brevity)
```

**Step 9** To add an “A” Resource Record (RR) to a forward zone (domain) and map a name to an IP address, enter the **zone** command:

```
nrcmd> zone the.net. addRR bobslake-nas-02 A 172.21.10.18

@                IN      NS      onionring.the.net.
@                IN      SOA     onionring.the.net. netadmin.the.net. 56 10800
3600 604800 86400
Dynamic Resource Records
Static Resource Records
aurora           IN      A        172.21.100.100
bobslake-nas-01  IN      A        172.21.10.10
bobslake-nas-02  IN      A        172.21.10.18
doc-2610-01      IN      A        172.21.10.13
doc-3810a-01     IN      A        172.21.10.14
doc-3810d-01     IN      A        172.21.10.15
doc-AS5850-01    IN      A        172.21.10.11
doc-core-01      IN      A        172.21.10.5
doc-core-02      IN      A        172.21.10.6
doc-core-03      IN      A        172.21.10.7
(truncated for brevity)
```

In the previous example, the **zone** command:

- Creates an A record for the.net
- Assigns the IP address 172.21.10.18 to the router bobslake-nas-02

**Step 10** To reload the server to make all IP assignments or changes take effect, enter the following command:

```
nrcmd> server dns reload
```



**Note** Reload all changes into the DNS database, so that the changes can be resolved upon lookup.

## Using a Batch File to Make Changes to a DNS Configuration

CNR can use batch files to make large and small-scale changes to the DNS configuration within your network.

To use the batch-file facility to add and remove entries, follow these steps:

### Step 1 Define the batch file by entering **zone** commands:

```
zone the.net. addRR doc-core-02 A 172.21.10.6
zone the.net. addRR doc-core-03 A 172.21.10.7
zone 10.21.172.in-addr.arpa. removeRR 6 PTR unused-6.the.net.
zone 10.21.172.in-addr.arpa. removeRR 7 PTR unused-7.the.net.
zone 10.21.172.in-addr.arpa. addRR 6 PTR doc-core-02.the.net.
zone 10.21.172.in-addr.arpa. addRR 7 PTR doc-core-03.the.net.
server dns reload
```

The previous batch-file example shows how to add two new device/IP addresses. In addition to adding two “A” records (lines 1 and 2), remove the “unused” PTR records from the reverse zone (lines 3 and 4) before adding the new “PTR” records, in place of the unused records, to the reverse zone (lines 5 and 6). See line 7 to reload the DNS server.

### Step 2 Run the script by using the **-b** option:

```
nrcmd> -b < 172.21.10.batch
```

The following output appears:

```
nrcmd>
zone the.net. addRR doc-core-02 A 172.21.10.6
100 Ok
doc-core-02                IN      A      172.21.10.6

nrcmd>
zone the.net. addRR doc-core-03 A 172.21.10.7
100 Ok
doc-core-03                IN      A      172.21.10.7

nrcmd>
zone 10.21.172.in-addr.arpa. removeRR 6 PTR unused-6.the.net.
100 Ok
removing 6                  IN      PTR      unused-6.the.net.

nrcmd>
zone 10.21.172.in-addr.arpa. removeRR 7 PTR unused-7.the.net.
100 Ok
removing 7                  IN      PTR      unused-7.the.net.

nrcmd>
zone 10.21.172.in-addr.arpa. addRR 6 PTR doc-core-02.the.net.
100 Ok
6                            IN      PTR      doc-core-02.the.net.

nrcmd>
zone 10.21.172.in-addr.arpa. addRR 7 PTR doc-core-03.the.net.
100 Ok
7                            IN      PTR      doc-core-03.the.net.

nrcmd>
server dns reload
100 Ok
```

## Creating a Primary Forward Zone

To create a domain (or forward zone) and include all forward mapping (the “A” records) for the domain, follow these steps:

- Step 1** Create a domain and include all forward mapping (the “A” records) by entering the **zone** command with the **create** option:

```
nrcmd> zone the.net create primary file=the.net.zone.txt
```

To create new subnets by using the CLI, import a BIND zone definition file, which can be edited by using an ASCII text editor. The following example shows an edited BIND file.

```
@                IN      SOA      onionring.the.net. netadmin.the.net. (
                2000071600    ; serial number
                3600          ; Refresh 1 hours
                1800          ; Retry 30 minutes
                86400         ; Expire 24 hours
                86400         ; TTL 24 hours
                )
doc-rtr58-01     IN      NS       onionring.the.net.
doc-rtr54-01     IN      A        172.21.101.20
doc-rtr53-01     IN      A        172.21.101.21
doc-rtr53-01     IN      A        172.21.101.22
doc-rtr53-05     IN      A        172.21.101.23
doc-3810a-01     IN      A        172.21.10.14
doc-3810d-01     IN      A        172.21.10.15
doc-ubr7246-01   IN      A        172.21.10.16
doc-switch-02    IN      A        172.21.10.17
```

- Step 2** Verify that the primary zone was created by entering the **zone** command with the **listRR** option:

```
nrcmd> zone the.net listRR
100 Ok
Static Resource Records
@                IN      SOA      onionring.the.net.
netadmin.the.net.0
@                IN      NS       onionring.the.net.
doc-rtr58-01     IN      A        172.21.101.20
doc-rtr54-01     IN      A        172.21.101.21
doc-rtr53-01     IN      A        172.21.101.22
doc-rtr53-05     IN      A        172.21.101.23
(Truncated for brevity)
Dynamic Resource Records
```

## Creating an IP Tracker Web Page

An IP tracker web page:

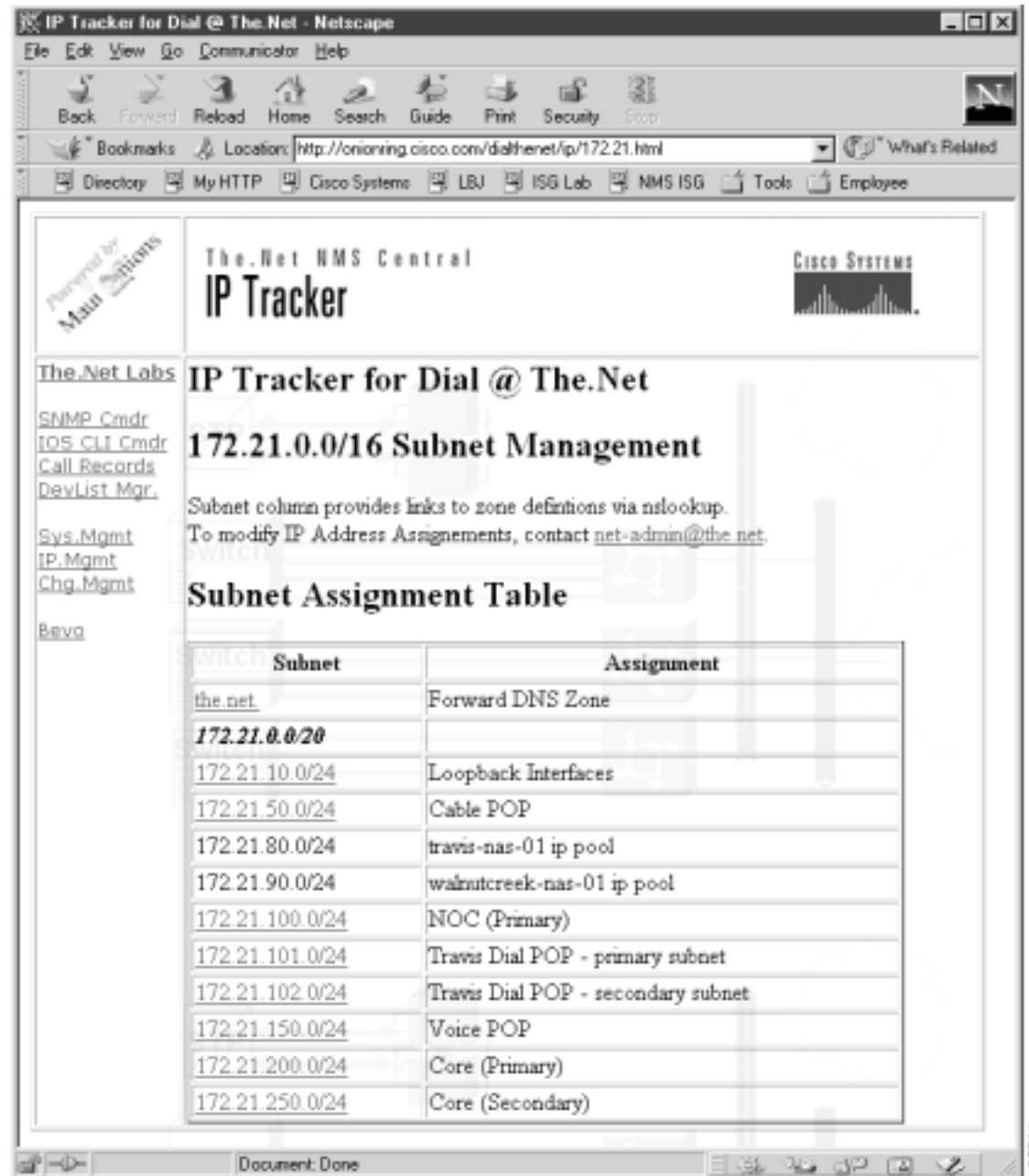
- Provides web access to the IP database that is managed by Cisco Network Registrar.
- Retrieves current IP address block assignments from a DNS server.
- Uses two CGI scripts to provide a web-enabled look into DNS for each zone.



To create an IP tracker web page, follow these steps:

- Step 1** Become familiar with the layout of an IP tracker web page. In Figure 24, the subnet column shows a list of all managed zones. The assignment column describes the purpose of each zone.

**Figure 24 IP Tracker Web Page**



**Step 2** Understand how the CGI scripts function.

There are two scripts that work together to return an NSLOOKUP list query (ls) for a specified zone in a CGI link.

- *dnszone.pl*—Runs the CGI process. In the subnet column in Figure 24, the entry 172.21.10.0/24 is an active link that calls the *dnszone.pl* script.

The active link is coded as:

```
<td><a href="/cgi-lwt/dnszone.pl?zone=10.21.172.in-addr.arpa.">172.21.10.0/24</a></td>
```

Once invoked, *dnszone.pl* calls the second script, *dnszone\_dump*.

- *dnszone\_dump*—An expect script that steps through the NSLOOKUP interactive mode and returns the output of a “ls [ZONE]” command to the *dnszone.pl* script. The zone list, returned to the requesting web-based management browser, appears:

```
ls 10.21.172.in-addr.arpa.
```

```
[www.the.net]
0          host = broadcast-0.the.net
1          host = unused-1.the.net
2          host = unused-2.the.net
3          host = unused-3.the.net
4          host = unused-4.the.net
5          host = doc-core-01.the.net
6          host = doc-core-02.the.net
7          host = doc-core-03.the.net
8          host = doc-ls1010-01.the.net
9          host = doc-switch-01.the.net
10         host = doc-pix-01.the.net
10.21.172.in-addr.arpa.  server = onionring.the.net
11         host = doc-AS5850-01.the.net
12         host = doc-oob-03.the.net
13         host = doc-2610-01.the.net
14         host = doc-3810a-01.the.net
15         host = doc-3810d-01.the.net
16         host = doc-ubr7246-01.the.net
17         host = doc-switch-02.the.net
```

**Step 3** Download the source code for the scripts and customize them for your environment.

Go to <http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/dnszone.txt>

# How to Create a Reverse DNS Zone

By creating reverse lookup zones for each IP subnet, you gain a robust database that can be used to track assignments within an IP address space. Reverse lookups can determine the allocation status of any address from any DNS client.

Network operators must account for used and unused IP addresses. It is recommended that each IP address be given a DNS PTR Resource Record, even if the address is unused. For example, you can look up and resolve an IP address as “unused-XXX.the.net.”

See the following example to create a zone from a BIND file by entering the **zone** command:

```
nrcmd> zone 101.21.172.in-addr.arpa. create primary file=the.net_rev_zone.txt
```

The following edited BIND definition file is for “the.net\_rev\_zone.txt.”

```
@                IN      SOA      onionring.the.net
esupport-austin.the.net. (
                        2000071600      ; serial number
                        3600             ; Refresh 1 hours
                        1800             ; Retry 30 minutes
                        86400            ; Expire 24 hours
                        86400            ; TTL 24 hours
                        )
;
                        IN      NS      onionring.the.net.
;
0                IN      PTR      broadcast-0.the.net.
1                IN      PTR      unused-1.the.net.
2                IN      PTR      unused-2.the.net.
3                IN      PTR      unused-3.the.net.
4                IN      PTR      unused-4.the.net.
5                IN      PTR      unused-5.the.net.
6                IN      PTR      unused-6.the.net.
7                IN      PTR      unused-7.the.net.
8                IN      PTR      unused-8.the.net.
9                IN      PTR      unused-9.the.net.
10               IN      PTR      unused-10.the.net.
11               IN      PTR      unused-11.the.net.
12               IN      PTR      unused-12.the.net.
13               IN      PTR      unused-13.the.net.
14               IN      PTR      unused-14.the.net.
15               IN      PTR      unused-15.the.net.
16               IN      PTR      unused-16.the.net.
17               IN      PTR      unused-17.the.net.
18               IN      PTR      unused-18.the.net.
19               IN      PTR      unused-19.the.net.
20               IN      PTR      doc-rtr58-01.the.net.
21               IN      PTR      doc-rtr54-01.the.net.
22               IN      PTR      doc-rtr53-01.the.net.
23               IN      PTR      doc-rtr53-01.the.net.

(Truncated for brevity..)

253              IN      PTR      unused-253.the.net.
254              IN      PTR      unused-254.the.net.
255              IN      PTR      broadcast-255.the.net.
```

For a sample BIND file that can be used as a template and edited for your environment, go to <http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/bindtemp.txt>





## Task 7—Using HP OpenView to Create the SNMP Framework

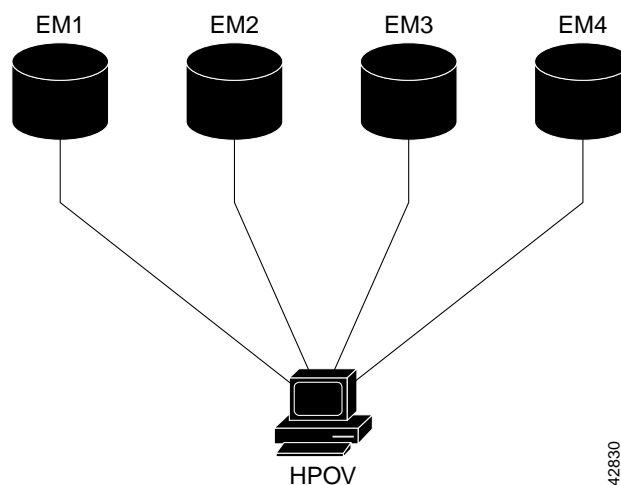
### About HP OpenView

The primary function of HP OpenView (HPOV) is to manage faults.

In this case study, HP OpenView:

- Discovers all the devices in the network.
- Functions as the central-starting point for other element managers (EM). After HPOV is installed, the remaining components of the network management architecture are built around HPOV.
- Resides on the same Unix workstation as CiscoWorks 2000 Resource Manager Essentials, which gathers the following database information from HPOV:
  - Device names and IP addresses
  - Community strings

**Figure 25** Other Element Managers Start from HPOV



**Note**

This section assumes that HP Network Node Manager Release 5.0 is already installed on a Solaris workstation.

Describing the advanced capabilities of HPOV is outside the scope of this document. For more information, go to [http://ovweb.external.hp.com/lpe/doc\\_serv/](http://ovweb.external.hp.com/lpe/doc_serv/) and <http://www.openview.hp.com>

For Cisco IOS SNMP configurations, see the “Task 1—Enabling SNMP in a Cisco IOS Device” section on page 41.

## Verifying the SNMP Configuration

To verify that the HPOV daemons are running and the SNMP configuration is correct, follow these steps:

- Step 1** Start HPOV from the command line by entering the **ovw&** command from the /opt/OV/bin directory:

```
aurora:/opt/OV/bin ->ovw&
[1]      5079
```

- Step 2** Verify that all the HPOV daemons are running by entering the **ovstatus** command from the root directory:

```
aurora:/ ->ovstatus
object manager name: OVSPMD
state:                RUNNING
PID:                  430
exit status:          -

object manager name: ovwdb
state:                RUNNING
PID:                  431
last message:         Initialization complete.
exit status:          -

object manager name: ovtrapd
state:                RUNNING
PID:                  433
last message:         Initialization complete.
exit status:          -

object manager name: ovactiond
state:                RUNNING
PID:                  434
last message:         Initialization complete.
exit status:          -

object manager name: pmd
state:                RUNNING
PID:                  432
last message:         Initialization complete.
exit status:          -

object manager name: ovtopmd
state:                RUNNING
PID:                  435
last message:         Connected to native database: "openview".
exit status:          -

object manager name: netmon
state:                RUNNING
PID:                  450
last message:         Initialization complete.
exit status:          -
```

```
object manager name: snmpCollect
state:                RUNNING
PID:                  451
last message:         No values configured for collection.
exit status:          -

object manager name: ovrepld
state:                RUNNING
PID:                  452
last message:         Initialization Complete.
exit status:          -
```



**Note** If a daemon is not running, try restarting it by using the commands **ovstop** *daemon-name* and **ovstart** *daemon-name*. If a daemon is still not running, an HPOV license issue may exist. For more information, go to <http://www.openview.hp.com>

**Step 3** From HPOV, enter the SNMP community strings and target loopback IP addresses for each Cisco IOS device. From the **Options** menu, select **SNMP Configuration**.

In the SNMP Configuration screen, enter the following information:

- Target field—The target loopback IP address (for example, 172.21.10.1)
- Community field—The Read-Only (RO) community string (for example, 5urf5h0p)
- Set Community field—The Read-Write (RW) community string (for example, 5crapmeta1)



**Note**

Accept the default SNMP parameters in the other fields in the SNMP Configuration screen.



**Caution**

Do not use the SNMP community strings “public,” “private,” or “cisco.” These strings are well-known within the industry, and they are common defaults. These strings are open invitations to attacks—even if you use filters.

Figure 26 SNMP Configuration: Loopback IP Address and Community Strings

SNMP Configuration for aurora

Specific Nodes

Node	Community	Set Community	Proxy	Timeout	Retry	Port	Polling
172.21.10.1	Surf5h0p	Scrapmetal	<none>	-	-	-	-

IP Address Wildcards

IP Wildcard	Community	Set Community	Proxy	Timeout	Retry	Port	Polling
-------------	-----------	---------------	-------	---------	-------	------	---------

Default

Default	Community	Set Community	Proxy	Timeout	Retry	Port	Polling
Global Default	public	-	<none>	0.8	2	-	5s

SNMP Parameters

☐ Use Proxy to Access Target

Proxy

Target

Community

Set Community

Timeout

Retry Count

Remote Port

Status Polling

172.21.10.1

Surf5h0p

Scrapmetal

Add

Reset

Replace

Delete

Reorder

OK

Apply

Close

Help

Step 4 Click **Add** and **Apply** to submit the entries.



## About SNMP Demand Polls

Perform an SNMP demand poll for a new managed device if you do not want to wait for the next automatic topology poll. HPOV performs less frequent automatic topology demand polls as your network and the HPOV device database becomes more static.

When the HPOV daemons start, HPOV discovers the devices in your network. Depending on which discovery options are configured, the device map is based on Layer 2 or Layer 3 information. Choosing discovery options is outside the scope of this document.

Depending on the number of devices that need to be discovered, it could take hours or even days for HPOV to discover a device. If HPOV cannot find a device, enter the device manually into the database. See the “Using the HPOV CLI to Enter a Device into the Database” section on page 115.

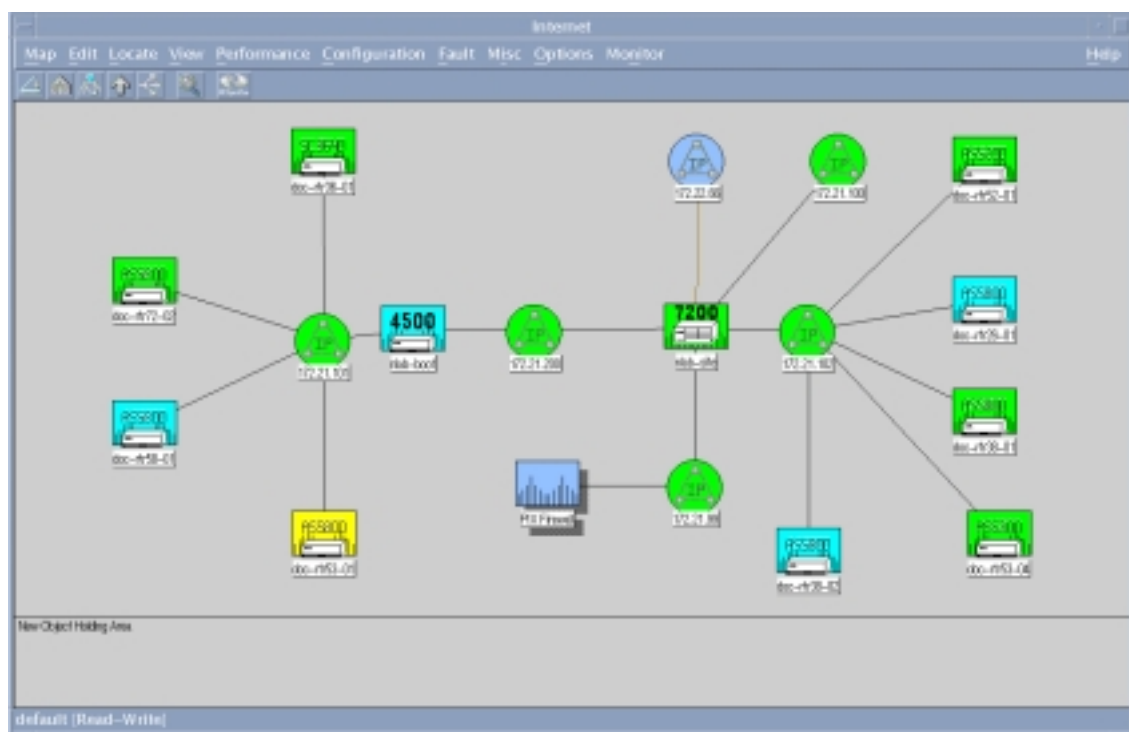
To organize and adjust the top-level map, see the “Creating and Adjusting Maps” section on page 111.

## Performing an SNMP Demand Poll

To perform an SNMP demand poll, follow these steps:

- Step 1** From the Root screen, double click the planet Earth Internet icon.
- Step 2** Inspect the top-level map of the discovered devices in your network.

**Figure 27 The Top-Level Device Map**



Map color legend:

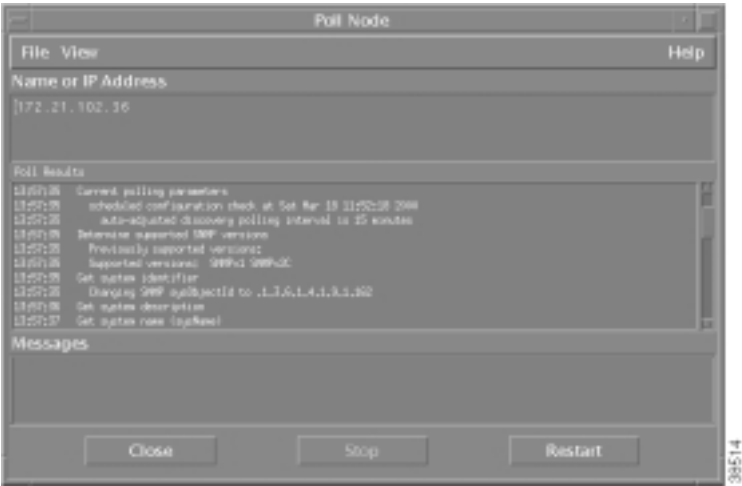
- Green—The device is up.
- Yellow—Multiple interfaces are down.
- Light blue—One interface is down.
- Dark blue—The device is detected, but it has never been managed. The device is unreachable.
- Red—The device is down and unreachable.

**Step 3** Select a device icon in the map (single click).

**Step 4** Go to **Fault**.

**Step 5** Select **Network Connectivity: Poll Node**.

**Figure 28** SNMP Walk-Polling Results



Demand polls enable HPOV to:

- Detect the sysobjectID (vendor ID) for each Cisco device.
- Associate MIBs with each device.
- Collect interface information.

**Table 31** Important Fields to Inspect In the Polling Results

Field	Description
Changing SNMP sysobjectID to .1.3.6.1.4.1.9.1.162	Indicates SNMP is working and the system identifier for the device was found. This field appears only the first time a device is successfully polled.  HPOV changes a generic router icon into a Cisco device icon after the sysobjectID is found. The trailing number series, for example .1.3.6.1.4.1.9.1.162, is the OID that identifies a node as a Cisco device.
Supported versions	Describes which versions of SNMP are supported by HPOV, such as SNMPv1 and SNMPv2C.
Verify node name	Verifies the node name is valid.

**Table 31** Important Fields to Inspect In the Polling Results (continued)

Field	Description
Interface	Confirms the interfaces were successfully pinged.
Get system description	Verifies that the system description information was collected, so you can identify the software version running on the device.

## Testing SNMP Get Requests

To test that a device responds to SNMP **Get** requests, follow these steps:

- Step 1** Select a device icon in the map (single click).
- Step 2** From the **Fault** menu, select **Test IP/TCP/SNMP**.

**Figure 29** Successful SNMP Test

This action performs one ICMP echo, one TCP connection, and one SNMP get. SNMP is working if the “OK” message appears under the SNMP Get field.

Table 32 describes the important fields in Figure 29.

**Table 32** Test IP/TCP/SNMP Field Descriptions

Field	Returned Value	Description
Node	172.21.102.33	The target loopback IP address of the Cisco device.
ICMP Echo	26 ms	HPOV successfully pinged the device.
TCP Connect	OK	HPOV successfully made a TCP connection with the device.
SNMP Get	OK	HPOV successfully made an SNMP query to the device.

# Troubleshooting SNMP and a Demand Poll

If a device is not responding to a demand poll, follow these steps:

- Step 1** Poll a different device to see if it responds to SNMP. If the device responds, HPOV is not the problem.
- Step 2** Ping the device that is not responding. If the ping works, the devices are communicating.



**Note** A firewall in the communication path can block ping and SNMP packets.

- Step 3** Verify that the SNMP community strings are correct.
- Step 4** Try polling the device from the HPOV command line. For example, enter the commands **snmpwalk** and **snmpget**.

The syntax for the **snmpget** command line is as follows:

**snmpget** [options] node object-id [object-id]...

Options:

-d	dump ASN.1 packet trace
-v version	protocol version (1 or 2c)
-c community	community string
-p port	remote port
-t timeout	retransmission timeout (1/10th seconds)
-r retries	maximum retransmission attempts



**Caution** Overpolling the wrong OIDs overloads CPUs and crashes network devices.

## Verifying that SNMP Traps Are Received

Traps appear in the All Events Browser, which reports what is happening in the network. The events are updated every few seconds. Understanding the severity level of a trap is important. One trap can be critical; whereas, another trap can be informative.

Other ways to look for traps include:

- Using a network analyzer to capture and inspect data on the line.
- Using the **snoop** Unix command to sniff the line and inspect data.

To monitor the limits of a network, configure thresholds to set off alarms. For example, set up an alarm for a CPU that sustains a 98 percent utilization for a specific amount of time.

Common mistakes include:

- Setting thresholds too low.
- HPOV is in a constant alarm state because you do not understand how to operate or monitor the dynamics of the equipment.

Setting up alarms for different kinds of traps is outside the scope of this document.

To verify that HPOV is receiving traps from devices in the network, follow these steps:

- Step 1** Open the All Events Browser. From the **Fault** menu, select **Events**.

**Figure 30** Traps in the All Events Browser

All	Severity	Description	Source	Message
Major	25	23:41:12	slab-site.cisco.com	172.21.302.31 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Major	25	23:41:12	slab-site.cisco.com	172.21.302.31 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Minor	16	04:21:21	172.21.182.20	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Major	25	08:52:28	slab-site.cisco.com	172.21.302.31 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Minor	16	00:01:44	172.21.182.20	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	05:04:06	172.21.182.20	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	07:04:28	172.21.182.20	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	09:04:52	172.21.182.20	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Major	25	18:09:39	slab-site.cisco.com	172.21.302.36 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Major	25	18:34:29	slab-site.cisco.com	172.21.302.36 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Major	25	11:01:12	slab-site.cisco.com	172.21.302.31 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Minor	16	11:05:19	172.21.182.20	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Major	25	11:40:04	slab-site.cisco.com	172.21.302.31 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Major	25	12:26:28	slab-site.cisco.com	172.21.302.31 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Major	25	18:52:28	slab-site.cisco.com	172.21.302.31 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Major	25	11:00:58	slab-site.cisco.com	172.21.302.36 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Minor	16	11:41:49	172.21.182.1	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	11:41:49	172.21.182.1	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	11:41:49	172.21.182.1	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	11:49:07	slab-site.cisco.com	Network Mode Manager license expires on the Jul 27 16:58:19 2008
Major	25	12:23:35	slab-site.cisco.com	172.21.302.31 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Minor	16	13:40:14	172.21.182.1	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	13:40:14	172.21.182.1	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	13:40:14	172.21.182.1	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Major	25	14:04:06	slab-site.cisco.com	172.21.302.36 reports address (000000000000) for 172.21.182.1, slab-site.cisco.com reported 0000000000 via SNMP
Minor	16	15:31:06	172.21.182.20	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Major	25	15:34:08	slab-site.cisco.com	Network Mode Manager license expires on the Jul 27 16:58:19 2008
Major	25	15:39:54	slab-site.cisco.com	Network Mode Manager license expires on the Jul 27 16:58:19 2008
Warning	18	15:39:17	172.21.182.1	Class Inconsistent Community Name (authenticationFailure) Trap: notMib: source
Warning	18	15:39:19	172.21.182.1	Class Inconsistent Community Name (authenticationFailure) Trap: notMib: source
Warning	18	15:39:19	172.21.182.1	Class Inconsistent Community Name (authenticationFailure) Trap: notMib: source
Minor	16	15:40:58	172.21.182.1	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	15:40:58	172.21.182.1	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1
Minor	16	15:40:58	172.21.182.1	TIP connection has been terminated. (tcpConnection: Trap) to: 172.21.182.1

- Step 2** Force a trap to be sent into the browser by manually causing a fault. Pull out a card on a Cisco device or shut down an interface.



**Caution**

Do not shut down a communication link that can cause a service outage.

- Step 3** Look for traps in the browser.

## Unmanaging the Dial Ports

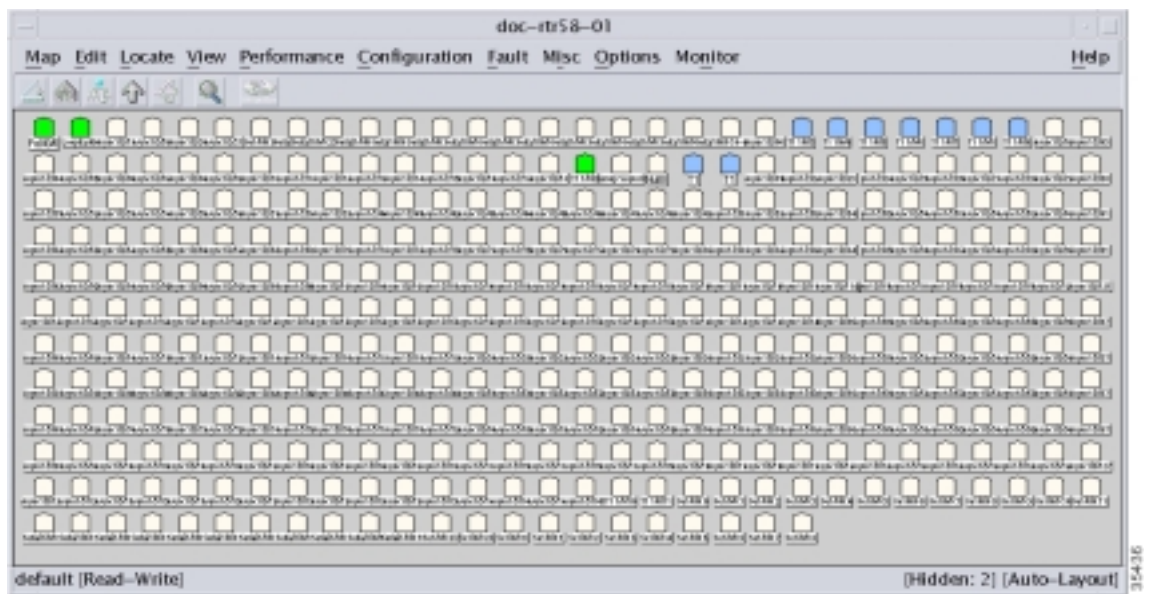
Do not poll the asynchronous and serial interfaces on Cisco access servers. The reasons for this recommendation include:

- As remote users dial in to an access server, it is normal behavior for asynchronous and serial interfaces to regularly go up and down.
- On an average 20-minute call, one modem normally produces three alerts. At approximately 6 alerts per hour, one modem can produce up 144 events each day. One Cisco AS5800 fitted with 1296 modems can produce up to 186,624 modem events per day.

To unmanage the asynchronous and serial interfaces for a Cisco access server, follow these steps:

- Step 1** From the top-level map, double click on an access server icon. The available interfaces and ports appear.

**Figure 31** Available Interfaces and Ports for a Cisco AS5800



Color legend:

- Green—The port is managed, and it is up.
- Blue—The port is managed, but it is administratively down on the Cisco IOS.
- Tan—The port is unmanaged.
- Red—The port is managed, but it is in a down state.

**Step 2** Find the following interfaces:

- Serial interface channels (B and D channels). For example, Se1/0/0:6 and Se1/0/0:23
- Asynchronous interfaces. For example, Async 1/2/1

**Step 3** Select a group of ports to unmanage. Draw a box around the ports, or select them individually.

**Step 4** From the **Map** menu, select **Unmanage Objects**. Unmanage all ports except the T1 trunks, loopback management interface, and Ethernet interface. Statistics are polled from managed ports.



**Note**

---

You must unmanage the serial and asynchronous ports, which appear tan.

---



**Tips**

---

When the status of an object changes (to managed or unmanaged), HPOV switches to synchronization mode.

---

## Creating and Adjusting Maps

Maps provide a view of the network topology, and they enable you to quickly troubleshoot faults in the network. HPOV automatically polls devices and builds maps for you; however, devices often get stacked in the map, which is undesirable.

The following procedure saves you from having to refresh all your submaps each time a new device appears in the network. After you implement the following procedure, new devices will appear in the New Object Holding Area.



**Caution**

---

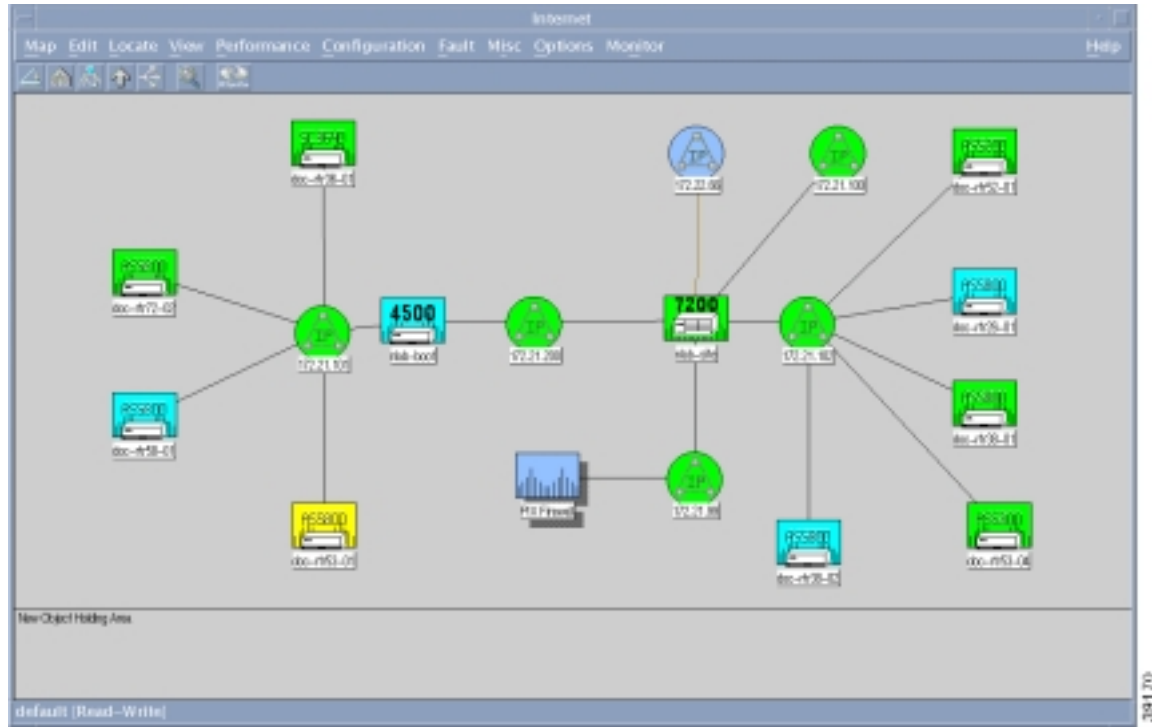
Deleting a device from a submap removes the device from the database. To load a device back into the database, see the “Using the HPOV CLI to Enter a Device into the Database” section on page 115.

---

To manually re-structure device maps to adequately represent your network and turn off the automatic-layout function for the top-level map, follow these steps:

- Step 1** Re-structure the top-level map by selecting and moving device icons. For example, put a collapsed backbone in the center of the map; then, position devices around the backbone.

**Figure 32 Top-Level Map Adjustments**



- Step 2** Go to **View**.
- Step 3** Select **Automatic Layout**.
- Step 4** Choose **Off For This Submap**.

## About Discovery Filters

A discovery filter is an ASCII file that HPOV reads to limit the discovery of devices on the network.

Use a discovery filter to:

- Define the subnets and devices you want to monitor.
- Avoid managing PCs and other non SNMP devices on the network.

Sometimes HPOV discovers too many devices. If HPOV discovers devices beyond your target network, such as the entire Internet, the performance of the Unix host decreases significantly. If the device maps begin filling up with networks, routers, and other devices that do not belong to you, use a discovery filter.



After a filter is set up, HPOV will not discover devices unless they are defined by the filter. Edit the filter each time a new device is added to the network.

For more information about discovery filters, go to <http://www.openview.hp.com>

## Setting Up and Editing a Discovery Filter

The filter file is located in the `/etc/opt/OV/share/conf/C` directory. A sample file is shown in the following step-by-step example. The file has been manually edited and abbreviated to include a specific node list and filter list for this case study:

- **Node list**—A list of specific devices. In the example, the list is called `TheNetNodes`. There are two devices in the list: `AS5800-1` and `AS5800-2`.
- **Filter list**—A list of attributes for the specified devices. In the example, the list is called `TheNetFilters`, which specifies the filtering attributes for the devices in the node list. For example, all devices must be SNMP compliant and Cisco devices.

To see a complete filter file, go to

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialnms/filter.txt>

To set up and edit a discovery filter, follow these steps:

---

**Step 1** Find the filters file on your Unix workstation:

```
aurora:/etc/opt/OV/share/conf/C ->ls
filters      oid_to_sym  trapd.conf
```

**Step 2** Edit the filters file by using a text editor to include a node list and a filter list for your network environment:

```
aurora:/etc/opt/OV/share/conf/C ->vi filters
//
// @(#) $OV_CONF/$LANG/filters
// @(#) HP OpenView NNM Release B.05.01 Jun 21 1997
// @(#) Copyright (c) 1990-1997 Hewlett-Packard Company
// $Revision: /main/TORNADO/NNM_NT/5 $ $Date: 1997/01/13 19:35 UTC $
//
// This is the default filter file. These filters are examples
// which may be useful in your environment. Feel free to modify
// these filters and/or add your own. See OVfilterIntro(5)
// for more information on this file.

// NOTE: The behavior of topology filters in a distributed environment
// changed as of DFIX 5027. This file documents the behavior as of that
// patch level. This should be considered the correct specification of
// how topology filtering behaves in a distributed environment.

//
// Sets are a simple way to list string values to test
// against in a filter. The "IN" operator tests a field value
// for membership in a set defined here.
//
Sets {
//
// These are simple examples of sets.
//
servers "Set of Servers" { "sv1", "sv2", "sv3" }
gateways "Backbone gateways" { "gw1", "gw2", "gw3" }
TheNetNodes "TheNet Node List" { "AS5800-1", "AS5800-2" }
```

```

}
.
.
.
FilterExpressions {
    //
    // The following combines the two set filters
    // defined above into one FilterExpression.
    // It works unmodified as a discovery filter.
    // To work as a map filter, network and segment filtering
    // must be added (see below).
    VitalNodes "All Gateways and Servers" { GatewaysSet || ServersSet }

    //
    // One can turn the filters defined above into viable map or
    // topology filters by simply adding "|| NetsNSegs". (Doing so
    // does not invalidate the filters as discovery
    // filters. It just adds a superfluous test.)
    //
    VitalNodesMap "All nets & segs, but only gateway and server nodes"
        { GatewaysSet || ServersSet || NetsNSegs }
    LocalLANView "All nets & segs, but only local nodes"
        { LocalLAN || NetsNSegs }
    NetInfrastructure "Any network connecting device and what they connect"
        { Routers || Bridges || Hubs || NetsNSegs }
    NetBackbone "Networks and gateways/routers"
        { Routers || Networks }

    // Using the filters defined above that include only a specific
    // network, we can also exclude the specific network like this
    // Note the use of the more specific form to exclude only the segments
    // in the engineering lan. This could have been specified directly
    // as a negation in the filter part, but this form works well if you
    // have several networks to manipulate in this manner.
    EverythingButEngr "Everything but the engineering LAN"
        { !EngrLan2 }

    // Of course the above filter expressions, when used as
    // map filters, pass all networks and segments. You
    // may wish to see only a particular network. The following map
    // filters accomplish this. Note that though segments
    // and nodes from other networks will pass the filters, IP Map
    // will ignore them because their parent networks will not pass.
    // NOTE: These filters will not work as Discovery
    // filters because all network and segments automatically pass
    // Discovery and Topology filters.
    //
    MyNetMap "Only the network of interest and all its constituent parts"
        { MyNet || Segments || Nodes }
    MyVitalNodesMap "Gateways, servers and segments in the net of interest"
        { MyNet || Segments || GatewaysSet || ServersSet }
    TheNetNodeList "This is the filter for TheNet nodeslist"
        { TheNetNodes || TheNetFilters }

    // This is a map persistence filter which ensures that
    // all Ungermann-Bass are kept in memory and up to date.
    // Note that this will also keep any containing submaps in memory.
    //
    PersFilter "Objects to keep in map memory" { UBNodes }
}

```

## Using the HPOV CLI to Enter a Device into the Database

Sometimes devices do not appear in the device map, or they are accidentally deleted from the HPOV database.

To manually load devices in to the HPOV database by using the CLI, follow these steps:

- Step 1** This step ensures that new host entries are safely loaded in to the database. Shutdown the netmon daemon by entering the **ovstop netmon** command from the root directory. All automatic network polling and database updates stops.

```
aurora:/ ->ovstop netmon
aurora:/ ->ovstatus netmon
object manager name: netmon
state: NOT_RUNNING
PID: 450
last message: Exited due to user request
exit status: Exit(0)
```

- Step 2** To load new devices in to the database, enter the **loadhosts -m** command from the root directory followed by a single netmask for the devices. Include an end of file statement (EOF) to enter multiple lines with one return.

```
aurora:/ ->loadhosts -m 255.255.255.0 <<EOF
> 10.10.10.104      hostname
> 14.14.14.14      host2name
> EOF
aurora:/ ->
```



**Note** Enter devices by using a DNS format (IP address then hostname). Use spaces (not tabs) to separate IP addresses from hostnames.

- Step 3** Restart the netmon daemon by entering the following commands:

```
aurora:/ ->ovstart netmon
aurora:/ ->ovstatus netmon
object manager name: netmon
state: RUNNING
PID: 12812
last message: Initialization complete.
exit status:
```

- Step 4** Go to the GUI and look for the new devices that appear in the new object holding area.
- Step 5** Perform a demand poll on each device to get the sysobjectIDs. After the demand poll is performed, HPOV puts each new device into its correct place in the map.





## Task 8—Using CiscoWorks 2000 Resource Manager Essentials

---

### About CiscoWorks 2000 RME

Cisco Works 2000 Resource Manager Essentials (CW2000 RME) is an element manager used to routinely manage Cisco equipment.

In this case study, CW2000 RME is used for the following tasks:

- Inspecting syslogs to isolate faults and device problems.
- Sorting syslog messages based on device and date.
- Polling for device and interface status.
- Backing up and restoring Cisco IOS configurations (images and configuration files).

The following installation assumptions are made in this case study:

- CW2000 maintenance release 2 has been installed on a Solaris workstation. RME version 2.2 is available.
- CW2000 is installed on the same Unix workstation as HP OpenView (HPOV).
- CiscoView uses HPOV as a starting point.

**Table 33**    *Related References and Documents*

Reference	URL
<b>CiscoWorks 2000 TAC Support Page</b> —Provides links to technical information for implementing, operating, and troubleshooting Cisco Works 2000.	<a href="http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Software:CiscoWorks2000">http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Software:CiscoWorks2000</a>
<b>CiscoWorks 2000 Documentation Set</b> —A collection of configuration guides and reference manuals.	<a href="http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm</a>

## Importing Devices from HPOV and Populating the Databases

In this case study, CW2000 RME relies on the automatic-discovery mechanism in HPOV to discover devices in the network. CW2000 RME extracts the following information from the HPOV database after HPOV discovers the devices:

- SNMP community strings
- Device IP addresses
- Device names

Device information is stored in the following database locations:

- For HPOV, /var/opt/OV/share/databases
- For CW2000, /opt/CSCOpX/objects/db/px.db



**Note** Alternatively, you can use Cisco Works for Switched Internetworking (CWSI) to discover devices instead of using HPOV.

To import the list of devices and SNMP community strings from HPOV into CW2000 RME, follow these steps:

**Step 1** Verify that the basic setup for HPOV is working correctly.

Incorrect SNMP community strings prevent polling cycles. For basic verification steps, see the “Task 7—Using HP OpenView to Create the SNMP Framework” section on page 101.

**Step 2** From the root directory, verify that the HPOV database daemon is running in the background by entering the **ovstatus ovwdb** command:

```
aurora:/ ->ovstatus ovwdb
object manager name: ovwdb
state:                RUNNING
PID:                  442
last message:         Initialization complete.
exit status:          -
```

```
aurora:/ ->
```



**Note** If a daemon is not running, try restarting it by using the commands **ovstop daemon-name** and **ovstart daemon-name**. If a daemon is still not running, an HPOV license issue may exist. For more information, go to <http://www.openview.hp.com>

**Step 3** From a web browser, log in to CW2000 RME.

**Step 4** Click on the **Admin** menu on the left toolbar.

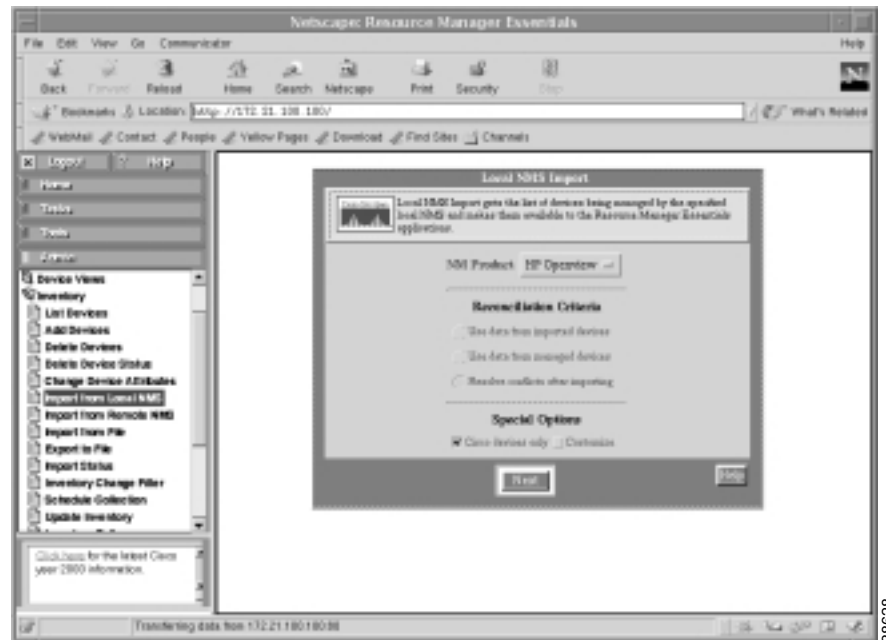
**Step 5** Select **Inventory: Import from Local NMS**.

**Step 6** In the Import from Local NMS screen:

- Select **HP Openview** from the NM Product rectangular-shaped menu.
- Choose **Resolve conflicts after importing**.
- Choose **Cisco devices only**.

The SNMP community strings are automatically set during the import operation.

**Figure 33** *Devices Imported from HP OpenView*



**Step 7** Click **Next**.

The devices are imported and a status summary appears.

**Step 8** Click **Update** until you see all the devices classified as managed devices.

A constant pending or conflicting state indicates a problem that requires resolution:

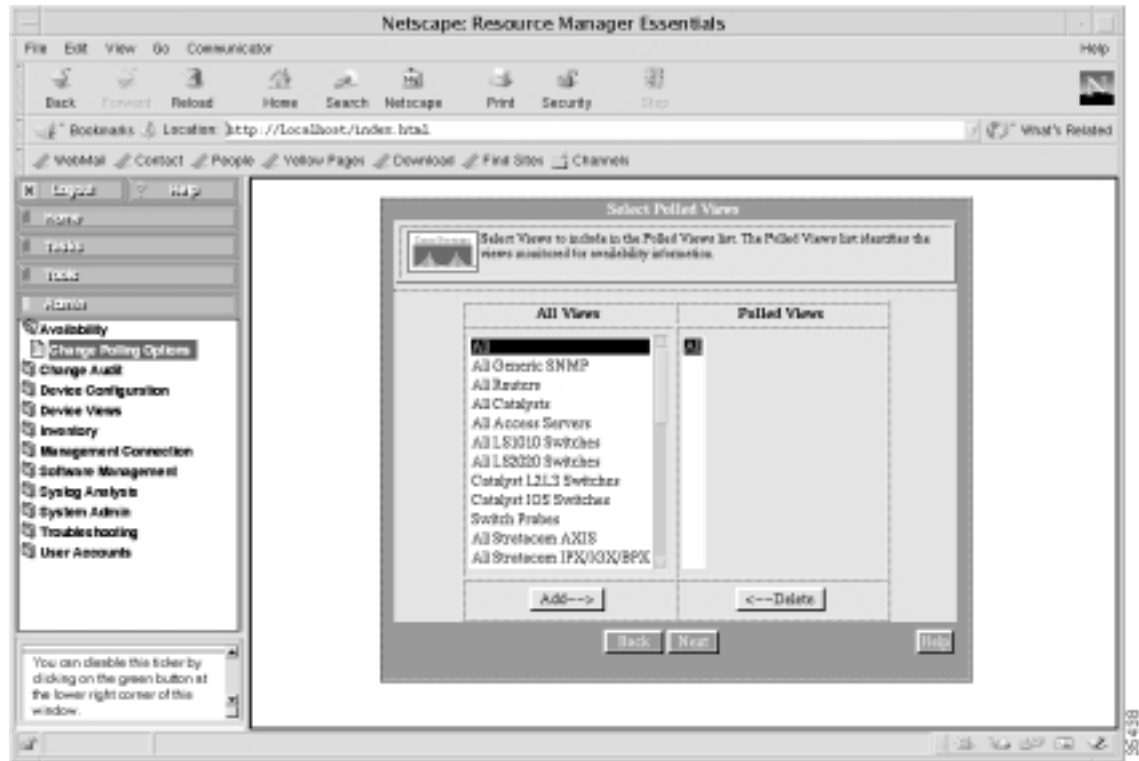
- Inspect the details of the device.
- Verify that the SNMP community strings are correct.

## Verifying that Device Polling is Turned On

To verify that polling is enabled or to alter any polling settings, follow these steps.

- Step 1** From the **Admin** menu, click on **Availability: Change Polling Options**.
- Step 2** In the Select Polled Views screen, select **All Views** and **All Polled Views**.

**Figure 34** Polling Setup



- Step 3** Click **Next**.
- Step 4** To accept the default settings, click **Finish**.

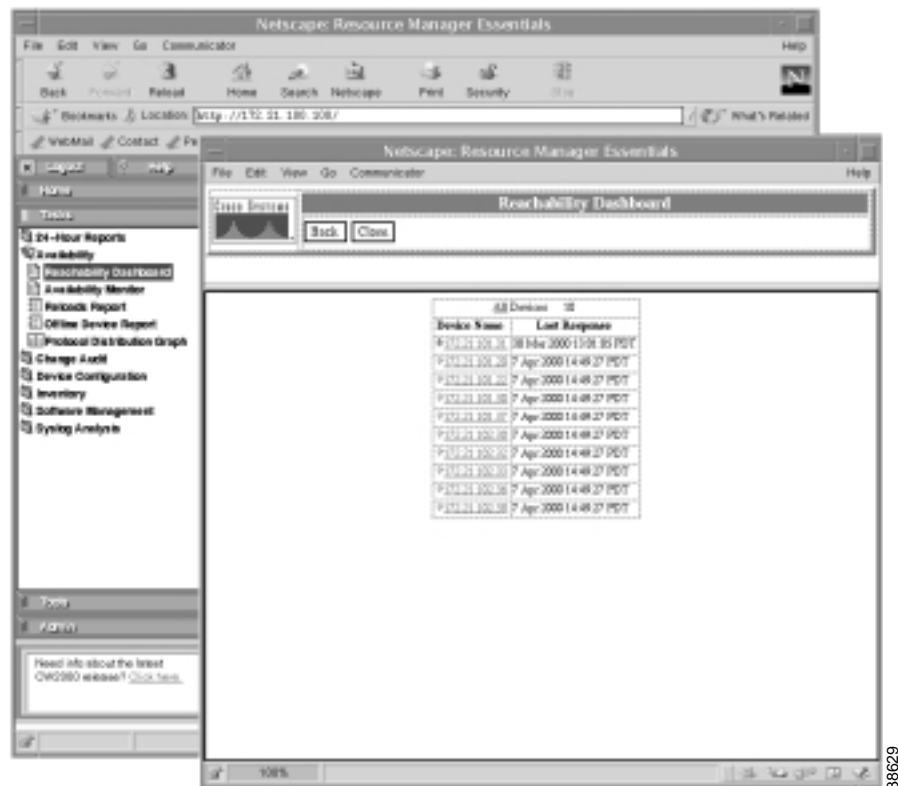


## Polling the Devices

To inspect the status and availability of the devices, follow these steps.

- Step 1** From the **Tasks** menu, click on **Availability: Reachability Dashboard**.

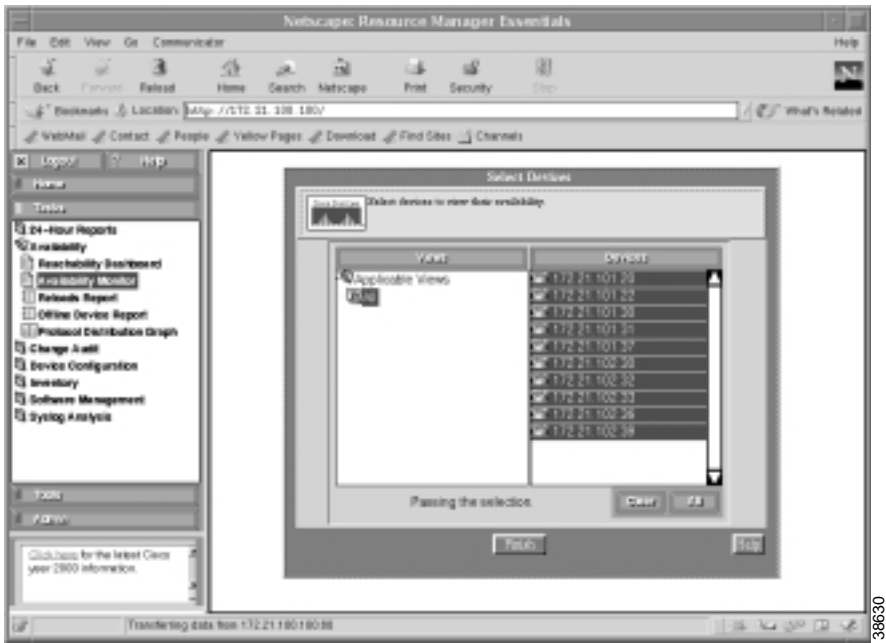
**Figure 35** *The Status of the Devices*



- Step 2** Click a device to become familiar with the different management elements. Green arrows indicate devices that are up. Red arrows indicate devices that are down.
- Step 3** To turn on continuous availability monitoring and reporting, go to the **Tasks** menu. Click on **Availability: Availability Monitor**.

**Step 4** Select **All** in the Views window.

**Figure 36** *Devices Listed in the Availability Monitor*



- Step 5** Select one or more devices.
- Step 6** Click **Finish**.
- Step 7** Inspect the available elements for the devices.

## Backing up Cisco IOS Configurations

Having quick access to archived configuration files reduces network downtime when problems occur.

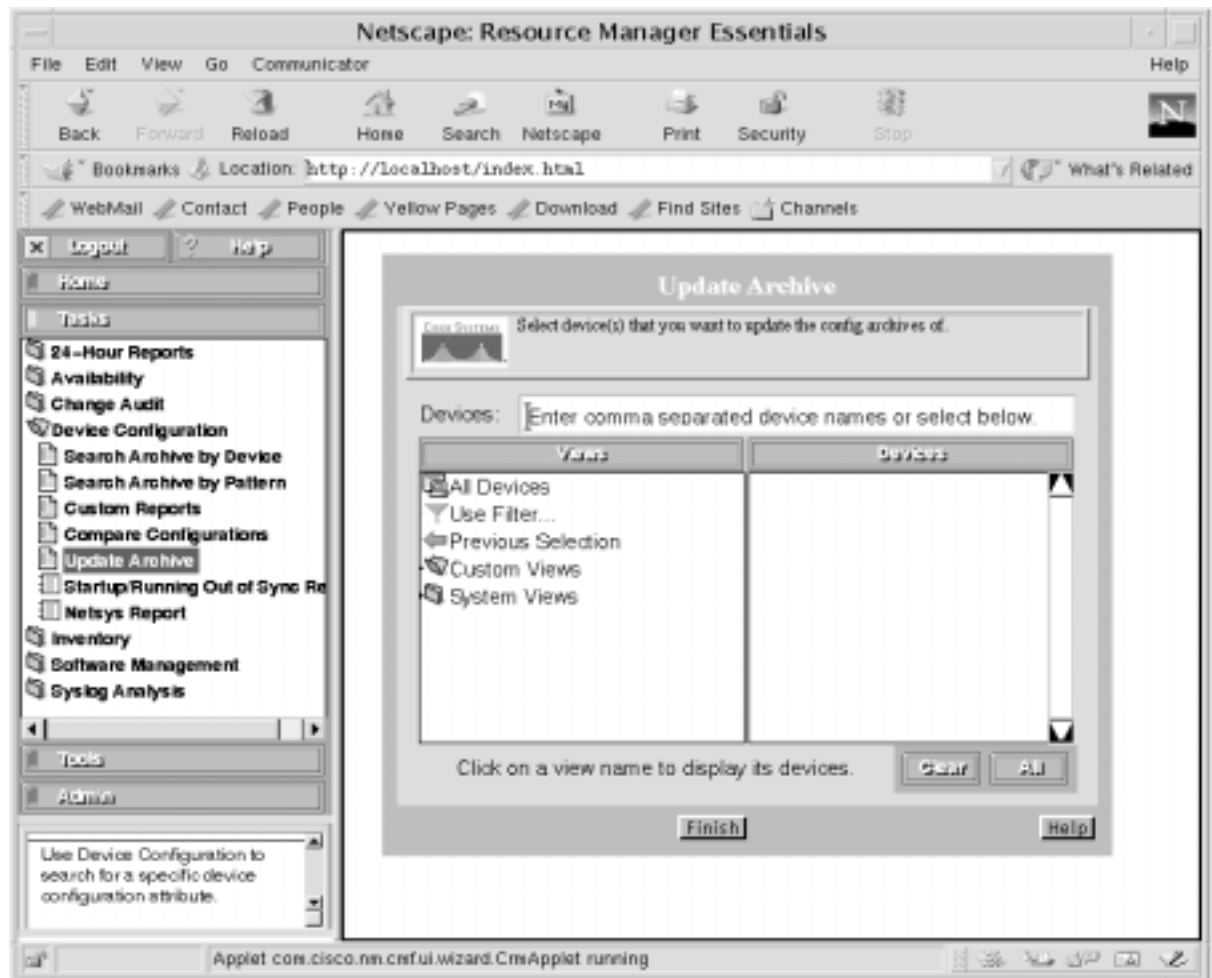


**Note** You can only back up managed devices.

To back up the Cisco IOS start-up configuration files for devices within the network, follow these steps:

- Step 1** From the **Tasks** menu, select **Device Configuration: Update Archive**.

**Figure 37** The Update Archive Screen



- Step 2** Select **All Devices**.

- Step 3** Select one or more devices from the list that appears.

- Step 4** Click **Finish**.

The Cisco IOS start-up configuration file is copied from the router to the Unix workstation.

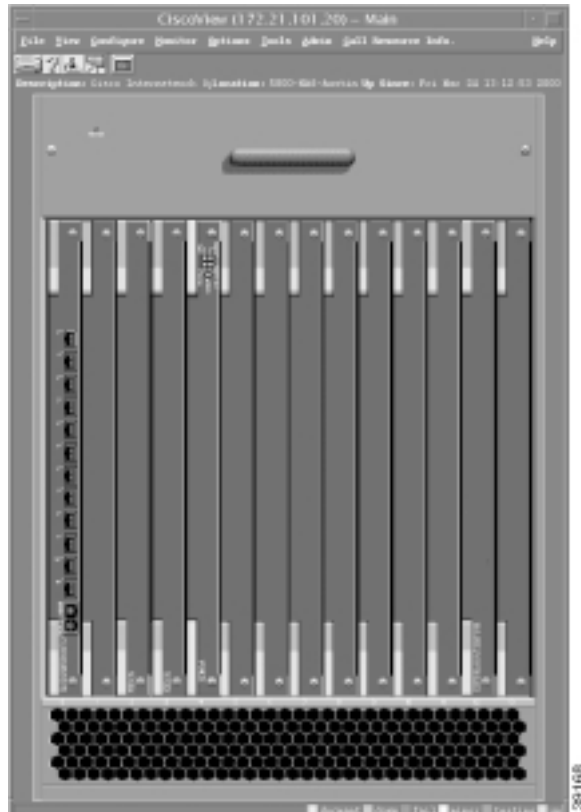
## Using CiscoView

CiscoView is a GUI-based device management software application that lets you access dynamic status, statistics, and comprehensive configuration information for Cisco products.

To inspect device-specific characteristics on different Cisco devices, follow these steps:

- 
- Step 1** From the top-level map in HPOV, select a device.
  - Step 2** Go to **Monitor: CiscoView**.
  - Step 3** Select and view different system components.

**Figure 38** Card Positions in the Cisco AS5800 Dial Shelf



**Figure 39** Available Modems in the Cisco AS5800 Dial Shelf





## INDEX

---

### A

#### AAA

- case study **x**
- CLI commands **27, 28**
- design **27**
- negotiation **57**
- servers **31**

---

### B

- busy hour ratio **31**

---

### C

- capacity planning **31**

#### Cisco 2511 **31**

- setting up **83**

- Cisco 2511, console connection, troubleshooting **85**

#### Cisco AS5300

- MRTG configuration file **60**
- MRTG graphs **57**

#### Cisco AS5800 **31**

#### Cisco IOS CLI Commander **89**

#### Cisco IOS configurations

- HTTP **86**
- modem call records **75**
- NTP **71**
- SNMP **41**
- syslog **67**
- terminal server, Cisco 2511 **85**
- troubleshooting **87**

- Cisco IOS configurations, backing up **123**

#### Cisco Network Registrar

- about **91**
- batch files, using **95**
- CLI commands, using **92**
- forward zone, creating **96**
- reverse zone, creating **99**

#### Cisco PIX **31**

#### CiscoSecure Unix **33**

#### Cisco TAC online **ix**

#### CiscoView **124**

#### CiscoWorks 2000 RME

- about **117**
- configurations, backing up **123**
- design **32**
- devices, importing **118**
- devices, polling **120**

#### clear line command **85**

#### CLI commands for dial operations **27, 38, 87**

#### clocking, NTP configuration **71**

#### clock summer-time command **71**

#### clock timezone command **71**

#### community strings **42**

#### configuration management

- Cisco IOS, backing up **123**
- CiscoView **124**
- CiscoWorks 2000 RME **117**
- CLI commands **87**
- design **27, 28**
- IP addresses, managing **91**
- MIBs to use **37**

#### console server, setting up **83, 85**

#### crontab **63**

---

**D**

- Device Linker, setting up **83**
- dial NMS
  - benefits **24**
  - case study **23**
  - configuration design parameters **33**
  - hardware requirements **31**
  - implementation and operation tasks **35**
  - network topology **30**
  - planning questionnaire **25**
  - service definition **27**
  - software requirements **32**
- dir command **87**
- DNS
  - about **91**
  - IP addresses **91**

---

**F**

- fault management
  - CLI commands **27, 88**
  - description **67**
  - HP OpenView, using **101**
  - syslog and NTP, configuring **69**
- FCAPS **27**
- freeware
  - Cisco IOS CLI Command Center **86**
  - IP tracker web page **96**
  - Modem Call Record Viewer **70**
  - MRTG **53**
  - SNMP Commander **49**
  - UCD-SNMP **45**
- FTP
  - MIBs **46**
  - syslog messages **78**

---

**H**

- hardware for a dial NMS **30**
  - HP OpenView
    - about **101**
    - basic setup **102**
    - CLI, entering devices **115**
    - color legend **106, 110**
    - design **32**
    - devices, entering **115**
    - dial ports, unmanaging **110**
    - discovery filters
      - about **112**
      - setting up **113**
    - filters, setting up **112**
    - get requests, testing **107**
    - maps, adjusting **111**
    - polling devices
      - about **105**
      - demand polls, performing **105**
    - SNMP, troubleshooting **108**
    - SNMP configuration, verifying **102**
    - sysobjectID **106**
    - traps, verifying **108**
    - web site **102**
  - HTTP
    - access to CLI commands, using **86**
- 
- implemenation tasks for a dial NMS **35**
  - interface loopback command **42**
  - interfaces
    - capacity planning **31**
    - unmanaging **110**
  - IOS, See Cisco IOS **41**
  - IP addresses, managing **91, 96**
  - IP design **33, 34**
  - ip http authentication aaa command **86**



ip http server command 86

## L

line requirements 31  
loadhosts -m command 115  
logging, See syslog 67  
logging buffered command 75  
logging command 75  
logging console command 75  
logging facility command 75  
logging trap command 75  
loopback address 34

## M

### MIBs

about 16  
downloading from Cisco 46  
exploring by using UCD-SNMP 45  
ftp.cisco.com 46  
new dial features 38  
OIDs for MRTG 54  
recommended for the dial NMS 37

### modem call records

about 69  
Cisco IOS configuration 75

### modems

call records 70, 75  
modulation trends 69  
OIDs to poll 55

### MRTG

configuration files, editing 59, 60  
design 32  
dial counters 54, 59  
electronic template 60  
functions 53  
installing 59

OIDs to poll 54

web site 59

## N

network topology, dial NMS 30

### NTP

about 69  
client, setting up 72  
client, troubleshooting 74  
enabling on a Cisco IOS device 71  
verifying 71

ntp clock-period command 71

ntpq -p command 73

ntp server command 71

ntp update-calendar command 71

## O

### OIDs 38

circuit utilization 54  
description 16  
modem information 54  
user information 54

OpenView, See HP OpenView 101

operation tasks for a dial NMS 35

out-of-band console 83

ovstatus command 102, 115

ovstop command 115

ovw& command 102

## P

### performance management

CLI commands 27, 29  
Connection Success Rate 57  
OIDs to query 54

planning questionnaire 25

## polling devices

CiscoWorks 2000 RME 120

warnings 37, 54

portal, for a dial NMS 81

PPP 57, 69

PRI lines 31

ps -elf command 77

---

**R**RADIUS design 26, 29

---

**S**

## security management

AAA case study x

CLI commands 27, 29

for IP networks x

HTTP 86

incident tracking 69

SNMP 21

service definition 27

service timestamps command 71

show caller command 39, 88

show controllers t1 call-counters command 38

show dialer command 88

show file systems command 87

show flash command 87

show ip interface brief command 87

show ip route command 87

show isdn history command 40

show isdn memory command 38

show isdn service command 87

show isdn status command 87

show logging command 74

show modem call-stats command 88

show modem command 39, 88

show modem connect-speeds command 39

show modem summary command 38

show modem version command 87

show ntp association command 72

show ntp status command 71

show users command 85, 88

## SNMP

about 13

agent 14

community strings 42

enabling in a Cisco IOS device 41

FAQ 14

managed devices 14

management 20

message types and commands 15

MIBs 16

NMS 14

security 21

SNMPv1 18

SNMPv2 19

TAC support 14

trap link status events, disabling 76

using HP OpenView 102

using MRTG 53

## SNMP Commander

about 49

setting up 49

snmp host command 42

snmp-server community command 42

snmp-server contact command 42

snmp-server enable command 42

snmp-server engineID command 42

snmp-server location command 42

snmp-server packetsize command 42

snmp-server trap-source command 42

software for a dial NMS 32

Solaris workstations 31

subnetting plan 33

## syslog

about 67

- console warnings **75**
- daemon, configuring **76**
- design **30**
- destinations **68**
- enabling on a Cisco IOS device **74**
- link status events, disabling **76**
- log file, inspecting **78**
- server **68**
- severity levels **68**
- WAN links **31**

---

## T

- T3 cards **31**
- TACACS+ design **26, 29**
- tail -f command **78**
- terminal server, setting up **83**
- topology
  - NOC **30**
  - POP **30**
- touch command **77**
- troubleshooting
  - HP OpenView **108**
  - terminal server **85**
  - using modem call records **69, 75**
  - using NTP **69**
  - using syslog **69**

---

## U

- UCD-SNMP
  - about **45**
  - design **32**
  - downloading MIBs **46**
  - installing **46**
  - MIBs for dial, exploring **46**
  - web-based access, setting up **49**
  - web site **46**

- Unix workstations **31**
- user-growth projections **25, 31**
- user IDs **69**

---

## W

- War Dialer **33**
- web server, setting up **64**

---

## X

- xntpd command **73**

