This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the Product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable license for the Product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of any product referenced in the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2008 CA. All rights reserved.
CA Product References

This document may reference the following CA products:

- CA eHealth® AdvantEDGE View
- CA eHealth® Application Response
- CA eHealth® Business Service Console (eHealth BSC)
- CA eHealth® Distributed eHealth
- CA eHealth® Fault Manager
- CA eHealth® Live Health® Application
- CA eHealth® Response
- CA eHealth® Service Availability
- CA eHealth® SystemEDGE
- CA eHealth® TrapEXPLODER
- CA eHealth® Voice Quality Monitor (VQM)
- CA eHealth® AIM for Apache
- CA eHealth® AIM for Microsoft Exchange
- CA eHealth® AIM for Microsoft IIS
- CA eHealth® AIM for Microsoft SQL Server
- CA eHealth® AIM for Oracle
- CA Insight AIM for CA eHealth®
- CA Insight™ Database Performance Monitor for Distributed Databases (CA Insight DPM for Distributed Databases)
- CA eHealth® Integration for Alcatel (eHealth - Alcatel)
- CA eHealth® Integration for Cisco IP Solution Center (eHealth - Cisco ISC)
- CA eHealth® Integration for Cisco WAN Manager (eHealth - Cisco WAN Manager)
- CA eHealth® Integration for HP OpenView (eHealth - OpenView)
- CA eHealth® Integration for Lucent (eHealth - Lucent)
- CA eHealth® Integration for Netcool (eHealth - Netcool)
- CA eHealth® Integration for Nortel Preside (eHealth - Nortel Preside)
- CA eHealth® Integration for Nortel Shasta SCS GGSN (eHealth - Nortel GGSN)
- CA eHealth® Integration for Psytechnics (eHealth - Psytechnics)
CA eHealth® Integration for Starent PDSN (eHealth - Starent PDSN)

CA SPECTRUM®

CA Unicenter® Network and Systems Management (Unicenter NSM)

CA eTrust® Identity and Access Management (eTrust IAM)

CA Embedded Entitlements Manager (CA EEM)

**Note:** CA Embedded Entitlements Manager (CA EEM) is the new name for eTrust IAM. This product will be rebranded throughout the documentation in a future release.

CA XOsoft™ Replication

---

**Contact CA**

**Contact Technical Support**

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at [http://ca.com/support](http://ca.com/support).

**Provide Feedback**

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, please complete our short [customer survey](http://ca.com/support), which is also available on the CA Support website.
# Contents

## Chapter 1: Introducing eHealth

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>Network Management</td>
<td>9</td>
</tr>
<tr>
<td>Systems and Application Management</td>
<td>10</td>
</tr>
<tr>
<td>Application Performance Management</td>
<td>11</td>
</tr>
<tr>
<td>End-to-End Infrastructure Management</td>
<td>11</td>
</tr>
<tr>
<td>eHealth Products and Components</td>
<td>12</td>
</tr>
<tr>
<td>eHealth AdvantEDGE View</td>
<td>12</td>
</tr>
<tr>
<td>Distributed eHealth</td>
<td>13</td>
</tr>
<tr>
<td>Integration Modules</td>
<td>14</td>
</tr>
<tr>
<td>Live Health</td>
<td>15</td>
</tr>
<tr>
<td>Remote Polling</td>
<td>15</td>
</tr>
<tr>
<td>Technology Keys</td>
<td>16</td>
</tr>
<tr>
<td>Traffic Accountant</td>
<td>16</td>
</tr>
</tbody>
</table>

## Chapter 2: Working with eHealth

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection</td>
<td>19</td>
</tr>
<tr>
<td>Data Collection Agents</td>
<td>20</td>
</tr>
<tr>
<td>Data Storage</td>
<td>27</td>
</tr>
<tr>
<td>Report Generation</td>
<td>27</td>
</tr>
<tr>
<td>Data Analysis</td>
<td>28</td>
</tr>
</tbody>
</table>

## Chapter 3: Administration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Discovery</td>
<td>31</td>
</tr>
<tr>
<td>Element Creation</td>
<td>32</td>
</tr>
<tr>
<td>Data Collection Maintenance</td>
<td>33</td>
</tr>
<tr>
<td>Discovered Elements and the eHealth Poller</td>
<td>33</td>
</tr>
<tr>
<td>Maintenance of Poller Configuration</td>
<td>33</td>
</tr>
<tr>
<td>Report Management</td>
<td>34</td>
</tr>
<tr>
<td>System Processes Management</td>
<td>34</td>
</tr>
<tr>
<td>Database Management</td>
<td>35</td>
</tr>
<tr>
<td>Capacity Planning</td>
<td>35</td>
</tr>
<tr>
<td>Underutilized Resources</td>
<td>35</td>
</tr>
<tr>
<td>Overutilized Resources</td>
<td>38</td>
</tr>
<tr>
<td>Planning for Future Capacity</td>
<td>41</td>
</tr>
<tr>
<td>Maintenance</td>
<td>43</td>
</tr>
</tbody>
</table>
Advanced Logging ................................................................. 43
Upgrades ............................................................................ 43
Service Packs ..................................................................... 44

Chapter 4: Reports ................................................................. 45
About Historical Data .......................................................... 45
Standard Reports .................................................................. 46
  Trend Reports .................................................................... 46
  At-a-Glance Reports ............................................................ 46
  Top N Reports .................................................................... 46
  What-If Reports ................................................................ 47
Historical Analysis Reports ...................................................... 47
  Health Reports .................................................................... 47
  Service Level Reports ............................................................ 48
  Scheduling Health and Service Level Reports ....................... 48
Drill-Down Reports ............................................................... 48
MyHealth Reports ................................................................. 49
Report Center ....................................................................... 49
  Customization Features .......................................................... 50
  User Roles .......................................................................... 51
  Applications ........................................................................ 51
  Sample Reports .................................................................... 52
  Common Report Center Tasks ................................................. 56

Chapter 5: Managing Fault and Performance ........................................ 57
Faults and Performance ............................................................. 57
  Fault Management ................................................................. 57
  Performance Management ....................................................... 57
  Real-Time Data .................................................................... 58
Business Service Console ........................................................... 58
Live Health Overview ................................................................. 59
  How Live Health Works ......................................................... 59
  Live Status ........................................................................... 60
  Live Exceptions ................................................................... 61
  Live Trend ............................................................................ 71
  Live Health Fault Manager ....................................................... 72
Case Study: Keeping Customers by Maximizing Uptime ....................... 72

Chapter 6: Traffic Accountant ...................................................... 75
Introduction to Traffic Accountant ................................................ 75
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP Executive Report</td>
<td>103</td>
</tr>
<tr>
<td>VoIP Service Customer Report</td>
<td>105</td>
</tr>
<tr>
<td>VoIP IT Manager Report</td>
<td>106</td>
</tr>
<tr>
<td>At-a-Glance Reports for VoIP</td>
<td>106</td>
</tr>
<tr>
<td>Trend and Top N Reports for VoIP</td>
<td>106</td>
</tr>
<tr>
<td>Quality of Service (QoS) Reports</td>
<td>107</td>
</tr>
<tr>
<td>Reports for Voice Quality with Cisco SA</td>
<td>107</td>
</tr>
<tr>
<td>Additional Queries for VoIP Components</td>
<td>108</td>
</tr>
</tbody>
</table>

**Glossary** 109

**Index** 125
Chapter 1: Introducing eHealth

This section contains the following topics:

Introduction (see page 9)
Network Management (see page 9)
Systems and Application Management (see page 10)
Application Performance Management (see page 11)
End-to-End Infrastructure Management (see page 11)
eHealth Products and Components (see page 12)

Introduction

To help you manage the end-to-end performance and availability of your Information Technology (IT) infrastructure, the eHealth suite offers solutions for the following areas:

- Network management
- System and application management
- Application performance management
- End-to-end infrastructure management

Each solution integrates relevant components of the eHealth suite to provide a comprehensive answer to your IT needs. This chapter provides a brief overview of these solutions.

Network Management

When you manage and maintain a network, you keep track of every router, switch, and other network components. You also monitor the performance of the network to determine the percentage of time the network components are available, whether the current network bandwidth is sufficient, and whether network traffic is increasing over time.

eHealth delivers integrated and proactive fault, performance, and availability management across complex, heterogeneous IT environments. With eHealth, you can do the following:

- Manage multiple IT platforms and architectures.
- Manage critical network services.
- Achieve integrated fault and performance management.
Systems and Application Management

- Perform intelligent capacity planning.
- Manage and document service levels.

eHealth collects a wide variety of data from your network infrastructure to generate alarms and reports.

**Systems and Application Management**

Besides monitoring network components, you need to make sure the systems and applications that form the underlying framework of your infrastructure can support your business. If critical systems are unavailable, or key applications (such as email, Web servers, and database management systems) perform poorly, user productivity declines.

eHealth provides integrated fault, performance, and availability management across complex, heterogeneous systems and applications environments. By automatically detecting, isolating, and correcting problems, eHealth helps improve the availability and performance of systems and applications, resulting in improved user productivity.

With eHealth, you can do the following:

- Manage multi-platform systems.
- Manage infrastructure applications.
- Manage internally developed applications.
- Receive immediate notification of service outages.
- Lower IT costs with management by exception.
- Map IT to the business.
- Track hardware and software assets.

The systems and applications that you can monitor and manage using eHealth include the following:

- Servers
- Desktops
- Web servers
Application Performance Management

When business applications perform slowly, user productivity declines and business is affected. To ensure maximum performance, you need to be able to monitor the application response times and availability that end users experience.

eHealth lets you measure and monitor actual end-user application response time for commercial or custom Windows or Web applications that are TCP/IP-based. It also helps you understand application availability through a synthetic (test) approach from anywhere in the world. With this information, you can help ensure that business-critical applications are available and performing well so that users and your customers function effectively.

With eHealth, you can do the following:

- Monitor and manage the response times of business-critical applications and individual transactions.
- Receive alarms based on custom thresholds for end-user response performance and application availability.
- Enhance troubleshooting by drilling down from real-time alarms to historical application performance reports.
- Provide reports for capacity planning and service level documentation.

End-to-End Infrastructure Management

The health and well-being of the entire IT infrastructure depends upon the performance of all the business resources: applications, systems, and networks.

eHealth provides integrated and proactive fault, performance, and availability management across applications, systems, and networks. It increases your quality of service by reducing the mean time to repair (MTTR), lowers cost of ownership, and provides automated service level management.
eHealth offers the following:
- Network management
- Application response management
- Multi-platform systems management
- Integrated fault and performance management
- Immediate notification of service outages
- Capacity planning and service level management
- Infrastructure applications management

eHealth can provide a single, integrated view of the health of your entire IT infrastructure, including networks, systems, and applications, to do the following:
- Identify trouble spots from personalized business views.
- Monitor network devices, systems, and response paths.
- Provide automatic assessment of impact by customer, regions, and technologies.

eHealth Products and Components

The eHealth suite includes the following products and components:
- eHealth AdvantEDGE View
- Distributed eHealth
- Integration Modules
- Live Health
- Remote Polling
- Technology Keys
- Traffic Accountant

eHealth AdvantEDGE View

eHealth AdvantEDGE View is the Web-based graphical user interface and element manager for use with SystemEDGE agents. Because it is Web-based, you can access eHealth AdvantEDGE View from any location using a standard Web browser.
You can use eHealth AdvantEDGE View to do the following:

- Determine the real-time status of critical systems and applications.
- Access configuration and performance information across groups or individual systems.
- Configure, license, and define actions for SystemEDGE agents.
- Receive and process event notifications (traps) originating from SystemEDGE agents.
- Deploy SystemEDGE agents, AIMs, and AR agents to Windows systems.

With eHealth AdvantEDGE View, you can logically group systems to reflect the way your business operates, such as by business function, geographic location, or system type. After you define groups, eHealth AdvantEDGE View configures and queries entire groups of systems at one time. You can set management policies and performance thresholds for groups of systems.

You can also search through systems to find the precise data that you need, answering questions such as the following:

- Which file systems are more than 75 percent full?
- Which systems have been upgraded with the new operating system (OS) patch?

eHealth AdvantEDGE View provides queries for the following types of information:

- Configuration
- Performance
- Network
- Services

You can use eHealth AdvantEDGE View and SystemEDGE separately or with eHealth for integrated performance and availability management across your infrastructure.

**Note:** For more information about eHealth AdvantEDGE View, see the online help. For more information about SystemEDGE agents, see the *SystemEDGE User Guide*.

### Distributed eHealth

Distributed eHealth is a highly scalable solution for managing large infrastructures using a single integrated view across multiple eHealth systems. It lets you monitor and manage up to one million elements across a worldwide network.
With Distributed eHealth, you can deploy multiple Distributed eHealth Systems that gather data and provide local management on various segments of your network. You can deploy these systems remotely across large geographic ranges or locate them centrally. You connect the Distributed eHealth Systems in a configuration referred to as a cluster. In addition to providing local management, these clustered Distributed eHealth Systems are also responsible for processing requests from the Distributed eHealth Console.

The Distributed eHealth Console is the reporting front end from which users access their distributed reports. It has knowledge of and access to data that resides on any or all of the Distributed eHealth Systems. When you request a report that contains elements managed by one or more Distributed eHealth Systems, the systems process their specific data in parallel and then send it to the Distributed eHealth Console, which collates the data into a single report. This architecture distributes the workload of collecting and processing data across multiple systems that work in parallel.

Through a single Web access point, one or more report users can access critical information across several systems spread over multiple worldwide geographical locations. This integrated single point of access to current and historical data significantly enhances the ability to detect and isolate current and potential problems across your infrastructure.

**Note:** For more information, see the *Distributed eHealth Administration Guide*.

**Integration Modules**

Integration modules help eHealth do either or both of the following:

- Import configuration and performance data about network components from other software solutions. This data is then used by eHealth reports and Live Health.

- Export intelligent alarms from Live Health to network management systems, letting Network Operations Center (NOC) administrators troubleshoot problems using the workflow with which they are familiar. In some cases, administrators can drill down from the network management system to eHealth reports to investigate the source of an alarm.

Integration modules let you obtain as much information as possible about the performance and availability of your network and view it all in one place.

A current list of integration modules is available at [http://support.ca.com](http://support.ca.com).

**Note:** For more information about using the integration modules, see the guides for specific modules.
Live Health

Live Health is a software solution that provides real-time fault, performance, and availability management for any of the eHealth components that you have purchased. When used with all components, Live Health provides real-time management capabilities across your entire IT infrastructure. It monitors your network, systems, and applications to detect faults, potential outages, and delays that can cause downtime and service degradation.

Live Health’s embedded intelligence and natural alarm consolidation ensure that existing human resources are applied as efficiently and effectively as possible. It alerts IT staff to faults and potential outages with more precision and less noise (redundant alarms with little meaning or value), letting them quickly identify and resolve performance problems.

**Note:** For more information about Live Health, see Live Health Overview and the *eHealth Help*.

Remote Polling

As an alternative to Distributed eHealth, you can use a remote polling environment. With remote polling, you install eHealth on remote systems (called remote sites) and set up each site to poll a set of elements. The database at each site contains data for the elements it is polling, and you can manage those elements using eHealth. A central eHealth system retrieves information and performance data from the remote eHealth systems and periodically merges the data into one central eHealth database. From this central database, you can run reports for all elements. The central site can support up to 80,000 elements, depending on the system configuration and the reports that you run.

You may choose to implement remote polling instead of Distributed eHealth for security or logistics reasons. For security, you can prevent each remote polling site from having knowledge of other sites. A remote poller shares its data *only* with the central site—not with any other remote pollers. (In a Distributed eHealth environment, Distributed eHealth Systems share information such as group and group list names with one another, and administrators can run commands that affect all cluster members.) Remote pollers can be important for service providers or large corporations with separate divisions. For logistics purposes, remote polling can assist with infrastructures that consist of multiple subnetworks that are connected using intermittent or dial-up links. (With Distributed eHealth, the interfaces that connect eHealth systems must support communications traffic between cluster members.)
You can combine remote polling with Distributed eHealth to gain the advantages of each. For example, a Distributed eHealth System can be a central site that collects data from several polling sites. In this way, you can segregate some systems from knowledge of each other but still have a way to perform distributed reporting. Segregating systems can be important for service providers that need to isolate customers from one another or for a large parent corporation that needs to keep its divisions separate.

**Note:** For more information about remote polling, see the *Administration Guide*.

### Technology Keys

Since every IT infrastructure is different, eHealth is designed to be flexible enough to meet the needs of small, medium, and large enterprises as well as the needs of service providers. To meet your specific needs, eHealth offers technology keys or license keys. Most of these keys are included in the End-to-End Console License; certain technology keys must be obtained individually.

**Note:** Out of the box, eHealth can discover and poll elements without a license.

Each technology key helps you collect and report on performance data for a particular part of your infrastructure and to integrate that data with other components of eHealth.

Based on the technology keys in use, eHealth collects data from the appropriate parts of your infrastructure at user-defined intervals and stores it in the eHealth database. It establishes a baseline of performance to document normal behavior and informs you when conditions are deteriorating.

When eHealth collects data from these technologies and displays it in reports, you can use the information to perform capacity planning, troubleshoot potential problems, and manage the overall quality of service delivered to users. In most cases, you can report on this data using standard eHealth reports, Service Level reports, and Health reports, or you can direct dataLive Health for real-time analysis.

**Note:** For more information about licensing, see the *Installation Guide*. For more information about technology keys, see Technology Keys and the online help.

### Traffic Accountant

Traffic Accountant is an eHealth product that provides network traffic analysis and reporting for use with RMON2 probes and Cisco NetFlow.
You can use Traffic Accountant to document which individual users and departments are consuming the most network resources. Using this information, you can relate network costs to departments based on their usage levels.

Traffic Accountant also provides insight on trends and usage patterns that impact the performance of your network to help you match your network resources to the needs of the user and the demands of the application.

**Note:** For more information about Traffic Accountant, see Traffic Accountant and the *Traffic Accountant Administration Guide*. 
Data Collection

Your IT infrastructure consists of hundreds, even thousands of *elements*, such as applications, servers, clients, routers, modems, hubs, switches, ISDN interfaces, RAS devices, and more. As a system for monitoring the performance and availability of your infrastructure, eHealth must have a way to gather information about those elements.

eHealth can monitor the performance of a physical element, such as a specific port on a specific card of a specific router. It can also monitor a logical element, which refers to the logical purpose for a device or component, such as a network link between Boston and Chicago. This logical element does not specify which network devices are used to form the link; instead, it involves the logical connection itself.

When setting up the software, an eHealth administrator begins by identifying the elements to monitor for performance and availability. The administrator can specify the elements to monitor using the following methods:

**Discover**

- eHealth provides a special process, called the `discover` process, to search your network for devices with SNMP agents at the IP addresses you specify.

**Import**

- If your organization uses an inventory system, a provisioning system, or a network management system (NMS) that maintains information about network resources, you may be able to import the element information into eHealth.

**Auto-register**

- The agents for some eHealth components register automatically with eHealth when they begin monitoring.
After it knows which elements to monitor, eHealth collects performance data about those elements on a regular basis. eHealth can collect data using the following methods:

**Poll**
In many cases, eHealth collects performance and availability data about an element from an SNMP agent. At scheduled intervals, a special process called the *eHealth poller* asks an element’s SNMP agent for its performance data, and the agent responds with the current values.

**Import**
In some cases, eHealth can import performance data from a network management system at regular intervals.

**Push**
eHealth Application Response uses a special process to send (push) performance data to the eHealth database at regular intervals.

**Send Traps**
You can configure SNMP agents to send traps to eHealth when certain events occur. Live Exceptions analyzes this data to generate alarms.

### Data Collection Agents

eHealth uses the following agents to collect data about your infrastructure to provide the information that you need for troubleshooting, analysis, and planning:

- SNMP agents
- Unicenter Network and Systems Management (NSM) agents
- eHealth SystemEDGE agents
- eHealth Application Response agents
- Cisco IOS IP Service Level Agreements (SLAs)
- Juniper real-time performance monitoring (RPM)

**Note:** Cisco IOS IP SLA was previously named the Cisco Service Assurance agent (SAA).

### SNMP Agents

To monitor the network, eHealth relies on SNMP agents embedded in the network devices that you want to monitor. eHealth discovers these devices through SNMP, polls the statistics collected by each device’s MIB at user-defined intervals, and collects the information into a database. eHealth establishes a baseline of network performance to document normal behavior for the devices and informs you when conditions are deteriorating.
eHealth supports more than 500 devices from over 70 leading vendors. For a list of devices with SNMP agents certified to work with eHealth, see http://support.concord.com/devices.

**NSM Agents**

Network and Systems Management (NSM) agents monitor your critical business systems, helping you to check for consistent performance and enhance system management.

You can use the eHealth suite of software to supplement the robust performance reporting available with NSM. Together, eHealth and NSM provide you with the ability to perform trend analysis, capacity planning, and proactive, real-time self-management. When you combine these products with eHealth Live Health, you can also generate alarms when system performance is outside the service thresholds that you define.

**SystemEDGE Agents**

The eHealth SystemEDGE agent operates autonomously. It lets you offload the task of routine system monitoring from IT personnel to the systems where problems occur. You can use SystemEDGE as a stand-alone solution to monitor critical systems and applications or you can use it as part of an integrated eHealth solution.
With SystemEDGE, you can manage your heterogeneous mix of operating systems in a single, homogeneous manner, so you do not need a separate IT expert for each operating system in use. SystemEDGE operates on a client or server system, continuously monitoring changing conditions and providing detailed information about the system’s configuration, status, performance, users, applications, file systems, and other critical resources.

SystemEDGE includes the following features:

**Automatic Notification and Action**

The SystemEDGE agent can monitor exception conditions automatically, reducing or eliminating the need for constant polling by a network management system. When SystemEDGE detects a problem, it can automatically notify appropriate personnel or fix the problem with actions that you specify.

For example, when you install SystemEDGE on a Web server, it can do the following:

- Monitor system CPU, memory, and file system space and notify you if the system begins to run out of resources.
- Monitor the Web server daemon process to detect failures and automatically restart the process when it fails.
- Monitor Web server log files for important information (such as Common Gateway Interface [CGI] errors, which can indicate attempts to compromise system security or poor performance of the Web site) and send an SNMP trap to a network management system.

**Top Processes**

SystemEDGE offers a feature called Top Processes, which lets the agent report on processes that are consuming the most CPU resources at any time. With instantaneous detection and isolation of CPU-dominating processes, you can immediately reallocate resources to help ensure high application availability and optimal performance.

**Asset Tracking**

SystemEDGE also helps automate asset tracking, providing an up-to-date picture of your installed hardware and software. With SystemEDGE, you can determine whether your systems are properly configured and whether operating systems have current patches and service packs. This information can help simplify system management, improve performance, and reduce security risks.
Integration and Small Footprint

As an SNMP agent, SystemEDGE can provide data to eHealth and network management systems such as HP OpenView or Micromuse Netcool. It uses less than one percent of the CPU and about three MB of memory. This small footprint means that you can install SystemEDGE agents on server and client computers without affecting performance.

Scalability

By automating system management with SystemEDGE, IT organizations can scale to managing hundreds or thousands of systems without increasing staff. SystemEDGE lets you fix problems before they affect users while reducing the work load of IT personnel.

You can deploy, license, and manage SystemEDGE agents with eHealth AdvantEDGE View, a graphical user interface and element manager.

To extend the monitoring capabilities of SystemEDGE to include business-critical applications and services, eHealth offers the following plug-in modules:

- Application insight modules
- Service Availability

Note: For more information about SystemEDGE agents, see the SystemEDGE User Guide.
**Application Insight Modules (AIMs)**

eHealth application insight modules (AIMs) are application-specific plug-in components for the SystemEDGE agent. With AIMs, SystemEDGE can provide more detailed monitoring and management of business-critical applications that reside on the target system.

AIMs help you do the following:

- Detect and correct performance problems with mission-critical applications in real-time
- Help ensure sufficient system resources for these applications
- Track usage statistics for the applications
- Monitor AIM effect on critical system resources
- Determine application configuration information (for use in fine-tuning performance or to train new IT personnel)

eHealth offers a variety of AIMs for SystemEDGE to manage specific applications, such as email, web servers, databases, network services, and voice.

AIMs can be used with SystemEDGE agents as a stand-alone solution or with eHealth as part of an end-to-end solution.

**Service Availability**

eHealth Service Availability is a plug-in module for the SystemEDGE agent. It manages and monitors response time and availability of the following Internet services:

- Hypertext Transfer Protocol (HTTP)
- Secure HTTP (HTTPS)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP3)
- Domain Name System (DNS)
- Network News Transfer Protocol (NNTP)
- File Transfer Protocol (FTP)
- Packet internetwork groper (PING)
- TCP-connect
- Active Directory
- Dynamic Host Configuration Protocol (DHCP)
- File I/O
Data Collection

- Internet Message Access Protocol (IMAP)
- Lightweight Directory Access Protocol (LDAP)
- Messaging Application Programming Interface (MAPI)
- Network Information Service (NIS)
- Simple Network Management Protocol (SNMP)
- SQL Query
- Trivial File Transfer Protocol (TFTP)
- Virtual User
- Generic
- Custom

Service Availability also helps you create custom scripts and programs to define service tests for additional services. After you create the custom script or program, you can use it to measure availability from any system within the network.

**eHealth Application Response Agents**

eHealth Application Response measures actual, observed response time from the end user’s point-of-view. With eHealth Application Response, you can do the following:

- Understand how applications are currently performing by measuring average response time for each application (including terminal server applications) as well as response times for individual transactions and groups of transactions.
- Learn which user groups are experiencing slow application performance and understand why.
- Manage service levels proactively and perform capacity planning.

To gather application response data, you install eHealth Application Response agents on Windows-based client systems or terminal servers (such as servers for Citrix MetaFrame or Microsoft Windows Terminal Services). These agents measure the actual response times of transactions performed by end users for the monitored applications. The agents then aggregate this data into an average response time for each application. eHealth Application Response can also track response times for individual transactions and groups of transactions.
The eHealth Application Response agents regularly send the application response time data, along with other aggregated data, to eHealth. eHealth stores this data in the database and uses the data in reports. eHealth Live Health also uses the response data to generate real-time alarms when response time exceeds defined thresholds for applications.

When you identify an application response time problem, you can use Agent Transaction Viewer (ATV) to obtain more details about transactions. The ATV is helpful in troubleshooting and diagnosing application response time problems. You can run the ATV from the eHealth Web interface or drill down to it from Trend reports and Live Health.

Cisco IOS IP SLAs

With the increasing importance of mission-critical applications and networks that link global enterprises, customers want service level agreements (SLAs) that guarantee minimum acceptable levels of service. Cisco IOS IP SLAs (previously called Cisco SAA) provide a reliable mechanism to accurately measure and monitor important metrics to ensure a high quality of network service.

Cisco IP SLA is bundled with equipment from Cisco Systems, Inc. This agent enhances the management and measurement of enterprise and service provider networks by testing service and response from Cisco routers to critical resources.

When you configure Cisco IP SLA with eHealth, the Cisco router generates traffic to specified network resources, and measures the availability of the resource and response time between the router and that resource. Cisco IP SLA can also measure important metrics such as latency, packet loss, and jitter (the variation in delay between two successive packets in a simulated real-time voice or video data flow). These metrics are then stored in the eHealth database.

You can use this information to troubleshoot network problems, identify and analyze potential problems before they occur, and design future network topologies. Response data from Cisco IP SLA can appear in the eHealth reports. Live Health also compares the response data with profiles and generates real-time alarms.

Juniper Real-Time Performance Monitoring (RPM)

The Juniper real-time performance monitoring (RPM) feature monitors network performance between a Juniper router and a remote device. RPM sends probes between two network endpoints, and measures performance information including availability, packet response time and jitter. This information lets you perform service level monitoring, troubleshooting, and resource planning.
You use eHealth to configure the Juniper RPM router to generate traffic to critical network resources. The router then actively measures the response time between the router and the resource. These measurements provide detailed data on performance metrics such as availability, round-trip delay, and jitter, providing an accurate view of the quality of service a user experiences.

You can use this information to troubleshoot network problems, identify and analyze potential problems before they occur, and design future network topologies. Response data from Juniper RPM can appear in the eHealth reports and can be used by Live Health to generate real-time alarms.

**Note:** Juniper RPM defines jitter as the difference between the maximum response time and the minimum response time for a group of pings. This jitter measurement may differ from that calculated by other devices.

---

**Data Storage**

When eHealth collects data about the performance of your IT infrastructure (for example, every five minutes), it stores the data in its database. In its raw form, this detailed performance data is called *as-polled data*.

To reduce the amount of data it stores, saving storage capacity, eHealth aggregates the data as it ages. By default, eHealth keeps the most recent three days’ worth of as-polled data in the database. This lets you run detailed reports for today and the previous two days.

When the as-polled data becomes older than three days, eHealth aggregates it into hourly samples and retains that data for several weeks. When the hourly data ages, eHealth aggregates it into daily and weekly samples, retaining that data for many more weeks. You can still run reports using this data, but you will not be able to see the same level of detail that the as-polled data provides.

This process of aggregating data is called *database rollup*. The eHealth administrator can define the database rollup schedule and change the length of time for which eHealth retains as-polled data, as well as the rolled-up hourly, daily, and weekly data, based on the reporting needs of your organization.

---

**Report Generation**

eHealth offers a comprehensive set of reports to provide the information you need to manage your IT infrastructure. You can use each type of report in several ways to show different types of information, depending on the filter criteria that you use to run the report.
To make eHealth reports more meaningful and useful, an eHealth administrator can define *groups* of elements. For example, your organization may decide to organize elements by geographic location, by department or organization, or by customer. You can then run reports for selected groups.

To further organize elements and groups, the eHealth administrator can create *group lists*, which are collections of groups. With group lists you can run a report to show the performance of all the resources of a specified type in all locations (for example, sales in all locations), of all monitored elements in one location, or of the resources located in just one location.

Furthermore, an element can belong to multiple groups and a group can belong to multiple group lists. For example, element XYZ can belong to the Sales group *and* to the Boston group. The Boston group can belong to the Windows group list *and* to the EastCoast group list. As a result, performance data for XYZ can appear in a report showing performance for the Sales group *and* a report for the EastCoast group list. By using groups and group lists, you can report on precisely the elements that interest you.

**Data Analysis**

eHealth lets you run reports on demand or schedule them to run regularly. When you run a report on demand, eHealth analyzes the data while the report runs, which can cause some reports to take a long time to finish. eHealth discards the analysis when it finishes the report.

For some scheduled reports, eHealth preprocesses the data to reduce the amount of time required to generate the report. Every day before running these scheduled reports, eHealth runs a special data analysis process to analyze the previous day’s data. It uses this data to calculate averages, analyze trends, and calculate a health index for each element.

The health index is a poll-by-poll measure of the performance of each element based on various criteria. It appears in certain reports to indicate the health of resources. A high health index indicates problems and a low one indicates a healthy element. eHealth averages the health index for all elements to provide an overall health index for the IT infrastructure.

eHealth also uses trend thresholds to identify problem areas. eHealth analyzes trends to anticipate performance problems. Trend thresholds are upper limits for utilization and error detection that, when reached, indicate a problem. eHealth uses the health index and trend thresholds to evaluate the current status of your IT infrastructure and to identify changes in its condition.
The eHealth administrator can define trend thresholds and the performance ranges used for health indexes, as well as service level ranges, to customize the data analysis process to meet your reporting needs. These policy settings are stored as service profiles, which control how eHealth analyzes the data against which it generates reports.

The data analysis process runs each night to process the previous day’s as-polled data.

Many eHealth reports compare current performance to a baseline, which is typical behavior for that element (or group or group list) based on the past several weeks of performance data. The baseline period is a rolling period that projects back from the day on which the report is run. eHealth reports compare hourly information to the same hour of the day, and daily information to the same day of the week in the baseline period. By default, eHealth uses a baseline period of six weeks for daily reports, 13 weeks for weekly reports, and 12 months for monthly reports.

When you notice significant changes between the baseline and current performance, you can check other graphs and reports to help identify which elements might be responsible for the changes.
Chapter 3: Administration

This section contains the following topics:

- Resource Discovery (see page 31)
- Discovered Elements and the eHealth Poller (see page 33)
- Report Management (see page 34)
- System Processes Management (see page 34)
- Database Management (see page 35)
- Capacity Planning (see page 35)
- Maintenance (see page 43)

Resource Discovery

To monitor and manage the performance of networks, systems, and applications, the eHealth software locates resources, or elements, within your infrastructure and collects data about them. eHealth monitors two types of elements, as follows:

- Statistics elements—devices and interfaces within the network
- Conversation elements—monitor traffic flow among nodes and applications using the network.

Statistics elements include the following:

- Local area network (LAN) and wide area network (WAN) interfaces
- Quality of Service (QoS)
- Routers, their central processing units (CPUs), and interfaces
- Mobile wireless and wireless interfaces
- Systems, their disks, interfaces, partitions, CPUs, and process sets
- Remote access server (RAS) devices, modem pools, modems, and Integrated Services Digital Network (ISDN) interfaces
- Application services and their process sets
- Response sources, destinations, and paths
- Synchronous Optical Network (SONET) interfaces
- Storage area networks (SANs)
- Digital subscriber line (DSL) interfaces and cable modems
- Voice over IP (VoIP) features such as call managers, voice line quality, and services
Conversations elements include devices that use Remote Network Monitoring version 2 (RMON2) or similar agents to monitor traffic, and Cisco NetFlow collectors.

**Note:** For more information about administration, see the *Administration Guide*.

### Element Creation

*Discovery* is the process of locating your resources and creating elements for them. To find the resources, eHealth uses Simple Network Management Protocol (SNMP) to search for agents at the IP addresses that you specify. It then obtains information from the management information base (MIB) on each agent and creates elements based on that information. When you save the discover process results, eHealth stores the element information in its database with its poller configuration.

### Element Information Importation Using DataSync

If you have a network management system (NMS) or other source at your site that collects configuration information and data for your resources, you can use the eHealth DataSync application programming interface to import your element information. To use DataSync successfully, however, you must be comfortable creating programs, scripts, and files that use complex syntax and have a working knowledge of eHealth.

**Note:** For more information, see the *Data Integration Guide*.

### Element Information for Integration Modules

eHealth provides a set of integration modules that let you use eHealth to report about the data that various network management systems collect. When you add licenses for these integration modules, you can access a script (installed with eHealth) to install them. They can input bulk performance and configuration data into eHealth, providing critical data quickly and eliminating the need for duplicate polling.

**Note:** For more information, see the appropriate user guide for the integration module.
Data Collection Maintenance

Resource discovery is a critical step in eHealth administration, so it is important to understand the various ways that your element configuration can change and the steps that you can take to effectively maintain data continuity. After performing a discovery, it is good practice to do the following:

- Review your discovery logs carefully for changes that have occurred.
- Retire or delete elements that you no longer want to monitor.
- Resolve resource changes that the discover process was unable to resolve.

When performing future discoveries, use a filtering method to find only the elements that you want to monitor. By rediscovering often, data collection remains continuous so it can significantly reduce the number of resource changes that the discovery process is unable to resolve.

You can run the discovery process interactively or schedule it to run at regular times to maintain your element information and the poller configuration.

Discovered Elements and the eHealth Poller

eHealth collects performance and availability data from your discovered elements by polling them. Polling is the process of collecting statistics about network, system, and applications data directly from elements. The eHealth poller automatically collects data for any element in the eHealth poller configuration. The poller configuration defines the information for each element such as the name, a polling rate (the frequency with which eHealth polls the element), and the agent type (the type of element that eHealth discovered).

Maintenance of Poller Configuration

While discovery can keep your poller configuration up-to-date, it works most effectively when you maintain your configuration by correcting problems with resources that you are monitoring, adding new resources, and deleting those that have been removed from the infrastructure. eHealth provides you with the tools that you need to manage your poller configuration to let eHealth collect data regularly on your resources.
Organization of Elements by Grouping

By grouping related elements, you can simplify reporting for your users and effectively organize the data. Since you can discover thousands of elements, eHealth provides a grouping capability. You can organize elements based on geographic location or function by creating groups, organize those groups into group lists, and then run reports about them.

For example, if you want to monitor all systems supporting your business within Europe, you could create a group for each country and include systems that support offices in that country. You can then add the groups to a group list called Europe and generate data about the group list.

Report Management

As an eHealth administrator, you can generate reports from the eHealth console and output them to your screen, the Web, or a printer, or save them as files. You can also email reports to eHealth users. To help eHealth users generate and view reports from the Web interface, you can set the appropriate permissions on their Web user accounts. Most Web reports have drill-down capabilities that let Web users view additional reports and obtain more information about the elements.

To meet the specific needs of a user or organization, you can customize reports in various ways, and control access to particular report types and drill-down report features. You can run reports on demand or schedule them to run on a regular basis.

System Processes Management

An important task of eHealth administration is monitoring the eHealth system and its critical processes to confirm that everything is functioning properly. To monitor eHealth processes, you can use the eHealth History and System Information features of the OneClick for eHealth console to view all historical activity that has occurred on your system. To determine whether critical processes are running or certain events have occurred on the eHealth system, you can place a management agent on the eHealth system.
Database Management

eHealth includes a fully-integrated database that does not require a dedicated database administrator to operate it. As an eHealth administrator, you may be responsible for managing the eHealth database so that critical resource information is saved and is always available for reporting and management. You must confirm that the database software is running smoothly and that the data is backed up regularly. In addition, you must manage the growth of the database so that it does not run out of disk space.

Capacity Planning

eHealth helps perform the following major capacity planning activities:

- Identify underutilized resources.
- Identify overutilized resources.
- Plan future capacity needs.

Efficient capacity planning helps reduce costs, improve performance, reduce server and network downtime, and improve budget predictability.

Underutilized Resources

The Underutilized Elements report lets you quickly identify elements that may be underutilized. You can then investigate the utilization of these elements using Health and Trend reports, and plan your options using the Capacity Trend What-If report. This process can yield significant results quickly, saving you money by cancelling unused leased lines, downgrading underused lines to less expensive options, or relocating demand from overused to underused WAN interfaces, disks, or systems.

Correct underused resources using the following process:

1. Identify underutilized resources.
2. Confirm underutilization.
3. Address underutilized resources.

Identify Underutilized Resources

To identify underutilized resources in your network, schedule the Underutilized Elements report to run as part of a daily Health report.
You can schedule this report to run at periodic intervals (weekly or monthly) depending on your specific needs. When you first install eHealth, run it weekly to identify resources that are not being used. After this initial period, you can run it less frequently (monthly or quarterly) to identify usage changes in your network.

Since the Underutilized Elements report looks at data from the past eight days, you should schedule the report to run on Sunday so that you get data for an entire business week.

Depending on how your network is used, you can edit the service profile so the report includes data from only certain days or times, to eliminate periods of low network usage such as nights or weekends.

The Underutilized Elements report lists elements that meet the following criteria for the past eight days:

- Never reached 50 percent utilization
- Did not reach ten percent utilization more than five percent of the time

Use the Underutilized Elements report to locate leased lines, routers, switches, and systems that have underutilized bandwidth, CPU capacity, memory, or disk space.

When you run an Underutilized Elements report for only LAN/WAN elements, the elements are sorted first by speed (since faster WAN links are more expensive), and then by the percentage of time they were underutilized.

**Confirm Underutilization**

Once you identify network elements that may be underutilized, analyze the purpose of each element and run reports to confirm that they are really being underused.

Before going further, review any unused network links to determine whether they are backups. Since backups are used only when the primary fails, they often have no usage. If a candidate element is not a backup, confirm that it has been underutilized for at least a month by running a monthly Health Report.

Select Element Detail in the Health Report, and examine the Bandwidth Utilization chart. The Bandwidth Utilization chart shows the load on each of the network interfaces over the report period. Usage percentage is color-coded, showing the percentage of time the interface was in each usage range. Gray bars in the chart represent lines that have not been used at all, while no color indicates that no data was collected.
Click the bar for the element you suspect is underused to run a Bandwidth Trend Report. The Bandwidth Trend Report shows the utilization for that element for the same time period as the Health Report. Examine the chart for constant underuse, or for a sudden decrease in usage due to network reconfiguration.

When you confirm that a resource is underutilized, establish a report trail to document evidence of low usage. In addition to weekly and monthly Health Reports, you can run a Service Customer Service Level report for longer term (quarterly or yearly) bandwidth utilization data. The Service Customer report also contains the Daily Bandwidth Utilization chart, which provides a detailed picture of daily usage.

**Address Underutilized Resources**

Once you document the underutilized resource, you can address the issue by doing one or more the following:

- Eliminate unused lines.
- Downgrade underused lines.
- Reroute traffic to the underused line.

**Downgrade Underutilized High-Speed Lines**

When high-speed leased lines are underutilized, you can often save money by downgrading the capacity of the link. This solution is effective when the link is a fractional T1, frame relay circuit, or ATM channel, but may not be practical if you have to change technologies or run new cable.

Depending on your usage patterns and the technology of the link, you may also be able to downgrade just one direction of the link, and have different speeds in each direction.

Before downgrading a high-speed line, run a Capacity Trend What-If report to visualize the effect of lowered capacity, and determine the optimal capacity of the new line.

**Relocate Demand to Underutilized Lines**

If you have overused lines in the same location, or multiple underused lines that can be consolidated, it may make sense to reroute network traffic to an underused line.
If you do not have other traffic from the same location, you can use a link more efficiently by doing the following:

- Relocate local servers to a central site, increasing traffic over the underused line and lowering costs through server consolidation.
- Aggregate traffic from several small local links to a regional center and use one shared high-speed link to the central site.

When relocating demand to an underused line, run a Capacity Trend What-If report to visualize the effect of added demand to the target resource.

**After Changes Are Made**

After making configuration changes, run eHealth rediscover and update line speeds in the element information. Be aware that future reports for the time range including the change may show unusual utilization percentages.

If you decreased capacity or added demand to existing resources, run Trend and Health reports on those resources. Look for any Health exceptions or other utilization problems that may result from the increased traffic.

If you eliminated an element, disable polling and retire the element in the eHealth database. Retiring the element lets you continue reporting about it until its data ages out of the database.

**Overutilized Resources**

By examining a single Health Report each week, you can identify network elements that are reaching their capacity. You can then consult other reports to analyze problems, and solve the issues before they become large problems for your IT team.

Correct overutilized resources using the following process:

1. Identify overutilized resources.
2. Confirm overutilization.
3. Address overutilized resources.

**Identify Overutilized Resources**

To identify overutilized resources in your network, schedule a weekly Health report to run on Sunday, so that you get data for an entire business week.
Review the Exceptions Summary Report in the Exceptions section of the Health report. The Exceptions Summary report identifies elements that have experienced unusual events or whose resources are consistently inadequate for the demand on them. The elements are ranked by exception points, so that those elements experiencing the worst problems are listed first.

Note any elements in the report that list Utilization Health Index or Congestion Health Index in the Leading Exception column. These elements are experiencing high volume and may be overutilized.

**Confirm Overutilization**

Once you identify network elements that may be overutilized, go to the Situations to Watch chart in the Summary section of the Health report. The Situations to Watch chart identifies elements that are predicted to exceed, reach, or come close to reaching their trend thresholds. The chart shows you how close each element is to its threshold, how fast utilization is growing, and how long until demand exceeds capacity.

Review the elements listed in the chart, looking for those that have exceeded their threshold or are growing fast enough to soon reach it. For example, in the following report, the first element (Virginia) has already exceeded its threshold for two days while the next two elements are predicted to reach their thresholds in the next week. All of these are likely to be overutilized elements. Demand on the final two elements is increasing but both are still at less than 20 percent capacity and do no represent a problem.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Element Name</th>
<th>Variable</th>
<th>Threshold</th>
<th>Daily Average</th>
<th>Days to (from)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Virginia (US)</td>
<td>Volume (Bandwidth %)</td>
<td>100.00</td>
<td>114.9</td>
<td>113.3</td>
</tr>
<tr>
<td>2</td>
<td>Dallas (US)</td>
<td>Congestion (rpm Frames)</td>
<td>1000.00</td>
<td>918.3</td>
<td>910.2</td>
</tr>
<tr>
<td>3</td>
<td>Colorado (US)</td>
<td>Volume (Bandwidth %)</td>
<td>100.00</td>
<td>88.5</td>
<td>88.2</td>
</tr>
<tr>
<td>4</td>
<td>Miami (US)</td>
<td>Volume (Bandwidth %)</td>
<td>100.00</td>
<td>55</td>
<td>58 Increasing</td>
</tr>
<tr>
<td>5</td>
<td>Michigan (US)</td>
<td>Congestion (rpm Frames)</td>
<td>1000.00</td>
<td>110.2</td>
<td>114.2 Increasing</td>
</tr>
</tbody>
</table>

Select Element Detail in the Health Report, and examine the Bandwidth Utilization chart for the elements you suspect to be overutilized. The Bandwidth Utilization chart shows the percentage of time each element was in each usage range. Generally, purple and red colors indicate an overutilized resource. Purple indicates greater than 100 percent utilization, meaning that the element is probably a leased line exceeding its contracted bandwidth, and therefore incurring overage charges.

Examine the chart to see how often a suspected element was overutilized during the course of the week. Some elements may show consistently high demand, but since demand varies over time, most elements will show significant periods of low usage. Depending on your network activity, an element may even have no usage at certain times (overnight for example), but still be overutilized because demand exceeds capacity at peak times.
To obtain more details about an element’s performance, create an At-a-Glance report by right-clicking on that element in the Bandwidth Utilization chart. Review the Bandwidth Utilization charts in the At-a-Glance report to see how frequently the element was overused, and during what time periods. Depending on your business needs, an element that reaches its capacity for only one hour per week may be acceptable, or that one hour of overutilization could be a critical problem.

Review the other charts in the At-a-Glance report for any anomalies, including high error rates or signs of congestion (FECNs, BECNs, discards). Use this information to determine the conditions that might be affecting the element, including:

■ Insufficient capacity
■ Inefficient or misconfigured applications consuming excessive bandwidth
■ Too many or too few stations overloading a WAN link
■ A highly repeated or bridged domain that should be routed

Once you have confirmed that a resource is overutilized, establish a report trail to document evidence of high usage. In addition to the reports described above, you can select specific elements in the Exceptions Summary Report and Situations to Watch chart to run detail reports for those elements. You can also run Bandwidth Trend reports on specific elements to show the long-term utilization of a resource.

Address Overutilized Resources

Once you document the overutilized resource, you can address the issue by doing one or more of the following:

■ Upgrade the element to a higher capacity.
■ Relocate demand to other resources.
■ Add additional elements to share the workload.

Finally, run Capacity Trend What-If reports to visualize the effects of higher capacity or lower demand on the overutilized element, and determine the optimal capacity of any new resources.
Planning for Future Capacity

eHealth provides capacity planning tools that let you analyze the behavior of your resources under varying conditions, and predict where and when you will need to add capacity. eHealth reports make capacity planning easier and more accurate by helping you do the following:

- Predict where and when you need to make capacity upgrades based on historical trends.
- Analyze future capacity based on hypothetical changes that you plan to make or on expectations of growth.

With eHealth reports, you can plan capital expenses for IT upgrades and forecast how your current usage might be affected by changes in capacity, demand, or both.

Use the following process to project capacity changes:

1. Identify potential capacity changes.
2. Analyze capacity trends.
3. Address capacity changes.

Identify Potential Capacity Changes

To help predict which elements are approaching their capacity, schedule a weekly Health report to run on Sundays so that you get data for an entire business week.

Examine the Situations to Watch chart in the Summary section of the Health report. The Situations to Watch chart shows the top 10 elements (network interfaces, CPUs, disk partitions) that are nearing their capacity. The chart shows you how close each element is to its threshold, how fast utilization is growing, and how long until demand exceeds capacity.
The following sample report shows several user partitions that are nearing their thresholds. In the Days To Threshold column, System-Orange shows 0, meaning that utilization has reached the Trend threshold. System-Green, shows 20 days to threshold, and System-Pink shows Increasing, indicating utilization is growing, but will not reach threshold for a long period of time.

Each of the systems at or near its threshold merits further investigation. For example, System-Orange could already be overutilized, or it could be a system partition designed to operate near capacity. System-Green, on the other hand, is 20 days from meeting its threshold, but could be a good candidate for upgrade if it is showing a steady increase in demand.

To quickly follow up with these situations, click the element name to run a Situations to Watch detail report for the partition. Examine the trend line in the detail report to see how quickly the trend is approaching the threshold. If the line is rising at a steady rate, consider adjusting capacity by increasing the size of the partition, deleting unneeded directories and files, or buying a new system.

### Analyze Capacity Trends

After you identify potential upgrade candidates, run Capacity Projection and Capacity Provisioning reports to forecast volume changes over the upcoming weeks and months, and predict when elements need to be upgraded.

The Capacity Projection report forecasts how the capacity of a particular variable (partition utilization, for example) will change in the future. You can run the report based on peak, average, or percentile capacity values. eHealth measures the predicted capacity values against a threshold you specify, and displays those elements predicted to exceed the threshold.

To project exactly when these elements will need to be upgraded, run a Capacity Provisioning report. The Capacity Provisioning report compares projected capacity values against an upgrade threshold, and displays those elements predicted to exceed the threshold, along with the number of days until an upgrade is required.
Like the Capacity Projection report, you can run this report based on peak, average, or percentile capacity values. You can set both the upgrade threshold and an upgrade lead-time window through the eHealth console.

**Address Capacity Changes**

When you predict changes in demand, or identify elements that need to be upgraded based on current usage trends, run a What-If Capacity Trend report to analyze potential solutions.

The What-If Capacity Trend report shows how resources perform as your infrastructure changes and grows. These reports let you leverage historical data to predict future patterns, model changes in capacity or demand, and see the effect on resources.

Using the report, you can determine whether an existing resource can support anticipated changes and, if not, how much capacity must be added. You can also illustrate potential problems so that you can justify requests for new equipment or upgrades.

**Maintenance**

Some important steps that you should take to proactively maintain your eHealth system are as follows:

- Use advanced logging to troubleshoot problems
- Upgrade to new releases
- Install patches

**Advanced Logging**

You can access two types of advanced logging tools to troubleshoot problems that you might encounter with eHealth using the OneClickEH console or the eHealth Web user interface. Some of the options can interfere with your system performance, and most of the log files consume a significant amount of disk space. Therefore, do not enable advanced logging unless you are troubleshooting a specific problem under the direction of Technical Support or your Sales Engineer.

**Upgrades**

When a new release of eHealth is available, you should upgrade to obtain the latest features and software fixes.
The InstallPlus program helps you reduce downtime by installing the latest fixes, certifications, and support as part of your upgrade. The InstallPlus program is the standard eHealth installation program; it is updated for every patch and certification release.

Use the InstallPlus program only when you install an eHealth release for the first time, or when you first upgrade from a previous eHealth release.

**Note:** For more information, see the *Installation Guide*.

**Service Packs**

InstallPlus does not replace the standard service pack (patch) installation program. After you have installed an eHealth release, continue to use the service pack installation program to install fixes and patches for your release.
Chapter 4: Reports

This section contains the following topics:

About Historical Data (see page 45)
Standard Reports (see page 46)
Historical Analysis Reports (see page 47)
Drill-Down Reports (see page 48)
MyHealth Reports (see page 49)
Report Center (see page 49)

About Historical Data

For eHealth, historical data is information about your IT infrastructure that is older than the most recent poll. For example, if eHealth collects data every five minutes, historical data is data that is older than five minutes. By default, eHealth retains historical data for more than one year; when it generates reports, eHealth may incorporate data from five minutes ago to more than one year ago.

You can use eHealth reports to do the following:

■ Troubleshoot a problem identified using Live Health.
■ Identify and analyze trends.
■ Perform capacity planning.
■ Monitor and manage the health of your IT infrastructure.

These reports can be used by many people, including NOC administrators, network planners, system administrators, CIOs, application managers, consultants and analysts, service providers and their customers, and eHealth administrators.

Many eHealth reports are available as Web reports, PDF files, and ASCII text files. The reports can be automatically generated and sent to specified recipients on a regular basis, such as daily, weekly, or monthly. The eHealth administrator can design and run reports from the eHealth console, and authorized users can view and run reports from the eHealth Web interface.

Note: For more information about how to use eHealth reports, see the Reports User and Administration Guide.
Standard Reports

eHealth provides a series of predefined, standard reports that you can use for troubleshooting, capacity planning, and trend analysis. These reports include the following:

- Trend reports
- At-a-Glance reports
- Top N reports
- What-If reports

Trend Reports

The Trend report is useful for troubleshooting. You can use a Trend report to plot one variable for up to ten elements over any time period or to plot up to ten variables for one element. You can also run a group Trend report that shows either of the following:

- Aggregate data for a group of elements, which lets you identify trends for the group as a whole
- A separate chart (for each of the chosen variables) for each element in a group, which lets you compare the performance of elements within a group

Due to its flexibility, you can use the Trend report to reveal variable patterns over time as well as relationships between elements and between variables.

At-a-Glance Reports

The At-a-Glance report provides an overall look at the critical performance indicators for an element. It also lets you examine key metrics for problem elements. The report automatically correlates important performance statistics in a single-page presentation for a specified time interval.

At-a-Glance reports can reduce the amount of time you spend troubleshooting problems by automatically capturing performance data and providing it in a uniform presentation.

Top N Reports

You can use the Top N report to identify elements that share specific performance characteristics. Top N refers to the highest-ranked subjects based on criteria that you specify. For example, you may want a list of the ten people who use a particular application the most: the top ten application users.
To identify overutilized elements, you can generate a Top N report for elements whose bandwidth utilization exceeds 90%. Similarly, to identify unreliable elements, you can generate a report for elements whose availability falls below 95%.

The Top N report can support up to six different variables. For example, you can generate a report to identify all elements for which bandwidth utilization exceeds 80% and availability falls below 99.9% and latency exceeds 50ms. This capability lets you identify which elements are the sources of a performance problem.

What-If Reports

What-If reports let you change various assumptions to determine how they affect performance. For example, the What-If Capacity Trend report lets you adjust the capacity (speed) or demand for an element and observe the effect of those changes in the resulting report.

Historical Analysis Reports

eHealth offers two reports that perform historical analysis, comparing current performance with past performance: Health reports and Service Level reports.

Health Reports

Health reports compare current performance to the historical performance of your IT infrastructure. They contain information about the performance of a group of elements for a specified time period and alert you to situations to investigate because of errors or unusual utilization rates or volume.

You can use a Health report to do the following:
- Identify normal and unusual behavior.
- Identify trends.
- Evaluate the health of your IT infrastructure and of specific elements by hour, day, or month.
- Identify elements that require further investigation.
- Send traps to other network management systems when problems are detected.
Drill-Down Reports

Service Level Reports

Service Level reports analyze and display service level information (such as availability, latency, and resource utilization) for a region, a department, or a business unit.

Service Level reports are designed to meet the needs of different audiences. Executive, IT Manager, and Service Customer reports are single-technology reports; you can generate each report for a particular technology type such as LAN/WAN interfaces, routers, or systems.

The Business Unit report, designed to provide service level information for an entire business segment, can include elements across different technology platforms. For example, the Business Unit report for a finance department would cover all of the systems, routers, and LAN/WAN segments within that department.

Scheduling Health and Service Level Reports

Health reports and Service Level reports can take a long time (up to several hours) to complete because eHealth must perform a complex data analysis to evaluate the health of the elements in a report. If you frequently run these reports on demand, consider scheduling them to run during off-peak hours. (Only eHealth administrators can schedule reports; users of the eHealth Web interface cannot schedule them.)

When you schedule these reports, eHealth runs a scheduled Data Analysis job and saves the daily analysis summaries for each element. Future Health and Service Level reports (run on demand or scheduled) for the same elements and profiles run faster because eHealth does not need to perform the data analysis for the elements that have existing analyzed summaries.

Drill-Down Reports

For Web-based eHealth reports, you can click a part of a report, such as a bar in a chart or an element name in a table, to drill down from the current report to another related report.

When you drill down from one report to another, eHealth automatically uses the context of the current report and the selected report item to determine the appropriate criteria to use when generating the new report. In addition, many areas offer multiple drill-down reports, so you can choose the type of report to generate from the selected item.
Drill-down reports are useful when troubleshooting a problem to determine its source. For example, when one report identifies a performance problem, you can drill down to a related report to determine which element or part of the IT infrastructure is the root cause of the report. This helps to streamline the problem resolution process and speeds time to resolution.

MyHealth Reports

To tailor a set of reports to meet your specific needs, you can use the MyHealth report. When authorized, you can create and run multiple MyHealth reports. Each report can contain several charts that summarize critical application, system, and network information. With MyHealth you can display the information that is important to you on one summary page. By viewing this report at regular intervals, you can quickly determine whether critical resources need attention.

You can view your MyHealth reports from the MyHealth tab of the eHealth Web interface. The eHealth administrator and authorized users design MyHealth reports by specifying the report panels, titles, baseline periods, and a service profile. The eHealth Web administrator specifies whether each user can view, create, edit, or run MyHealth reports on demand.

Report Center

eHealth Report Center is an optional reporting system that is used to customize the standard eHealth reports. Report Center offers an alternative to the eHealth Report Developer Language (RDL).

Report Center lets both users and administrators create and customize entirely new types of eHealth reports. These reports can answer different types of questions about the performance of network, system, and application resources. You can manipulate the appearance of reports and how existing eHealth data is represented.

This application offers a web-based, Windows folder-style interface that you can change based on your preferences. This intuitive interface lets you identify, view, and run reports. Report Center provides sample reports that you can run to view the performance of your resources or use as templates when creating new reports.
It also lets eHealth administrators set up user accounts with various permissions and assign user accounts to various roles. The roles range from those that permit users to perform basic tasks to those that provide permissions to accomplish complex report development tasks.

**Note:** For more information about how to use Report Center, see the *Report Center User and Administration Guide*.

### Customization Features

Report customization options exist to help report authors do the following:

- Change the location of charts and tables on the page
- Specify the content
- Control the appearance of titles, branding and colors
- Add text notes
- Define drill-down links to other reports and locations
- Create prompts for the subjects, time ranges and other input values for the report

Report Center also provides report authors with the ability to customize reports that run on demand, such as limit a report to show only the data of interest (date, time, group, granularity and so on).

A document management system lets report authors create and organize personal folders, providing a more intuitive way to locate reports. It offers a search feature and maintains a history so that previous versions of reports can be accessed. The document management system also offers better security of content on a per-user basis and the ability to share content among users.

A Web-based report scheduler lets you schedule reports to run during off-hours and be completed before you arrive at work.

Universal accessibility is provided to users as well as report authors. Report Center is Web-based; any authorized user can access the system from any desktop or workstation that has network access to the Report Center server.

Sample reports help answer new types of questions about eHealth resources. The sample reports also provide examples for report authors who want to customize reports or create similar types of reports.

**Note:** For information about how to use the Report Center applications, see the *Report Center User and Administration Guide*. 
User Roles

It is important to understand the different types of Report Center user roles. Users have access to various Report Center applications, depending upon the permissions that are set for the roles to which they are assigned:

**eHealth Administrators**

Access all Report Center tools and applications. They have the ability to manage user accounts and roles, public and personal folders, access permissions, and the eHealth system.

**Report Consumers**

View and run reports to answer questions about their eHealth elements.

**Report Authors**

Create and customize reports that usually address questions from consumers such as IT management or service customers.

**Report Administrators**

Set Report Center security permissions, import and export content, and perform other Report Center administrative tasks, but do not have access to eHealth-only administrative functions.

Applications

Report Center offers the following applications:

**Report Center Home Page**

Provides navigation to folders, access online help, and a variety of tools to customize windows. eHealth or report administrators can control access to folders and reports on a user-by-user basis.

**Report Studio**

Permits report authors to create new reports as well as customize existing reports. Report Studio is a highly versatile report authoring tool that lets users create a variety of multi-page, multi-chart reports, design page layouts, create programmatic prompts for report information, and even write SQL queries to read information from the eHealth database and include it in reports. Typically, authors use Report Studio to create reports that other users will run or schedule for more frequent use.

**Query Studio**

Provides the ability for report consumers and authors to run reports on demand and create quick tests of possible report content. Advanced report consumers can run a report to answer a specific question about their eHealth data. The information can include element information, variables, or both. The report is a simple tabular or single-chart report.
Sample Reports

Report Center offers sample reports that users can run to obtain different insights to their eHealth data. Some of the sample reports are variations of standard eHealth reports such as Top N. Others are different types of reports.

Report authors can also use the sample reports as templates that they can edit in Report Studio to learn how to create similar types of reports.

Incident Report on System Average CPU Utilization

This sample report lists each time, and for how long, a system CPU exceeded a service threshold specified for a group of systems:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Avg. CPU Utilization</th>
<th>Duration (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/6/05</td>
<td>2:00:00 AM</td>
<td>54.0%</td>
<td>300 seconds</td>
</tr>
<tr>
<td>11/6/05</td>
<td>5 minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11/7/05</td>
<td>1:30:00 AM</td>
<td>52.1%</td>
<td>300 seconds</td>
</tr>
<tr>
<td>11/7/05</td>
<td>1:35:00 AM</td>
<td>54.5%</td>
<td>300 seconds</td>
</tr>
<tr>
<td>11/7/05</td>
<td>5:05:00 AM</td>
<td>50.9%</td>
<td>300 seconds</td>
</tr>
<tr>
<td>11/7/05</td>
<td>15 minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Duration</td>
<td>20 minutes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Users specify the threshold when they run the report. This data can help to explain a performance problem that could have resulted in time-over-threshold Live Health alarms.

The report displays a page for each system in the group, and a page for each day of the report period in which an incident occurred. The report also summarizes the total amount of time that the element operated above the threshold.

For report authors, this report provides an example that uses queries to compare variable values to a threshold or goal value. Authors could use similar queries to create reports where variables such as memory, availability, or disk space are below a certain threshold.
Daily Busy Hour Report for Interfaces

This sample report identifies the 60-minute interval when the traffic or volume for a LAN/WAN interface was at its highest:

For each day of the report period, the report lists each element in the group and its highest hourly volume and overall data rate in bits per second (total, incoming, and outgoing). By identifying the highest traffic hour, you can evaluate whether the interface is operating at expected utilization rates or whether you might have capacity issues to address.

Daily Top N Utilization Report

This sample report is similar to the Element Summary table of an IT Manager report.

For each element in a LAN/WAN group, it lists the values for the following key performance variables for each day of the report time range:

- Daily bandwidth utilization
- Business day bandwidth utilization (Users specify the business hour range when they run the report.)
- Number of times (polls) in which utilization was in the range of 70-80 percent
- Number of times (polls) in which utilization was in the range of 80-90 percent
- Number of times (polls) in which utilization was over 90 percent
- Daily average latency (the network time for ping traffic to cross from the eHealth system to the device and back)
- Average latency during business hours

Unlike standard eHealth Top N reports, which can only compare up to six variable values, Report Center lets you create reports for any number of variables. Also, you can compute new columns using a variety of math functions such as percentiles, time over threshold, deviations, and busy hour.

**Comparison Report: Response Time and CPU Utilization**

This sample report helps identify possible correlations between increases in server CPU utilization and resulting response time degradations for an application response path to that server. This report can help answer questions about response time impacts when a server CPU is overutilized:

![Comparison Report - Response Time vs. CPU Utilization](image)

A correlation occurs when the datapoints show a linear increase; that is, as the variable on the horizontal axis increases, the variable on the vertical axis should also increase or decrease in a linear trend. If there is no linear change, there is no correlation between increases in server CPU utilization and increased response time. The response time problems for the path must be a result of either network or client delays, not the CPU of the application server.

This report can show evidence for a correlation between increased response time and increased CPU utilization. It can also show that there were times when response time was high at low CPU utilization times and where response times were low during high CPU utilization. These exceptions are common and indicate that the response time impacts are likely due to other causes, such as network or client response time.
For report authors, this sample report is important because it compares two variables from two elements of different technology types over the same time period. This comparison is not possible with standard eHealth reports. The scatterplot-style report format is also not available for standard Trend reports.

**Aggregate Throughput Report for Interfaces**

Within a network, you may have a set of links that carry the traffic between sites. The links share the workload, and if one link should fail, the traffic is routed to a backup link. These configurations are referred to as link (or path) bundles.

The Aggregate Throughput Report for Interfaces helps you visualize the traffic volume that normally crosses a set of links, and whether the capacity of a backup link is capable of carrying the volume of the primary links in the event of an emergency as shown in the following example:

You can compare the total traffic to a bottleneck speed to see when, and how often, the traffic reaches and exceeds the point at which discards and delays might affect the end users.

For example, the total traffic for a group of interfaces for inbound and outbound traffic can have a backup speed of 56,000 bps. The aggregate traffic for the first few hours of the day might be the same as the bottleneck speed. However, the traffic could increase at a certain time and remain in excess of the backup. If a network problem occurs and the traffic is rerouted to the backup, the backup would be congested. Discards and other problems will cause performance problems for users. The report lets you change the bottleneck speed and then rerun the report to determine how an increase (or decrease) in the capacity of the backup might better support the traffic.
Common Report Center Tasks

To run reports, you must connect to the eHealth system using the URL http://ehsystem, where ehsystem is the hostname or IP address of the eHealth system where Report Center is installed. Log in using your web user account and password.

For report consumers, you can perform four common tasks in Report Center as follows:

■ Run reports on demand.
■ Run and save reports.
■ Schedule reports to run periodically.
■ Email reports.

You click the Report Center tab to access the Report Center home page. To navigate to the sample reports, click eHealth Reporting, Sample Reports.

Note: If you do not see this tab, see your eHealth administrator for permissions.

When you run a report, you save the generated report on top of the report specification or a previously run report. You can view the saved report at any time without rerunning that report.

You can schedule reports to run automatically and be complete before you arrive at work. Running reports during off-peak hours helps to reduce impact on the eHealth system during peak hours and is useful for reports that take a long time to run.
Chapter 5: Managing Fault and Performance

This section contains the following topics:

- Faults and Performance (see page 57)
- Business Service Console (see page 58)
- Live Health Overview (see page 59)

Faults and Performance

While eHealth reports are useful for troubleshooting, trend analysis, and capacity planning, they do not let you anticipate and identify faults and slowdowns that are affecting users in real-time. To address this need, eHealth provides real-time fault and performance management capabilities, active displays (not static reports) that are updated as often as every 30 seconds for rapid problem diagnosis.

Fault Management

Fault management is the reactive process of detecting, logging, notifying users of, and (where possible) automatically fixing problems to keep the IT infrastructure operating effectively. Since faults can cause downtime and network degradation, fault management is a high priority for IT organizations. For example, if a critical process fails, a fault management system detects and records the failure, and notifies the appropriate IT staff. In addition, the fault management system may be able to restart the failed process automatically to minimize the impact of the failure.

Performance Management

Performance management is the proactive process of monitoring the performance of various components of the IT infrastructure and taking corrective action before degrading performance impacts the business. For example, you can use performance management to monitor network throughput, user response times, and line utilization.
A performance management system determines a baseline of normal performance for a component, sets thresholds to warn of problems, and generates alarms when thresholds are reached or exceeded. For example, the user response time for a particular application may be slowing significantly. When the performance management system notices that response time exceeds the threshold, it sends an alarm to specified users, such as on-call IT staff. It can also act to correct the problem, such as starting another application process to serve additional users.

Real-Time Data

Real-time data is the information that eHealth collected most recently. As it ages, this data is added to eHealth historical data, which is information about your infrastructure that is anywhere from five minutes to more than one year old.

eHealth provides two types of real-time data:
- Information that was collected during the last poll or sent as traps by SNMP agents. The eHealth application called Live Health uses this data. This chapter describes the real-time fault and performance management capabilities of Live Health.
- Information that is collected immediately. eHealth AdvantEDGE View uses this data.

Business Service Console

The eHealth Business Service Console (BSC) is a Web-based tool providing a high-level view of the availability and performance of your business services. By mapping important business services to the managed IT infrastructure, the Business Service Console provides a real-time, end-to-end view of the performance of key business services from a user’s perspective.

The BSC offers customized business views, immediate notification of performance problems, and drill-down capability for fault resolution, providing a snapshot view of the status of your business services. Throughout the day, you can monitor activity and status of applications, systems, or networks using a scrolling “ticker” located in the corner of your screen. The ticker provides a subset of the hierarchy represented within the console and expands to show the full console. If a critical availability or performance problem occurs that may impact your business, you can quickly determine whether someone is addressing it. An acknowledgment indicator shows whether someone is working on the problem, while a duration indicator shows the length of time the indicator has been in the current state of red or yellow.
The BSC provides additional details through pop-ups and navigation buttons, letting you go directly to a report generation window or to the Live Exceptions Browser to drill down to obtain details about the problem and determine the cause.

**Note:** For more information about administration of the BSC, see the *Business Service Console Administration Guide*.

---

**Live Health Overview**

Live Health is a set of applications that provides real-time fault, performance, and availability management for eHealth components.

Live Health consists of three applications:

- **Live Status**
  Provides a high-level view of the current status of monitored elements in your IT infrastructure.

- **Live Exceptions**
  Analyzes real-time performance data to detect problems and displays alarms in a browser.

- **Live Trend**
  Provides a real-time charting tool to monitor elements of your IT infrastructure.

**Note:** For more information about how to use Live Health, see the *eHealth Help*.

---

**How Live Health Works**

The Live Health process is as follows:

1. eHealth collects performance data across the entire delivery system, including applications and underlying network and system components.

2. Live Exceptions analyzes the data to identify outages and delays, and leverages the historical data in the eHealth database to identify true problems with greater precision. Live Health eliminates noisy, repetitive traps that provide little or no value.
3. When Live Exceptions detects a fault or potential outage, it generates a single intelligent alarm and sends it to the Live Exceptions Browser or to any SNMP-based network management system.

4. When the IT team is alerted to a performance problem, Live Health provides an intuitive workflow to quickly identify and resolve the problem. With seamless access to eHealth reports, team members can leverage robust historical and real-time analysis to quickly identify and correct performance problems.

**Live Status**

Live Status is a graphical visualization tool that provides a real-time, high-level view of the current status of monitored elements in your IT infrastructure. Using Live Status, you can identify problems as they occur, locate where the trouble is occurring, and see the severity of the problem.

The Live Status diagram is a fishbone style visualization as shown in the following illustration:
The horizontal spine in the center is the highest-order view of resources (a group list). Each rib off the spine is a set of related resources (a group). Each rib has one or more icons that represent an element. Color-coded icons indicate the operational status of the element and where the trouble spots are.

The Network Operations Center (NOC) team can use Live Status as the overhead display so team members can quickly identify problem elements that merit investigation. To simplify troubleshooting, Live Status is integrated with other eHealth components, providing drill-down capabilities to the Live Exceptions Browser, Live Trend reports, various eHealth reports, the Agent Transaction Viewer, and eHealth AdvantEDGE View. IT staff can glance at the display to identify problems and drill down to element-specific information to troubleshoot them.

Live Exceptions

Live Exceptions is the engine that powers the Live Health suite. It provides alarm reporting by identifying problems that include delay, errors, failures, security, or configuration changes. Network operations center and systems, application, and network management personnel can use Live Exceptions to monitor the status of their resources.

The default monitoring features included with Live Exceptions are as follows:

- Intelligent Alarm Processing
- The Notifier
- Live Exceptions Browser
- Filtering and Collapsing Alarms
- Alarm Profiles
- Acknowledgments and Annotations
- Drill-downs
- Fault Manager

These features can be tailored to your own specific infrastructure.

Live Exceptions analyzes real-time performance data to detect problems and display alarms in the Live Exceptions Browser, which provides a real-time view of the performance of your entire IT infrastructure. Live Exceptions can detect application slowdowns as well as performance problems with network elements and systems. It uses rules and profiles to determine when to generate an alarm. When Live Exceptions detects a problem based on these rules, it generates an alarm and sends it to the Live Exceptions Browser. (This browser appears when you start Live Exceptions.)
Notifier

The Notifier is a key component of Live Health. It takes immediate action when alarms are raised, cleared, or acknowledged, and lets you control notification frequency. The Notifier can send email notification to the appropriate IT personnel. It can also run scripts, such as pager and cellular telephone programs, or other commands to help manage expanding and escalating situations.

Live Exceptions also has an auto-acknowledge script that lets it automatically acknowledge an alarm when it is raised. This feature saves time when you have an established procedure for addressing certain alarm types.

This auto-acknowledge script can also be the basis for more customized Notifier actions or used to change default values. For example, you can change the default message in the Live Exceptions Browser Notes annotation field to identify the IT team member who typically responds to that alarm type.

Live Exceptions Browser

The Live Exceptions Browser is a user interface for the operations team, the help desk, customers of service providers, and management. It provides a real-time view of the performance of your entire IT infrastructure.

When Live Exceptions detects a fault, error, or delay, it forwards an alarm to the Live Exceptions Browser. The Live Exceptions Browser can display alarms for the entire organization or for a specific subject. Browser options let you sort, filter, and summarize (collapse) alarms so you can focus on a particular set of alarms. Live Exceptions keeps an alarm active until the condition no longer exists or a Live Exceptions administrator manually clears the alarm.

Service providers and enterprise users can deploy the Live Exceptions Browser as part of real-time service level agreement (SLA) monitoring services. End users can use the Live Exceptions Browser as a live interface to validate that expected service levels are being delivered. For real-time SLAs, service providers can restrict access to specific groups and can provide as much or as little detail as desired. The Live Exceptions Browser can support up to 50 simultaneous users.

If you use Distributed eHealth, the Live Exceptions Browser running on a Distributed eHealth Console can show you the alarms from all the eHealth systems in the cluster. You can identify which Distributed eHealth System is managing the problem elements and then open a Browser to that eHealth system to manage its alarms. This lets you manage the performance and availability of systems around the world from a single point.
How To Use Live Exceptions

When you first open Live Exceptions, a large quantity of information appears. To obtain value from Live Exceptions, you should follow this process:

1. Determine your permissions. Permissions control the tasks that you can perform in the Live Exceptions Browser and the reports and groups that you can view.

2. Review the groups. Rules are applied to groups and group lists. Determine whether they reflect your infrastructure.

3. View the alarms. View the information in the Browser, format the Browser so that the information is easier to view and relevant to your organization, and determine which alarms are important to you.

4. Obtain information about alarms and elements. Drill down from an alarm to view additional information that can help you resolve the problem.

Permissions

Live Exceptions has two types of users: administrators and general users. If your account has administrative privileges, you can perform additional tasks, such as creating and modifying rules, associating profiles to subjects, and creating notifications.

The groups and reports that you can view from the Live Exceptions Browser also depend on your account permissions. Your Web administrator defines the groups, group lists, and types of reports that you can view. If you cannot view the groups or reports that you need in the Live Exceptions Browser, contact your Web administrator.

Review Groups

Live Health monitors resources and displays alarm information based on groups and group lists. A group contains all the elements for something you want to monitor as a unit, such as a department, an office, or an application. Group lists are collections of these groups.

Organizing your resources into logical groups helps you manage your resources most effectively. You can group elements by location, business function, technology, or whatever makes the most sense for your situation. For example, you may want to create a group for all the elements in your engineering department, and another for all the elements in a specific office, regardless of department. Creating logical groups lets you see where trouble is starting and how severely specific services are impaired.

Use the Organization tab in the Live Exceptions Browser to view the groups and determine whether they correctly reflect your infrastructure. The eHealth administrator defines groups and group lists using the eHealth console.
You can also run reports that provide information about groups, group lists, elements, and the associated rules and profiles. Using this information, a user with administrative privileges can change the profiles and rules that are associated with a subject.

**Alarm Processing**

Instead of generating multiple redundant alarms for a single incident, Live Exceptions raises one alarm that remains active while the problem is present. This reduction in alarm noise lets you find, diagnose, and resolve problems without being distracted by repetitive alerts to the same problem.

Live Exceptions has can be configured to raise an alarm only when a threshold violation persists for a specified duration, which reduces the noise and distraction of alarms for transient events that occur and disappear immediately, such as random spikes. Since not all transient events are benign, Live Exceptions can be configured to raise alarms immediately for situations that concern you.

**View Alarms**

By default, when you first open Live Exceptions, the Organization tab has All Technologies selected. This option displays all alarms in the browser. To view alarms for a specific group or group list, select that group or group list in the Organization tab. The Event Table lists all alarms for the group or group list that you select.

The alarm severities are as follows:

**Red**
- Indicates a critical alarm. The element is down.

**Orange**
- Indicates a major alarm. The element has too many errors or may fail.

**Yellow**
- Indicates a minor alarm. The element is contributing to delay.

**Green**
- Specifies a warning. The element’s workload is unusual compared to a baseline of its normal activity.

**Muted/all colors**
- Indicates that alarms have been cleared for that element.

Live Exceptions keeps an alarm active until the condition no longer exists or an administrator manually clears the alarm.
Use the columns in the Event Table to obtain more information about an alarm. For example, you can determine the time that an alarm started, the IP address of the affected element, the reason that Live Exceptions raised the alarm (in the Rule Message column), and so on. You can sort, rearrange, and resize the columns to view critical information.

The options that appear in the menu depend on the element, your permissions, and the licenses installed on the eHealth system.

By default, the browser displays currently active alarms. However, you can view historical information about an alarm. You can also reduce or modify the information that appears in the Event Table so that you can focus on a particular set of alarms and perform any of the following tasks:

- Hide columns to eliminate information that you do not want to view.
- Collapse alarms to reduce the number of rows that appear in the browser and see how many alarms are active for a specific element.
- Filter elements so that only specific information appears.

When you collapse alarms, you can drill down for more details if needed.

**Additional Views in the Browser**

If several alarms appear in the browser, you may find it helpful to view the information in a different format. From the View menu, you can select the following options:

**Top 10 Alarms**

Displays the ten groups containing the most active alarms.

**Consolidate Events Over Time**

Consolidates similar alarms into one line when you view the browser in historical mode.

**Alarm Occurrences**

Displays a separate window of all alarms that appear as one consolidated line in the Consolidated Events over Time view or when you collapse alarms.
Acknowledgments and Annotations

Live Exceptions can show you and other users that a problem is being addressed – and how. You can view the Ack (acknowledgement) and Assigned columns of the Live Exceptions Browser to see status or information about problem resolution. This information can help reduce the number of telephone calls and emails you receive requesting problem status. Acknowledgments and annotations are visible to all Live Exceptions users and on the Business Services Console.

Acknowledging an alarm means that a problem has been discovered, noted, and is being addressed. When an alarm is acknowledged, the following actions occur: a check mark appears in the Ack field; your Web user account name appears in the Ack User field; and the day and time you acknowledged the alarm appears in the Ack Time field.

Live Exceptions provides fields that can be used to annotate an alarm; these annotations appear as columns in the Live Exceptions Browser. The default labels for these columns are: Ticket #; Status; Assigned; and Notes. These are freeform text fields that you can use to provide additional information about the problem or resolution state. You can also change the column names if you prefer alternate column headings. Annotation provides you with additional detail about an alarm. This detail is a snapshot of problem status, possible causes, and potentially an estimated time to repair.

More Alarm Information

You can select an alarm and right-click to display a pop-up menu that lets you obtain more information.

The following drill-downs are available from the right-click pop-up menu or the Run menu:

**At-a-Glance Report**

Displays a series of charts that show the performance of critical variables for the event related to the alarm you selected. The report period begins at midnight before the problem start time and ends at midnight on the day the alarm ended. The report ends at midnight of the current day if the alarm is still active.

**Trend Report**

Provides details about one or more variables. You can use this report to identify patterns over time, as well as relationships among elements and variables.
Reports
Displays a list of all reports that have been run for the element you selected. A Web browser opens and displays the element you selected on the Organization tab of the eHealth Web interface. A report list for that element appears in the right frame.

Live Trend
Lets you select a statistics element and drill down to run Live Trend. Live Trend is a real-time charting tool that you can use to monitor statistics elements that are polled by eHealth.

Response Transaction Log
Lets you select an element that has an eHealth Application Response agent and drill down to the Agent Transaction Viewer (ATV).

Note: This feature requires an eHealth Response License.

Alarm Information for Systems with eHealth AdvantEDGE View
If your eHealth system has an eHealth AdvantEDGE View license, you can select a system that has a SystemEDGE agent license and select the following drill-down options:

System Information
Displays an eHealth AdvantEDGE View query for the system that you selected, showing high-level information such as system name and location, operating system, basic system resources, and so on.

Performance Information
Displays an eHealth AdvantEDGE View query showing overall performance statistics for the selected element.

Event Information
Displays the eHealth AdvantEDGE View query showing the event information for the element selected, including the complete trap contents. This is available only if your system also has an eHealth Live Health Fault Manager license and the element has an event alarm. You can view, edit, disable, or delete the triggering monitoring entry on the source host. This lets you tune thresholds that were set incorrectly. If you want a high-level view of the alarms in a group or group list, use Live Status to obtain this information.
Administrator Tasks for Live Health

If you have administrator privileges for Live Health, you can also perform many additional tasks, including the following:

**Manage rules, profiles, and associations**

You can modify the rules, profiles, and associations that Live Exceptions automatically applies to your system. Initially, if many alarms appear in the browser, you can collapse rows to reduce the number of alarms in view. This lets you view the alarms generated by Live Exceptions while you determine whether the rules apply to your infrastructure.

Review the associations that are applied to your groups and group lists. The Monitored Subjects Summary Report provides an overview of subjects (groups or group lists) and the profiles associated with them. The Monitored Subjects Detail Report provides detailed information about the elements in a group or group list and their associated rules and profiles.

After reviewing the reports and viewing the generated alarms, you may determine that you want to modify the default information. While you cannot modify or delete the default rules and profiles that come with Live Exceptions, you can work around this restriction.

**Clear alarms**

Alarms that you know are not problems may appear in the browser. You can remove these alarms from the browser. Alarms remain cleared until Live Exceptions determines that the alarm condition has occurred again.

**Create notification rules**

You may want to be notified if certain alarms appear in the browser. Live Exceptions can send email, send a trap, or run a command when a specific alarm occurs. For example, you can specify that Live Exceptions sends an email to another user when an alarm occurs for a group being monitored by a specified profile with a specified rule message.

**Modify the Event Chart history time**

By default, Live Exceptions maintains a count of alarms for the previous two days in the Event Chart. You can modify the information.

**Note:** For information about how to perform these tasks, see the online help.
Rules

Rules define the conditions to monitor availability, thresholds, duration, and severity. Rules are grouped into profiles for easier administration. Each profile contains one or more rules that are applied to a subject (such as a group or group list).

There are four types of rules:

**Availability**
Generates an alarm when an element is unavailable.

**Reachability**
Generates an alarm when an element does not respond to a ping or an SNMP Get request.

**Variable**
Generates an alarm when data for a specific performance variable exceeds service thresholds. These alarms are based on three condition types: Time over Threshold; Deviation From Normal; and Time Over Dynamic Threshold.

**Event (trap)**
Generates an alarm when Live Exceptions receives traps.

Availability, reachability, and variable rules are processed for alarm conditions once during each polling interval (the default is five minutes). Event rules are processed when traps are received. Live Exceptions keeps an alarm active until the condition specified by the rule no longer exists or is manually cleared.

Profiles

Live Exceptions provides out-of-the-box *profiles* (collections of rules) that you can associate with groups or group lists of elements to specify the performance thresholds you want to apply to them. You can also tailor rules to reflect existing service level agreements (SLAs).

Service level agreements (SLAs) are common between IT departments and the users they serve. A structured service-level management approach is necessary to meet your SLAs. You can use the Live Exceptions Browser as part of real-time service monitoring; alarm profiles can be set relative to your service levels so you know when you are nearing an SLA violation and can take steps to restore performance before users complain or you incur contractual penalties.
Thresholds are important even in less formal settings. For example, you may want to inform management of serious problems as they occur, but not notify them of every minor alarm that IT addresses. You can create a separate profile for management with a higher threshold than IT uses, so that only the more serious issues are escalated to management.

**Examples: Time Over Threshold and Deviation from Normal Algorithms**

- In this example, this rule uses the Time Over Threshold algorithm. It identifies occurrences when a threshold (router CPU utilization greater than 60%) is exceeded for a certain amount of time (15 minutes out of one hour). This algorithm eliminates redundant and meaningless alarms that tell you of every instance when router CPU utilization exceeded 60%. Instead, Live Exceptions generates a *single* alarm when the conditions for the alarm rule are first met, and it clears the alarm when the conditions are no longer true.

  Generate an alarm when router CPU utilization exceeds 60% for 15 minutes (collectively) out of one hour.

  This technique is called *alarm consolidation*, and it lets IT staff identify and focus on solving problems without being sidetracked by repeated events.

- In this example, this rule uses the Deviation From Normal algorithm. Using a historical baseline, it identifies when an element’s performance is unusual compared to normal behavior patterns. For example, the performance of an element at 2:00 p.m. on Tuesday is compared to the performance of that element at 2:00 p.m. on previous Tuesdays. Since performance is measured against a baseline that is unique to your environment, this is a more powerful level of analysis than observing a flat threshold.

  Generate an alarm whenever router CPU utilization is outside 1 standard deviation of baseline performance for 15 minutes (collectively) out of one hour.

**Profile Customization**

As a best practice, begin to monitor your groups using the default profiles. Based on the alarms you see, you can decide to create your own alarm rules and profiles to better suit your specific infrastructure. For example, you may be responsible for only a certain set of resources. To eliminate alarms from other resources, you can copy and modify the default profile by deleting the alarm rule for conditions you do not need.

You can also lower thresholds to give yourself more time to rectify a problem that may endanger your SLAs. If you have established meaningful thresholds for performance problems and defined them in your eHealth report service profiles, you can create customized Live Health profiles based on that data.
For more information about Profiles, see the Live Health Profile Descriptions on the Device and Technology Certification page of the CA Support Web site (http://support.concord.com/devices).

Security Considerations

Live Health has two types of users: administrators and general users. General users can view alarms but have minimal management capabilities. Administrators can establish access and SLA policies to control the permissions a user has to change Live Health management policies.

Administrators can also enhance security by using Web user account permissions to filter the types of elements and groups that a user can see. For example, if you limit a user to see only LAN/WAN elements in the group named Sales, the user’s Live Exceptions Browser only shows the alarms for that technology and the elements in that group. In the case of an ISP using Live Health, Web user account permissions can be set so that the ISP’s administrator for Smith Corporation can only see and monitor information for Smith Corporation. This ensures the privacy of the ISP’s other customers and lets the administrator focus solely on the Smith Corporation.

Live Trend

Live Trend is a real-time charting tool for monitoring statistics elements polled by eHealth. It identifies affected elements to view performance patterns for your IT infrastructure and helps you determine the nature of a failure or slowdown by monitoring multiple variables in real time. It also lets you monitor continuous real-time performance to determine whether your corrective action is working.

For a majority of alarms (except traps), you can select the alarm and drill down to Live Trend. Live Trend creates charts that monitor the elements you are polling using eHealth.

You can use Live Trend charts to plot the following:

**Element trends**

- A single element with multiple variables, which can indicate element problems and their possible causes

**Variable trends**

- A single variable for multiple elements, which can highlight problems, such as response time, for multiple elements.

Live Trend updates the charts each time eHealth polls the elements. You can display as-polled data, with charts updated every five minutes, and fast-sampled data, with charts updated every 30 seconds. You can also preload the chart with up to 48 hours of history.
From an alarm in Live Status or the Live Exceptions Browser, you can drill down to a Live Trend report for seamless real-time monitoring of troublesome elements. This streamlines the resolution process, helping the operations team resolve performance problems quickly. Since all report drill-downs are configured automatically, the operations team uses its time more effectively, taking action to improve performance and availability rather than configuring diagnostic reports.

Live Trend can be launched at any time, not just as a drill-down from an alarm.

**Live Health Fault Manager**

The eHealth Live Health Fault Manager feature receives SNMP traps from various sources and sends them to Live Exceptions for analysis and processing. This component lets you use Live Exceptions to analyze performance data from sources other than eHealth polled data, such as certified SNMP agents and network devices. Live Health Fault Manager lets you apply the same set of performance standards to all elements of your IT infrastructure and receive intelligent, consolidated alarms when problems occur.

When Live Health Fault Manager receives traps, it processes the data the same way as data collected by eHealth: it compares the performance statistics to rules defined in profiles and generates intelligent alarms when thresholds are exceeded. You can view these alarms in Live Status and the Live Exceptions Browser, which provide access to element-specific drill-down information when available.

**Case Study: Keeping Customers by Maximizing Uptime**

The end users of a major international telephony were complaining that they could not access critical applications in a reasonable amount of time. Since customer satisfaction was critical to this company’s continued growth, no instance of substandard service was considered acceptable.

To address this problem, the company needed to be proactive, find response time problems before users were affected, and address them immediately at any time of the day or night. The company installed Live Health.

Almost immediately, the Live Exceptions Browser identified several critical system problems. Drilling down on At-a-Glance and Trend reports for the most critical items told the company that server disk utilization was dangerously high, and several WAN links were overutilized, which was the major cause of the poor performance.
The following is a sample At-a-Glance report showing WAN links approaching critical usage levels:

**At-a-Glance Report**

A few days later, a critical application server began experiencing problems late on a Saturday night. Live Exceptions identified the problem, and using the Notifier, immediately paged the on-call IT personnel. When IT personnel checked in, Live Status revealed that the server was approaching maximum capacity, and critical applications were running slow enough to draw complaints from users. Using Live Exceptions, they drilled down into the heart of the problem with an At-a-Glance report, which illustrated the out-of-bounds conditions, how they related to other system functions, and how long they had been out of bounds. A Trend Report showed them how severe the CPU’s condition was.
The following sample Trend report shows severely erratic CPU performance:

Live Trend provided up-to-the-minute views of system performance to contrast with recent historical data; the Live Trend data reinforced the problem diagnoses. By adding hardware and reducing the number of processes and applications running on that particular server, along with minor operating system and application tuning, they were able to bring application response times back down into their acceptable range. Running new Trend reports and monitoring Live Exceptions for recurring alarms assured them that peak performance had been restored to their end users and a possible critical failure had been avoided.
Introduction to Traffic Accountant

eHealth Traffic Accountant analyzes the traffic sent between the nodes in your network and between nodes or autonomous systems on the Internet. Traffic is any data that is sent from one node to another node or from one autonomous system to another autonomous system.

Traffic Accountant collects and analyzes traffic from RMON2 probes and Netflow collectors. Currently Traffic Accountant supports only the Cisco Netflow Collector and the eHealth Netflow Collector.

If you purchase an eHealth Traffic Accountant license, you can generate Traffic Accountant reports to analyze the traffic in your Information Technology (IT) infrastructure from the eHealth console or your web browser (if your web user account is configured appropriately).

The eHealth Netflow Collector is integrated with Traffic Accountant as one package and does not require dual licensing.

Traffic Accountant reports show how nodes, autonomous systems, and applications use your network. You can use this information to analyze the network and solve problems. These reports can help you determine the following information:

- The nodes or autonomous systems that use the network most frequently
- The nodes or autonomous systems that use specific nodes or autonomous systems
- Whether any unassigned nodes are accessing certain network resources
- The volume trends for a node or autonomous system, group of nodes or autonomous systems, or a network segment
- The applications that are used most frequently on the network, by a certain node, an autonomous system, or on a network segment
- Traffic usage patterns for cost-effective partnering
You can use this information to plan and implement network reconfiguration, growth, and security procedures, as well as to relate network costs to the nodes, autonomous systems, and organizations that use the network.

For more information and procedures, see the *Traffic Accountant and Netflow Administration Guide* and the online help.

**Netflow Collectors**

Traffic Accountant monitors Netflow probes through the following methods:

- Using the Cisco Netflow collector through the integration module using legacy (non-enhanced) mode
- Using the Cisco Netflow Collector through the integration module using enhanced mode
- Using the eHealth Netflow Collector in enhanced mode

*Legacy* mode lets you run the Netflow Import Poller using the nhiImportNetflow module that existed in previous releases.

*Enhanced* mode lets you run the Netflow Import Poller using the NhiEhImportNetflow module to support more Netflow data available in your network. The NhiEhImportNetflow module updates the new set of Traffic Accountant database tables that are the foundation for the new Cognos Traffic Accountant reports in the eHealth Report Center. The NhiEhImportNetflow module imports both Node-to-Node and AS-to-AS data at the same time.

You use the legacy mode and enhanced mode in the same manner to perform setup, discovery, and polling.

**Traffic Accountant Reports**

eHealth offers the following types of Traffic Accountant reports:

- Quick Start
- Standard
- Cognos Report Center
- Customized

For information about how to use these reports, see the *Traffic Accountant Administration Guide* and the online help.
Quick Start Reports

Quick Start Traffic Accountant reports are a set of seven predefined reports that you can use to quickly obtain traffic information about a specific node or autonomous system, a specific probe element, a view or a group within a view, or the entire network.

You can run these reports to familiarize yourself with Traffic Accountant reports, as well as to help you to identify the following:

- Most active nodes or autonomous systems
- Nodes or autonomous systems that communicated with a node or autonomous systems
- Applications that are used most frequently
- Conversations that occurred on the network

Standard Reports

Standard reports are a set of defined reports that provide information about typical traffic and volume information for one or all nodes, a view, a group, and one or all probe elements. You cannot change or delete the standard reports. However, you can use them as templates for customized reports.

The standard reports provide you with more analysis and support features than the Quick Start Traffic Accountant reports. With standard reports, you can do the following:

- Use views and groups to refine the reports.
- Specify report intervals and report periods.
- Send reports to a PostScript printer; display them through a web browser; or save them as ASCII or PDF.
- Schedule reports.

Standard reports are grouped into eight categories:

- Custom
- Group
- Node
- Security
- Cost Allocation
- Network
Cognos Report Center Reports

Traffic Accountant offers Cognos Report Center reports for the Netflow tables when you use one of the following scenarios:

- eHealth Netflow Collector and Netflow Import Poller (in enhanced mode)
- eHealth Netflow Collector only

To switch the import poller from “legacy” mode to “enhanced” mode you must rerun the Netflow Import Poller configuration utility.

Some legacy reports are also available as Cognos reports. The Cognos versions of these reports are based upon the data collected by the Netflow Collector and the Netflow Import Poller.
Types of Report Center Reports

The following reports are available in Report Center for use with Traffic Accountant:

**Group Conversation Log Text report**
Shows the groups that communicate with a specified group and the total traffic volume for each group partner. This report helps determine how much to bill groups for using a group.

**Allocations By Service Provider report**
Shows percentage of traffic addressed to each BGP-Next-Hop for an optionally selected TA node group. This report helps determine how much to bill groups or clients for using a particular service provider or BGP connection, depending on whether you run the report for enterprise clients or service providers.

**Group Partner For Group report**
Shows the percentage of the group’s traffic volume for the top group partners.

**Group Partners Over MPLS (VPN) For Group report**
Shows which groups communicate with a selected node group over MPLS(VPN) and the amount of traffic.

**Applications For All Nodes report**
Shows the percentage of network traffic used by the top protocols in the network.

**MPLS Network Summary report**
Provides packet and byte counts for traffic on an MPLS network based upon label type (such as VPN, BGP, and so on), label, and next_hop during the time interval you select. This report helps determine the nature of the traffic using an MPLS network.

**Node Partners of a Server report**
Shows the node partners that communicate most with a server and the subnet in which the node partners belong. It also shows which applications are used by the node partners.

**Node Partners of a Service Provider report**
Shows the node partners that communicate most with a service provider (such as BGP-Next-Hop). It also shows which applications are used by the node partners.

**Most Active Nodes for Application report**
Identifies the nodes that are using an application the most, and how much traffic they are sending and receiving. The busiest nodes are likely to be servers.
**All Service Providers Seen by a Probe report**

Identifies the service providers (such as BGP-Next-Hop) who serve as destinations or sources of traffic on the selected network link. This report helps determine how much traffic is being sent to and received from service providers or clients.

**TopNodes For View/Group report**

Shows that top nodes with the highest volume in the view. The report also calculates the top applications used in the view. This report displays the information based upon the entire Traffic Accountant View rather than for a particular Traffic Accountant Group within a Traffic Accountant View.

**Top Groups And Service Providers report**

Shows the top node groups and their Service Provider destinations for the selected view. For enterprise clients, this report tells which service providers the top groups in a view use. For service providers, this report tells which clients the top groups in a view use.

**Most Active AS-to-AS conversations on a Netflow Interface**

Shows traffic volume for common source and destination autonomous systems (AS) and type of service (ToS) as seen by a selected Netflow interface. This report helps determine what the Type of Service (ToS) breakdown is for the most active AS-to-AS conversations on a particular network link.

**Most Active AS-to-AS conversations by service provider**

Shows traffic volume for common BGP Next Hop, source and destination AS and type of service ToS as seen by a selected Netflow interface. This report helps determine the ToS breakdown of the most active AS-to-AS conversations by service provider.

**Node-To-Node Conversations - All Nodes**

Shows traffic volume for the most active conversations on the network and which applications or protocols were used by those conversations.

**Top-AS-to-AS-conversations-detail report**

Shows traffic volume for common source and destination IP addresses, source and destination AS name and number, in and out interfaces, protocol and source and destination port as seen by a particular Netflow interface. This report helps determine the most active flows within AS-to-AS conversations on a specific network link.

For more information about the Traffic Accountant reports available through Report Center, see the online help.
Customized Reports

You can define your own customized Traffic Accountant reports to obtain specific information about your network. Customized reports can be variations of the standard reports or new reports that you create.

Create customized reports to obtain information about your network that the standard reports do not offer. Also, you can copy a standard report and modify it to change the format or the report parameters. eHealth automatically assigns all customized reports to the Custom category.

You can customize a Traffic Accountant report by creating a new customized report or by modifying a copy of an existing report (standard or customized).
Chapter 7: User Interfaces to eHealth

This section contains the following topics:

- User Interfaces (see page 83)
- eHealth Console (see page 83)
- Command Line Interface (see page 84)
- OneClick for eHealth (see page 85)
- Web Interface (see page 85)
- Administrator Roles (see page 89)

User Interfaces

The eHealth software offers four user interfaces (UIs):

- eHealth console
- eHealth command line interface (CLI)
- OneClick for eHealth (OneClickEH)
- eHealth Web interface

Not all functions are available through every eHealth interface. eHealth documentation provides guidelines for selecting the most efficient and practical method to perform a particular task. Choose the method with which you are most comfortable.

Note: Only authorized users have access to the eHealth console and the command interface.

eHealth Console

The eHealth Console lets you perform key administration tasks such as discovering and managing elements, adding scheduled jobs to automate tasks, and loading and saving the database.

You can access the following administrative features through the eHealth console menus:

Setup

Lets you perform the following administrative tasks:

- Perform an interactive discovery, and discover NetFlow probe elements.
- Manage the poller configuration.
CREATE and modify scheduled report jobs and discover jobs.

Change global console settings.

**Reports**

Let you perform the following administrative tasks:

- Run and customize reports.
- Manage service profiles for reports.
- Create and edit Traffic Accountant views.

**Database**

Let you perform the following administrative tasks:

- Load a new database, and save (back up) your database.
- Save system messages to a log file.

---

**Command Line Interface**

The eHealth command line interface (CLI) lets you run commands from a console or terminal window. Some command functions are also available through one of the administrative interfaces, but many advanced functions are available only through the CLI. For example, while you can use the job scheduler interface to modify the time at which a scheduled job runs, you must use the `nhSchedule` command to create new job types.

You can use the CLI to automate tasks by using scripts. The command line interface also makes available some advanced functions that are not available through the eHealth console.

For more information about commands, see the *Command and Environment Variables Reference Guide*. 
OneClick for eHealth

OneClick for eHealth (OneClickEH) acts as the main administrative interface to the eHealth system. You can launch this application from any Web browser and work simultaneously with other administrators to manage all of your eHealth systems. From this interface, you can perform a wide array of tasks such as:

- Monitor and manage all your eHealth systems.
- Manage groups and group lists.
- Schedule and manage jobs.
- Manage user accounts.
- View your element hierarchy.
- Discover elements.
- Manage discover policies.
- Manage Database Configuration Information (DCI) rules for use in Discover.
- View discover logs.

The Discover portion of the OneClickEH interface provides tabs that represent each aspect of the discover process, including a rules editor, policy set editor, scheduler, and Traffic Accountant view editor.

OneClickEH displays a tree structure on the left with access to the administrative functions. On the right, it displays a high-level status summary. From this window, you can access more information by drilling down to various functions.

To access the complete range of features available with OneClickEH, you must upgrade to the latest version of eHealth. A single OneClickEH interface can manage multiple eHealth systems, even if they are mixed versions.

**Note:** For more information about system requirements, see the Release Notes. For more information about using OneClickEH, see the online help.

Web Interface

The Web interface lets you view eHealth reports and other features from a remote system using a web browser. With this interface, you can view scheduled reports, run reports on demand, or use other authorized functions, regardless of whether they are local or remote.
Different groups of users can use the eHealth Web interface, including the following:

- Network Operations Center (NOC) administrators
- System administrators
- Network planners
- Chief Information Officers (CIOs)
- Application managers
- Consultants and analysts
- Service providers and their customers
- eHealth administrators

Users can use the Web interface to perform the following tasks:

- Access the OneClick for eHealth user interface
- View scheduled reports, including MyHealth reports.
- Run and view reports on demand.
- Download Live Exceptions, Live Status, and Live Trend.
- Manage eHealth Application Response and AR agents.
- Manage eHealth AdvantEDGE View and SystemEDGE agents.

Users can see only those functions or pages of the Web interface that they are permitted to use. The eHealth Web administrator controls access to the Web interface with Web user accounts and access settings, specifying which functions each user can access. The eHealth Web administrator can also customize the Web interface for your organization.

For more information about using the Web interface, see the online help.

**Overview of Web Pages**

The eHealth Web interface is organized as tabs to simplify your use of eHealth reports and applications as follows:

**Gateway**

Provides direct access to the information, applications, and Web links users require. By default, this page provides links to information available at the eHealth Support Web site (support.concord.com), including Technical Support contact information, information on certified devices, and white papers. Typically, your eHealth Web administrator customizes this page to meet the needs of your organization’s eHealth users.
Web Interface

Organization

Lets you view the structure of your organization and list available reports based on how elements are organized: by element, node, group, and group list. For example, you can select a group and view or run reports for that group. Viewing the structure of your organization helps you think in terms of the organization of your IT infrastructure, rather than in terms of which report you need to access to learn about a certain group of elements.

Report List

Provides a list of all generated reports that you can view. These reports can include scheduled reports and reports that were run on demand from the Web interface.

eHealth sorts the reports in reverse order by date, with the most recent report at the top of the list. To sort the reports differently, click a column heading; for example, click Title to sort the reports by report title.

You can filter the report list by subject, technology, report type, date, and whether the reports are scheduled.

Run Reports

Lets you run reports on demand. Running reports on demand can take time because eHealth may need to analyze the data that appears in the reports.

If you plan to run a certain report regularly, you can save the report definition.

MyHealth

Provides access to your MyHealth reports, each of which contains a series of charts and tables tailored to your specific interests. MyHealth lets you customize reports to show only the elements and groups that you consider critical.

If you or your eHealth Web administrator has already specified a MyHealth report, it appears on this page automatically. If the MyHealth page is empty, ask your eHealth Web administrator to create a report or to give you permission to create your own MyHealth report. You can use the Preview feature to check the layout of your MyHealth report, but you will need to wait (typically overnight) for the first report to generate.

Live Health

Lets you download Live Status, Live Exceptions, the Business Service Console, and Live Trend to the client desktop.
System & Apps

Provides access to three major eHealth applications:

■ eHealth AdvantEDGE View, the Web-based user interface and element manager for use with SystemEDGE agents
■ eHealth Application Response
■ Service Availability

You can use eHealth AdvantEDGE View to deploy, manage, and configure SystemEDGE agents and Application Integration Modules (AIMs); query SystemEDGE agents; and search MIBs.

Note: For more information about eHealth AdvantEDGE View, see the online help.

eHealth Application Response lets you manage Application Response agents; monitor specific business applications and view transactions of a selected application; identify servers associated with those applications; and download Application Response tools.

Service Availability lets you create and manage Service Availability tests, Service Availability test agents and test sets, and Service Availability test profiles; and monitor and generate reports on Service Availability agents and tests.

Administration

Provides access to administrative functions for authorized users and eHealth Web administrators. Authorized users can use this page to perform the following User Management functions:

■ Change your password.
■ Log in to a different user account.
■ Set user preferences.

eHealth Web administrators can use this page to perform management functions such as accessing OneClick for eHealth, obtaining scheduled job status, managing the web site configuration, reviewing access logs, enabling advanced logging, and removing reports marked for deletion.

Note: For more information about how to use the Web interface, see the online help.
Access the eHealth Web Interface

Before you can access the eHealth Web interface, you must obtain the following information from your eHealth Web administrator:

- The URL of the eHealth Web server
  
  The URL will use one of the following formats:
  
  - http://ipAddress
  - http://hostname.domain
  - http://hostname.domain:port

- User name and password

You can access all functions of the eHealth Web interface for which you are authorized. Only tabs that you are permitted to view appear in your eHealth Web interface.

To access the eHealth Web interface, click a tab on the navigation bar to access a Web page.

Online Help Access

The eHealth Web interface provides an online help system. You can access the online help using a Web browser to access the URL http://hostname/help/WebHelp/starthelp.htm, where hostname is the name or IP address of the eHealth system.

eHealth Web interface also lets you access the help from links within the interface. In the main Web interface tab navigation bar, the Help link opens the online help.

Administrator Roles

For most eHealth sites, the eHealth administrator who manages the eHealth console is also the administrator of the eHealth Web interface and OneClickEH. However, in larger sites these responsibilities might be shared by different people.

To administer the eHealth Console and CLI, you must log in to the eHealth system using an operating system account that has eHealth administration privileges.
To administer OneClickEH and the Web User Interface, you must log in to the eHealth system using a special eHealth web user account named admin. This account lets you configure these interfaces, control user access to them, and assign limited administrative privileges to other web users. By default, the eHealth web user account does not have permission to log in to OneClickEH.

Administrators can use secondary eHealth consoles to perform a subset of the tasks that can be performed from the primary console; however, secondary consoles consume system resources and can impact system performance.

**Note:** For more information, see the *Administration Guide*. 
Chapter 8: AdvantEDGE View

This section contains the following topics:

- Introduction to AdvantEDGE View (see page 91)
- Administrative Tasks with AdvantEDGE View (see page 91)
- User Tasks with AdvantEDGE View (see page 92)

Introduction to AdvantEDGE View

AdvantEDGE View is the Web-based graphical user interface and element manager that can receive and display data that is collected by SystemEDGE and the eHealth application insight modules (AIMs). AdvantEDGE View can also automate the deployment, licensing, and configuration of SystemEDGE agents and eHealth AIMs.

You can access AdvantEDGE View from the Systems & Apps tab of the eHealth Web interface to manage and monitor SystemEDGE agents and other SystemEDGE modules, such as eHealth AIMs.

AdvantEDGE View is installed as part of the eHealth Web interface, but you must have an AdvantEDGE View license to access the AdvantEDGE View tab from the eHealth Web interface. After you install and license AdvantEDGE View, you can access it from a Web browser.

For more information about AdvantEDGE View, see the eHealth Help.

Administrative Tasks with AdvantEDGE View

Your eHealth Web administrator sets up your user account, including your ability to access the AdvantEDGE View page and your user permissions for AdvantEDGE View.

If you are an eHealth Web Administrator, the following tasks can be performed for AdvantEDGE View users:

- Manage user accounts as follows:
  - Provide users with access to the Systems & Apps tab (under General Configuration).
  - Set user permissions (under AdvantEDGE View Configuration).
- Provide access to the Systems & Apps tab.
- Set user permissions for AdvantEDGE View.
User Tasks with AdvantEDGE View

After your AdvantEDGE View account is set up by an administrator, you can run queries on systems and applications and view configuration information for the SystemEDGE agent. Depending on your permissions, you may be able to perform the following additional tasks:

License Agents and eHealth AIMs

If you have Write or Admin permissions, you can use AdvantEDGE View License Management to license SystemEDGE agents, eHealth AIMs, and other SystemEDGE modules that eHealth discovered. You can also automatically license agents and eHealth AIMs when you are deploying them.

Run Queries

AdvantEDGE View provides a number of queries for monitoring performance, configuration, network operations, and client and server connections for systems and groups. You can query systems on which the SystemEDGE agent is installed and licensed.

Run Application Queries

AdvantEDGE View provides queries for the application-specific data that the eHealth AIMs collect. You can query systems on which the SystemEDGE agent and the appropriate eHealth AIM are installed and licensed.

View and Modify SystemEDGE Configuration Information

AdvantEDGE View provides a user interface for viewing and modifying the monitoring entries in the sysedge.mon configuration file. The SystemEDGE agent uses two configuration files: sysedge.cf and sysedge.mon. The agent reads both files, but the sysedge.cf file is the main configuration file. Entries in sysedge.cf take precedence over entries in sysedge.mon, which serves as a backing store for the agent’s self-monitoring tables. The sysedge.cf file is static; you cannot edit it remotely. The sysedge.mon file is dynamic, which means that AdvantEDGE View (and other management software) can update sysedge.mon through SNMP sets. When you edit the SystemEDGE configuration through AdvantEDGE View, you are modifying the sysedge.mon file.
Deploy Agents and eHealth AIMs

If you have Admin or Deploy permissions, you can deploy SystemEDGE agents, Application Response agents, eHealth AIMs, and other SystemEDGE modules from AdvantEDGE View.

Create and Apply Configuration Templates

If you have Deploy or Admin permissions, you can create, modify, and apply configuration templates for the SystemEDGE agent. Templates are text files that contain a series of configuration directives for the SystemEDGE agent. Each template can include entries for any or all of the SystemEDGE monitoring tables. Depending on your permissions, you can use the Template Manager to create, edit, copy, rename, and delete templates.
Chapter 9: eHealth and Voice Over IP

This section contains the following topics:

Voice Over IP (see page 95)
eHealth VoIP Management Support (see page 96)
Analog Telephones and PBXs (see page 97)
Voice Gateways (see page 97)
IP Telephones (see page 98)
QoS-Enabled Routers (see page 99)
Management and Monitoring of Voice Quality (see page 99)
Cisco IP SLA Routers (see page 102)
Manage Network Resources (see page 102)
Service Level Reports for VoIP (see page 103)
At-a-Glance Reports for VoIP (see page 106)
Trend and Top N Reports for VoIP (see page 106)
Quality of Service (QoS) Reports (see page 107)
Reports for Voice Quality with Cisco SA (see page 107)
Additional Queries for VoIP Components (see page 108)

Voice Over IP

In most networks, voice traffic travels over a public switched telephone network (PSTN), while workstation and application data travels over an IP-based wide area network (WAN). However, a WAN can also be a converged network — it carries both traditional data such as email, FTP, and business applications, as well as voice traffic such as telephone calls, teleconferences, and voice mail.

Most data networks use the Internet Protocol (IP) as the networking standard for connecting their LANs and WANs. Voice traffic carried by an IP-based network is referred to as Voice over IP (VoIP).

To manage VoIP, you must be able to test, monitor, and report on call quality to help ensure that users have clear calls. You want to know about problems with voice quality or outages quickly and whether your network can support the amount of voice traffic that you expect. In addition, you need to be certain that your network can still carry and process your non-voice data traffic. You might also want to be certain that your voice traffic can be routed back into the PSTN if network problems occur.

The VoIP management picture is complex, with many components to consider such as routers, call manager clusters, systems, analog telephones, and IP telephones. eHealth for Voice and the eHealth suite of products provides end-to-end visibility into this picture.
Note: For more information about eHealth for Voice, see the eHealth for Voice documentation.

eHealth VoIP Management Support

With the eHealth VoIP license, you can discover and report on voice gateways, DS0s, and gateway peer-to-peer links. The following eHealth VoIP products help you monitor key VoIP-related areas:

**eHealth Response**

Lets you create response paths to test and monitor jitter (interpacket delays) throughout your network. If you have Cisco routers with IP SLA support (formerly SAA), you can create response paths to test for jitter between the routers across your LANs and WANs.

**eHealth Quality of Service (QoS)**

Lets you monitor your QoS-enabled devices. You can monitor your network to be certain that your traffic policies are optimized for voice traffic support and obtain reports about how well your QoS-enabled routers are managing the various types of traffic in your network.

**eHealth Live Health and Fault Manager**

Helps you monitor your VoIP resources for immediate notifications of problems with gateways, QoS, and jitter.

**The eHealth Voice Quality Monitor module**

Lets you monitor and test voice quality within your network, plan for capacity and growth, and troubleshoot voice quality problems. In eHealth 5.7, VQM can run on Red Hat Linux Release 3 (Advanced Server and Workstation).

Note: For more information about platform support, see the Getting Started with eHealth Voice Quality Manager focus topic and the related online help files.

**eHealth for Voice**

Provides comprehensive performance management and reporting for TDM and VoIP voice systems, such as Avaya and Nortel communications servers and voice messaging systems. eHealth for Voice performs data retrieval and reports on system and network traffic, system events and a variety of other information. The product suite covers the portfolio of Avaya Definity and Communication Manager Platforms, Avaya Octel and Intuity Messaging systems (including the new Modular Messaging Platform). eHealth for Voice also supports Nortel Networks Meridian.
eHealth for Voice

Provides IP connectivity for data collection from legacy voice systems.

Integrated VoIP reports

Provides multi-technology service level reports that show trends and performance of the VoIP resources and MOS values.

To fully manage all the parts of your VoIP network, you can combine the eHealth VoIP solutions with the existing eHealth management solutions for your LAN and WAN interfaces, routers, switches, applications, and systems.

Analog Telephones and PBXs

An analog telephone is a typical telephone like those found in residences or most business offices. They convert the human voice to an electrical analog signal and then send the signal on a twisted-pair telephone wire.

Residence telephones are connected directly to the telephone service provider’s central office. In a business site, you may have private branch exchange (PBX) devices to manage multiple analog phones. The PBX usually connects many telephones to one or more leased telephone lines, letting users share the circuits available on the leased line.

Management of Analog Phones and PBXs

Analog telephones usually do not have any type of SNMP agent or MIB to collect performance data. PBXs may have an agent; at this time, no PBXs are certified for eHealth. Thus, eHealth cannot discover either of these devices.

If your PBX or another application collects data for the phones or PBX, you can use the eHealth developer tool kit to create custom element types and import the data. You can then create Live Health profiles to monitor your variables and run reports for the elements. This is very specialized eHealth work; make sure that you need to manage at this level before attempting it.

Depending on the PBX vendor, PBX devices can be very similar to systems or switches. Sometimes you can use eHealth to discover PBXs as systems or switches, and manage them for general health and availability.

Voice Gateways

If you have analog phones and PBXs, you can add their traffic to your existing data network by connecting the PBX to a voice gateway. A gateway is a device that converts signals from one format to another.
A voice gateway converts analog telephone signals into digital signals and can also convert T1/E1 digital signals into packets. It then processes the packets for transmission on the data network. Voice gateways on the receiving end of a call collect the digital voice signals and convert them back into analog signals.

Voice gateways may have links to the PSTN to help route traffic into the PSTN when there are network problems or congestion. They also have logical links to other voice gateways to help them quickly process calls and better manage the traffic across the network. These links are referred to as gateway peer-to-peer links.

**Manage Voice Gateways**

eHealth can discover and manage voice gateways using Remote Access Server (RAS) mode. Depending on the gateway hardware you use and the certification support, eHealth typically creates elements for the voice gateway device itself, each CPU, and each digital signal processor (DSP) card on the gateway.

If your gateways have peer-to-peer links with other gateways, eHealth creates voice gateway peer-to-peer link elements to monitor traffic statistics between them.

If you discover the gateway using LAN/WAN mode, you can create LAN/WAN elements for the gateway interfaces, such as the T1/E1 lines linking the gateway to the local area network or the trunks to the PSTN, and thus monitor the traffic on the interfaces from the gateway.

**IP Telephones**

An IP telephone is a telephone or device designed for use with IP networks. Similar to computers and other LAN devices, IP telephones connect into a standard LAN port in an office. Typically, you connect several IP telephones to a LAN switch that multiplexes the voice traffic into the IP network.

**Management of IP Telephones and LAN Switches**

eHealth cannot manage and report about individual IP telephones.
eHealth can manage the LAN switches; you can discover them using Router/Switch mode. Depending on the hardware and the certification support, eHealth typically creates a switch parent element, an element for each CPU, and elements for each interface or link from the switch to the IP network. eHealth reports show aggregated statistics for all the interfaces unless you configure the interfaces to collect detailed data. You can then report about statistics for the individual lines.

**QoS-Enabled Routers**

Your routers manage the flow of traffic across your LANs and WANs. In a VoIP network, routers are often configured to use Quality of Service (QoS) features to prioritize the voice traffic.

QoS-enabled routers are configured to recognize various types of traffic such as voice traffic, critical business application traffic, and general traffic such as email. They can also allocate a percentage of available bandwidth to each traffic type to make certain that your most important traffic gets the largest percentage of bandwidth. To manage the traffic, QoS-enabled routers can discard and delay packets that exceed assigned limits, and under high congestion conditions make sure that the most important traffic gets through before any less critical traffic.

**Manage QoS**

If your routers are QoS-enabled, you can discover them to create elements for each defined class of service (CoS). You can then monitor how well they are managing traffic prioritization and flow.

You can monitor the routers to determine whether voice traffic is being delayed or discarded, which gives you the information you need to change the QoS configuration and help ensure that the voice traffic gets through.

**Management and Monitoring of Voice Quality**

For internet voice telephony products, the Mean Opinion Score (MOS) value serves as the indicator of line quality. The MOS value is a number from 1 (worst) to 5 (best) that represents the quality of a voice signal.

High-quality signals are clear; listeners can discern the words as well as the speaker. Low quality signals may not be understandable or recognizable.
MOS testing began as a survey of the opinions of actual users who listened to prerecorded phone messages. They assigned a grade of 1 to 5 to reflect their opinions of the voice quality. The average grade for each message was the MOS value.

Rather than survey users, however, VoIP network providers require continuous, automatic monitoring of the MOS values. They need to know that call quality is stable, and they want early notice when voice quality begins to degrade (that is, when MOS values start to drop).

A MOS score of 5 is not possible over a data network. A MOS score of 4 is equivalent to toll quality calls. Any score below 4 is less than acceptable quality in most cases.

For VoIP connections, the quality of the telephone signal depends on a number of factors:

**Codec Implementation**

Codec (compression/decompression) standards define how a voice signal can be digitized and then compressed for best transmission over data lines. Various codec standards exist; some offer better voice quality, but your network requires more bandwidth to support that traffic. Other codes use less bandwidth, but the voice quality will be lower. VQM supports codecs for G.711, G.723-1 + VAD, and G.729 + VAD.

**Packet Loss and Discards**

When voice packets are lost, “gaps” occur in the compressed voice traffic. Telephony providers employ various techniques to cover the missing packets; they can replace the packets with “noise”, silence, or repeat the last received packet to fill the signal.

**Delay**

While delay does not typically result in loss of voice data, it does result in problems for users. Delay of greater than 200 milliseconds can result in some awkwardness in transitions from speaker to listener.
Jitter

Jitter is the variation in timing between packets sent on a network. Typically, jitter is irrelevant for data packets that carry traffic for applications such as FTP or email, but it is crucial for voice-related applications. Large variations and inconsistent packet spacing can severely impact call quality. VoIP implementations often use a buffer to queue voice packets (to keep the packet timing as consistent as possible).

Noise

Voice signal interference (noise) can impact VoIP calls, but the noise is not usually related to line quality. In VoIP, noise is usually a side-effect of codec processing and possibly interference from other network devices.

eHealth can help you to monitor all these factors for your VoIP services.

How eHealth Manages Voice Quality and MOS

eHealth provides an automatic and continuous method for testing VoIP call quality using the eHealth Voice Quality Monitor (VQM) module, a software application that you can distribute on Windows or Linux systems and laptops throughout your VoIP network. By placing the VQM modules close to the actual IP devices, your VQM modules show you the call quality experiences of your IP phone end users.

You can install the eHealth VQM module on laptops and locate them throughout the network as needed. You can configure new tests to obtain MOS values for a variety of potential network paths.

To use VQM, you must follow this process:

1. Install and license a minimum of two SystemEDGE agents and two eHealth VQM modules. You install an agent and module close to the sending IP phone and another agent and module close to the receiving IP phone. One VQM site serves as the transmitter/receiver, and one serves as the reflector for the MOS testing.

2. Configure the VQM testing by creating VQM paths at the transmitter using AdvantEDGE View. For each path, you can select the codec that you use and the reflector site.

VQM then creates and runs tests that send synthetic voice traffic between the transmitting (outgoing) and receiving (incoming) ends of the call to estimate the MOS values for the call quality. That is, one VQM path monitors the two-way MOS values between the sites.
Example: Place VQM Systems in Several Areas

An example of how you can place VQM systems in several areas follows:

- VQM A is a system on a switch that supports both IP phones and workstations.
- VQM B is located on a system close to the IP phones on the opposite side of the WAN.
- VQM C is located near voice-enabled client desktops.

Configure VQM paths between VQM A and VQM B, and between VQM A and VQM C. If the phones at B and C communicate, configure tests from VQM B to VQM C to estimate the MOS values there as well.

Cisco IP SLA Routers

If you have Cisco routers that support the IP SLA feature of the Cisco IOS, you can use eHealth Response to create response paths to monitor jitter to and from those Cisco devices.

How eHealth Manages Cisco IP SLA Jitter Testing

If your Cisco routers support IP SLA, you can discover them to create response source elements. Then, using the Path Manager dialog in the eHealth console, you can create response path elements to test jitter from the Cisco routers to other destinations. You can monitor these paths to determine whether your network can support your voice traffic needs.

You can run reports on a jitter response path to monitor several factors such as incoming and outgoing jitter (as perceived by the source router). If problems occur, you can use these reports to determine whether the problem is somewhere between your routers or between the phones and the LAN switches.

Manage Network Resources

You can use eHealth to manage your core network resources to help you to determine whether your network is large enough to accommodate your current and future voice traffic, and how well your devices and interfaces are operating.
eHealth for Voice helps you do the following:

- Discover important trunks, lines, and interfaces to monitor their traffic volume and overall health.
- Discover your LAN switches to manage their support of the IP devices that they control.
- Discover your routers to monitor the traffic across your LANs and WANs. Look for volume increases and discards which impact voice quality problems.

Service Level Reports for VoIP

eHealth VoIP offers three Service Level reports that are designed to provide high-level views of voice service:

- VoIP Executive Report
- VoIP Service Customer Report
- VoIP IT Manager Report

The recommended way to obtain these reports is to request that your eHealth administrator schedule them to run daily, weekly, or monthly. You can also run them from the eHealth Web interface, which takes longer.

VoIP Executive Report

Designed for the CIO or business manager who needs to be aware of the state of voice services, the VoIP Executive report answers these questions:

- What voice quality are users experiencing?
- Is voice service available 100% of the time?
- How much VoIP traffic is the network supporting?
The VoIP Executive report typically contains the five charts described in the following list. The report omits charts if the selected group or group list does not support that information.

**Average MOS**

Shows the average mean opinion score (MOS) for each day, week, or month. The MOS is a measurement of voice quality, from 1 (worst) to 5 (best). If a bar in the chart shows a MOS value lower than 4 (or 3.5, depending on the codec), drill down to a Worst Performers report; in that report, click a path name to generate an At-a-Glance report for more details.

**Call Path Service Availability**

Shows how often the VoIP service was available to users. If a bar in the chart does not meet the goal, click the bar and drill down to a Worst Performers report for a list of call paths with the least availability. From that report, click a call path name to generate an At-a-Glance report for further details.

**Call Volume**

Indicates the total connection time in call minutes. It also plots a trend line for total connection time over the report period. Use this chart to monitor the volume of calls and to identify trends in usage. If a bar in the chart is unusually high or low, click the bar and drill down to the Group Distribution report to determine whether a particular group in the group list had an unusual call volume.

**Calls**

Displays the total number of completed and incomplete calls during the report period. Use it to monitor call volume over time. If a bar indicates an unusually high number of incomplete calls, click the bar and drill down to a Worst Performers report. In that report, click a path name to drill down to an At-a-Glance report for further details.

**Network vs. Voice Call Volume**

Shows total network traffic over Class of Service (CoS) WAN links, indicating which portion of the traffic was voice traffic. If a bar in the chart indicates an unusually high call volume, click the bar and drill down to a Group Distribution report to determine which group in the group list initiated the high amount of voice traffic.
VoIP Service Customer Report

This report offers a summary of the level of voice service that service providers deliver to their customers. These are the same charts that are included in the VoIP Executive report, however, they show this information as it relates to a particular service customer. Service providers and their customers can use this information to determine whether the level of voice service delivered meets service level agreements (SLAs).

The included charts are as follows:

**Average MOS**

Shows the average mean opinion score (MOS) for each day, week, or month. The MOS is a measurement of voice quality, from 1 (worst) to 5 (best). If a bar in the chart shows a MOS value lower than 4 (or 3.5, depending on the codec), drill down to a Worst Performers report; in that report, click a path name to generate an At-a-Glance report for more details.

**Call Path Service Availability**

Shows how often the VoIP service was available to users. If a bar in the chart does not meet the goal, click the bar and drill down to a Worst Performers report for a list of call paths with the least availability. From that report, click a call path name to generate an At-a-Glance report for further details.

**Call Volume**

Indicates the total connection time in call minutes. It also plots a trend line for total connection time over the report period. Use this chart to monitor the volume of calls and to identify trends in usage. If a bar in the chart is unusually high or low, click the bar and drill down to the Group Distribution report to determine whether a particular group in the group list had an unusual call volume.

**Network vs. Voice Call Volume**

Shows total network traffic over Class of Service (CoS) WAN links, indicating which portion of the traffic was voice traffic. If a bar in the chart indicates an unusually high call volume, click the bar and drill down to a Group Distribution report to determine which group in the group list initiated the high amount of voice traffic.
VoIP IT Manager Report

Designed for the IT manager who needs to monitor the level of voice service provided, troubleshoot problems, and perform capacity planning, this report provides more detailed information than the other VoIP Service Level reports. It answers these questions:

- Is voice service acceptable? If not, why?
- Are the voice service and other VoIP components available and working well? If not, which components are having trouble?
- How much VoIP traffic is the network supporting?
- When will we need to increase capacity?

At-a-Glance Reports for VoIP

At-a-Glance reports provide the IT staff with summary information about the following VoIP components:

- Voice quality response paths
- Voice gateways
- CoS elements and associated WAN links

Each At-a-Glance report presents several charts on a single page which lets you compare several variables to troubleshoot problems with voice service and VoIP components. When you identify a problem, you can drill down to a Trend report for a closer view of that information.

Trend and Top N Reports for VoIP

Trend reports and Top N reports are often useful when troubleshooting problems with voice service or VoIP components. For example, suppose that in the VoIP Executive report, the Average MOS chart indicates that voice quality was unusually low on a particular day. From that chart, you can drill down to a Worst Performers report (a variation of the Top N report) to identify the call paths with the lowest MOS ratings.

From the Worst Performers report, you can click a path name to generate an At-a-Glance report for summary information about that call path. From a chart in the At-a-Glance report, you can drill down to a Trend report for more details about a trouble spot to help identify the source of the problem. For example, suppose that the Degradations from Maximum Call Quality Out chart (in the At-a-Glance report) shows a spike in voice quality degradation. You can click that chart to run a Trend report for a closer view of the sources of the degradation.
Quality of Service (QoS) Reports

QoS technology lets you implement different levels of service for different types of network traffic (voice, video, and data). If your routers are QoS-enabled, you can run eHealth reports to monitor and manage QoS metrics for voice traffic. This capability is especially important to service providers who need to meet customer SLAs for voice service.

eHealth QoS reports can help you do the following:

- Monitor SLA metrics by class of service (CoS).
- Detect proactively when a metric is about to be violated, so that you can take corrective action.
- Determine whether a customer has exceeded agreed-on CoS metrics.
- Identify which CoS elements are causing problems.

The QoS Health report displays metrics for your CoS elements on network utilization, packet drops, and packet delays. It compares performance variables to QoS parameters and indicates when a QoS SLA has been violated. When the QoS Health report indicates trouble, you can drill down to At-a-Glance, Trend, and Top N reports to investigate problems that may be degrading the quality and performance of your voice traffic.

Reports for Voice Quality with Cisco SA

If your Cisco routers are bundled with the Cisco Service Assurance (SA) Agent, you can use the agent with eHealth to provide additional metrics on voice quality. (This can be in addition to or instead of using eHealth Voice Quality Monitor [VQM] to monitor voice quality between end points.) When you use the Cisco SA Agent, eHealth configures a Cisco router to generate traffic to specified network resources. It regularly measures the availability of the resource and response time between the router and the resource. The Cisco SA Agent can also measure other important metrics such as latency, jitter, and packet loss. You can use this information to monitor metrics that affect voice quality.

Run At-a-Glance and Trend reports about performance variables such as round-trip delay, jitter, and jitter variation to obtain an accurate view of the quality of voice service that a user experiences.
Additional Queries for VoIP Components

In addition to the Service Level, At-a-Glance, Trend, and Top N reports, you can run AdvantEDGE View queries for details on the performance of your VoIP components. For example, you can run queries to monitor the following:

- Health and availability of applications and servers
- Voice quality for response paths between two systems, using active testing
agent

In network management, an agent is a program that provides information from a management information base (MIB) for SNMP agents. eHealth or a network management system (NMS) uses the information about managed devices and takes corrective action when appropriate.

AIM

See eHealth application insight module (AIM).

alarm

An alarm in Live Exceptions is a notification of a problem or potential problem somewhere in the infrastructure. The state of an alarm is one of four severity levels: warning, minor, major, and critical. The severity is the maximum severity of any of the alarms currently active on an element within a specific profile.

American Standard Code for Information Interchange (ASCII)

American Standard Code for Information Interchange (ASCII) is the most common format for character representation in computers and the Internet. Characters fit into a single byte. It was developed by the American National Standards Institute (ANSI).

Apache

Apache is a freely distributed Web server that runs on most UNIX, Linux, and Windows operating systems. eHealth SystemEDGE can monitor the Apache Web server when it is used with the eHealth application insight module (AIM) for Apache.

application

An application is a program that performs a specific function for one or more users or for another application program. Types of applications include communication programs, management programs, word processors, database management systems, and drawing programs.

ASCII

See American Standard Code for Information Interchange (ASCII).

Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is a high-speed networking standard that divides data packets into small cells and secures a virtual channel to enable a direct transfer of data between sending and receiving systems. ATM is a networking solution for carrying real-time video and voice services.

ATM

See Asynchronous Transfer Mode (ATM).
availability

*Availability* is the percentage of time that an element is operational during the eHealth report period. eHealth calculates availability for devices, interfaces, system processors and process sets, and response paths. The availability calculation depends on the element type.

bandwidth

*Bandwidth* is the throughput of a communications line usually measured in megabits per second (Mbps). Also refers to the difference between the highest and lowest frequencies in a communications channel, expressed in units of hertz (Hz), or cycles per second.

bridge

A *bridge* is a device that connects one LAN to another LAN of the same type.

cable modem

A *cable modem* is a device that connects a cable television (TV) line and either a personal computer (PC) or a television. The device communicates with a cable modem termination system at the local cable TV company office to receive and send data at a rate of up to 1.5 megabits per second (Mbps).

capacity

*Capacity* is the measurement of the volume that an element can support. For interfaces, this is the bandwidth that can be carried. For hard disks, it is the disk size or the amount of information that can be stored on the disks. See also traffic.

cell

A *cell* is a fixed-size packet used in Asynchronous Transfer Mode (ATM). Cells contain control and addressing information as well as data. ATM cells are 53 bytes long. Fixed-length cells have a constant delay when transmitted, making it easier to prioritize traffic.

central processing unit (CPU)

A *central processing unit (CPU)* is the component within a device that performs the instruction execution for the applications and programs that run on the device. Also referred to as a processor or microprocessor.

channel

A *channel* is a communication path between two or more devices. In the eHealth Asynchronous Transfer Mode (ATM) implementation, an ATM channel element represents a virtual circuit within an ATM path element. ATM channels enable several devices to use one ATM path element, dividing the cost of the path over multiple users and increasing overall throughput.

Chief Information Officer (CIO)

A *Chief Information Officer (CIO)* is a top-level manager who is ultimately responsible for all information systems in an organization.
cluster
A cluster is a loosely coupled set of eHealth systems that share information. A cluster can contain several Distributed eHealth Systems and Distributed eHealth Consoles as needed to meet an organization’s needs.

congestion
Congestion is a condition in which the network traffic is greater than the amount that the network can carry. Often causes performance problems and delays on a network.

connect time
Connect time is the total time that a user is connected to a network. Commonly used for defining customer expectations in a service level agreement.

CPU
See central processing unit (CPU).

Database Management System (DBMS)
A Database Management System (DBMS) is a program such as Oracle, Microsoft SQL Server, or Sybase for creating and providing access to one or more databases.

DBMS
See Database Management System (DBMS).

delay
Delay is the time required for a packet or frame to travel from the source to the destination.

Destination
Destination is an element that terminates a response path. The eHealth administrator can create a destination element from a router or server, or from some other system.

DHCP
See Dynamic Host Configuration Protocol (DHCP).

dial-up connection
A dial-up connection is a link to a data communications network through a public switched telecommunication network.
Digital Subscriber Line (DSL)

*Digital Subscriber Line (DSL)* is a wide area network (WAN) technology that enables dedicated high-bandwidth connections over standard copper telephone lines. Several types of DSL are available, classified together as xDSL technologies. Fixed-Rate DSL service has fixed speeds for transmissions from the server toward the end user (downstream) and transmissions from the end user toward the server (upstream). Rate-Adaptive DSL (RADSL) can adjust line speeds for local conditions and line quality. Most consumer DSL technologies are Asymmetric DSL (ADSL), which provides greater downstream speeds (up to 6-8 Mbps) than upstream speeds.

DNS

See domain name system (DNS).

domain name system (DNS)

*A domain name system (DNS)* is the system that locates and translates Internet domain names (for example, yourcompany.com) into Internet Protocol (IP) addresses. A DNS server is typically a device that translates domain names to IP addresses within your network.

DSL

See Digital Subscriber Line (DSL).

Dynamic Host Configuration Protocol (DHCP)

*Dynamic Host Configuration Protocol (DHCP)* is a protocol that enables dynamic allocation of IP addresses so that they can be reused.

eHealth administrator

An *eHealth administrator* is a person responsible for managing and administering the eHealth system from the eHealth console.

eHealth AIM

See eHealth application insight module (AIM).

eHealth application insight module (AIM)

An *eHealth application insight module (AIM)* is a plug-in (supplementary program) that extends the functionality of the eHealth SystemEDGE agent. AIMs add the capability to monitor and manage application-specific events and processes. AIMs were formerly called AdvantEDGE Point modules.

eHealth console

The *eHealth console* is the administration and configuration console that lets an administrator start and stop eHealth, manage the poller and the database, and administer the eHealth system. The eHealth console is not the same as the eHealth Web interface.
**eHealth Web administrator**

The *eHealth Web administrator* is a person responsible for managing and administering the eHealth Web server and eHealth Web interface.

**eHealth Web interface**

The *eHealth Web interface* is the eHealth interface that lets a user access eHealth reports and applications from a Web browser. See also *eHealth console*.

**element**

An *element* is a device or resource (such as a router, server, interface, modem, modem pool, or application) for which eHealth collects and analyzes data to generate reports.

**Exchange**

*Exchange* is the Microsoft Corporation groupware application that enables communication and collaborative work. At its core is an electronic mail routing, distribution, and storage facility.

**File Transfer Protocol (FTP)**

*File Transfer Protocol (FTP)* is a means for uploading and downloading files on the Internet (the oldest Internet protocol for retrieving files). You can use an FTP client application to request files from or transfer files to an FTP server.

**filter**

A *filter* is a set of selection criteria used to focus a report on the desired data.

**firewall**

A *firewall* is a server whose main purpose is to act as a gateway between a local area network (LAN) and a large network that is not secure (such as the Internet). A firewall server typically runs a software package that inspects inbound and outbound packets, and decides whether to allow the packets to pass.

**FireWall-1**

*FireWall-1* is a firewall software package developed by Check Point Software Technologies, Ltd. See also *firewall*.

**Frame Relay**

*Frame Relay* is a packet-switching standard for wide area networks (WANs) that support data rates at T1 (1.54 Mbps) and T3 (45 Mbps). Frame Relay connections are available from 56 Kilobits per second (Kbps) up to 1.54 Mbps.

**FTP**

See *File Transfer Protocol (FTP)*.
goal

Goal is an eHealth setting that specifies a preferred level of service. Top N reports can display the elements that exceed or fall below specified goals.

HTTP

See Hypertext Transfer Protocol (HTTP).

HTTPS

See Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).

Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) is an application protocol that defines the set of rules for exchanging files (text, graphics, multimedia, and other files) on the World Wide Web (WWW).

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is the use of Netscape’s Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.)

I/O

See input/output (I/O).

IIS

IIS is the Web server that is part of the Microsoft Windows Server application. IIS consists of several services, including World Wide Web (WWW), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Network News Transfer Protocol (NNTP). In versions of IIS prior to 5.0, IIS is an abbreviation for Internet Information Server. In version 5.0 and later, IIS is an abbreviation for Internet Information Services.

Information Technology (IT)

Information Technology (IT) is a widely used term to describe all of the technologies used for creating, exchanging, managing, and using information in various forms.

input/output (I/O)

Input/output (I/O) is any operation, program, or device that transfers data to or from a computer.

Integrated Services Digital Network (ISDN)

Integrated Services Digital Network (ISDN) is a high-speed carrier service offered by telecommunications companies.
Internet Information Server
See IIS.

Internet Information Services
See IIS.

Internet Protocol (IP)

Internet Protocol (IP) is the method (or protocol) by which packets of information are sent across the Internet. IP defines addressing, error handling, routing, and option codes for data transmission. IP requires no continuing connection between the endpoints that are communicating.

Internet Service Provider (ISP)
An Internet Service Provider (ISP) is a company that provides individuals and companies with access to the Internet. ISPs also provide related services such as Web site building and virtual hosting.

IP
See Internet Protocol (IP).

ISDN
See Integrated Services Digital Network (ISDN).

ISP
See Internet Service Provider (ISP).

IT
See Information Technology (IT).

IT infrastructure
An IT infrastructure consists of the applications, systems, and networks that an organization uses to manage its operations, for both internal use and for interfaces to the outside world.

jitter
Jitter is the variation in delay between two successive packets in a simulated real-time voice or video data flow.

LAN
See local area network (LAN).
latency

Latency is a measure of network delay. Depending on the type of element, eHealth reports can show two types of latency: eHealth latency, which is the length of time in milliseconds for a ping packet to travel from the eHealth system to a polled element and back; and alternate latency, which is the length of time in milliseconds for a ping packet to travel from a network resource (such as a router) to other critical network resources (such as routers and servers).

LDAP


Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) is a software protocol for locating organizations, individuals, and other resources, such as files and devices in a network. LDAP is based on a client/server model. The LDAP client makes a Transmission Control Protocol (TCP) connection to an LDAP server, and then sends requests and receives responses over this connection. For more information about LDAP, see RFC 2251.

line print (LP)

Line print (LP) is a common tool used to print documents over a UNIX network.

local area network (LAN)

A local area network (LAN) is a shared communication medium that connects computers and devices over a limited area. The area limitations of a LAN usually result from the electrical signal limits of the medium.

LP

See line print (LP).

MB

MB is the abbreviation for Megabytes.

mobile wireless

Mobile wireless is a technology that uses cellular communications to connect hand-held telephones, laptop computers, and personal devices, and that supports various services such as the Internet. Two common cellular airwave communications are general system for mobile communication (GSM), used mostly in Europe, and code-division multiple access (CDMA), used mostly in Asia and North America.

modem

A modem is a device that transmits and receives data through a medium such as a telephone line or cable. The term modem is a combination of modulator-demodulator.
network cloud

A network cloud is a generic representation of a complex interconnection of routing devices that form a network. Networks are often represented pictorially as a cloud.

network file system (NFS)

A network file system (NFS) is a program that lets users access file systems over the network.

network information service (NIS)

Network information service (NIS) is a protocol for administering network-wide databases. It includes programs for finding an NIS server and accessing the NIS database. Also referred to as network information name service.

network management system (NMS)

A network management system (NMS) is an application program usually residing on a computer that manages at least part of a network, including systems and applications. The NMS communicates with agents to monitor network statistics and resources, controls network device configuration, and analyzes network problems. See also agent.

Network News Transfer Protocol (NNTP)

Network News Transfer Protocol (NNTP) is the predominant protocol used by computers for managing messages posted on Usenet newsgroups.

NFS

See network file system (NFS).

NIS

See network information service (NIS).

NMS

See network management system (NMS).

NNTP

See Network News Transfer Protocol (NNTP).

normal

Normal is the range of values that are to be expected for a polled variable. eHealth computes normal values using a baseline time period (typically six weeks) for each hour of each day of the week. The normal values are calculated in one of three ways: absolute from mean, percentage from mean, or deviation from mean.

normalization

Normalization is the process by which a function is applied to a value to place the resulting value within a specific range or to convert values to a common unit. When appropriate, eHealth normalizes data to ensure consistent content and to allow for meaningful performance comparisons.
optical networking

*Optical networking* is a technology that uses fiber optics to transmit voice and data. Optical networking is also known by the names of two fiber optic standards: SONET and SDH. Optical networking consists of four physical layers, three of which can be monitored using eHealth: the section layer, the line layer, and the path layer.

packet

A *packet* is a logical unit of data routed between a source and a destination on the Internet or any other packet-switched network. On the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides a file into packets of manageable size for routing.

path

In networking, a *path* is a route from one location to another in a network. In an Asynchronous Transfer Mode (ATM) network, a path is a virtual pipe that can carry a number of channels. In eHealth Application Response, a path is the link between a response source and a response destination.

PC

See *personal computer (PC)*.

PDF

See *Portable Document Format (PDF)*.

personal computer

A *personal computer (PC)* is a computer designed for individual use. Prior to the PC, computers were designed to be used by many individuals and system resources were shared by all. A PC often refers to a computer with an Intel style microprocessor architecture and an operating system such as Microsoft DOS or Windows.

ping

A *ping* is an Internet echo message used to confirm the reachability of a network device. An abbreviation for Packet Internet or Inter-Network Groper.

POP3

See *Post Office Protocol 3 (POP3)*.

port

A *port* is the physical (hardware) connection on a device that connects the device to a network.

Portable Document Format (PDF)

A *Portable Document Format (PDF)* is a file format that captures all elements of a printed document as an electronic image that you can view, navigate, print, or forward to someone else. PDF files are created using Adobe Acrobat, Acrobat Capture, or similar products.
**Post Office Protocol 3 (POP3)**

Post Office Protocol 3 (POP3) is a standard client/server protocol for receiving e-mail, in which an Internet server receives the mail and a client periodically downloads it to a user's system.

**protocol**

A protocol is the set of rules by which the endpoints in a telecommunication connection communicate. The protocol defines the packet format of the transmitted information. On the Internet, common protocols are TCP, IP, HTTP, and FTP.

**RAS**

See remote access server (RAS).

**reachability**

Reachability is the ability of eHealth to contact an element over the network. eHealth uses ping to determine reachability. See also ping.

**real-time**

Real-time is a level of computer responsiveness that an end user would deem as immediate or fast enough to show incremental changes of an external process (for example, to present visualizations of the weather as it constantly changes).

**remote access server (RAS)**

A remote access server (RAS) is a device that provides remote users with dial-up access to a network. RAS devices usually contain modem or Integrated Services Digital Network (ISDN) cards that provide the connection services.

**remote network monitoring (RMON)**

Remote network monitoring (RMON) is a type of device that collects nine kinds of network management information, including packets sent, bytes sent, packets dropped, statistics by host, statistics by conversations between two sets of addresses, and certain kinds of events that have occurred. A probe is an example of an RMON device. RMON2 devices collect management information according to the latest version of the management information base (MIB) specification, RMON, version 2. For more information, see RFC 2021.

**report period**

A report period is the time range specified by the user to be included in an eHealth report. The time options vary with each report type, but the report period could consist of hours, days, weeks, or months.

**response endpoint**

A response endpoint is a router, server, or other system that is part of a response path. A response endpoint is either a response source or a response destination.
response path

A *response path* is the connection between a response source and a response destination over which transactions travel. See also response endpoint.

RMON

See remote network monitoring (RMON).

RMON2

See remote network monitoring (RMON).

router

A *router* is a device that connects networks. Routers learn the addresses of the network points that send data by reading the address information in the data frames. Hardware vendors often use the terms router and switch interchangeably. See also switch.

SAN

See storage area network (SAN).

sendmail

*Sendmail* is the mail transport agent (MTA) daemon that implements the Simple Mail Transfer Protocol (SMTP) mail protocol on UNIX systems.

service level agreement (SLA)

A *service level agreement (SLA)* is a contract between a provider and a user that details the service commitments to a user. An SLA typically includes the following: specific descriptions of services being delivered (including the criteria used to evaluate the service), reporting requirements, escalation agreements (how to address serious interruptions), and penalties for failing to meet the contract terms.

Simple Mail Transfer Protocol (SMTP)

*Simple Mail Transfer Protocol (SMTP)* is the Transfer Control Protocol/Internet Protocol (TCP/IP) protocol used for sending and receiving e-mail in data networks. See also sendmail.

Simple Network Management Protocol (SNMP)

*Simple Network Management Protocol (SNMP)* is the network management protocol used almost exclusively in data networks. A method for monitoring and controlling network devices, as well as managing configurations, statistics collection, performance, and security.

SLA

See service level agreement (SLA).

SMTP

See Simple Mail Transfer Protocol (SMTP).
SNMP


storage area network (SAN)

*Storage area network (SAN)* is a technology for exchanging data between servers and storage devices such as disks, tapes, and RAID arrays. They allow for device sharing across multiple clients and servers. SAN communication devices often use fiber channel LAN technology.

switch

*A switch* is a network device that determines the path for sending a frame across a network. It can also specify the adjacent network point where the frame will be sent. In general, a switch is considered a simpler and faster device than a router. However, hardware vendors often use these terms interchangeably. See also router.

T1

*T1* is a standard data transmission method with a rate equivalent to 1.54 Megabits per second (Mbps).

TCP

See Transmission Control Protocol (TCP).

TCP/IP

See Transmission Control Protocol (TCP) and Internet Protocol (IP).

throughput

*Throughput* is the rate of data transfer on an interface over time. At each poll, eHealth calculates throughput by dividing the total number of bits for an interface by the elapsed time in seconds since the previous poll.

traffic

*Traffic* refers to the data that travels over a network. Nodes create network traffic when they send data to one or more recipient nodes.

Transmission Control Protocol (TCP)

*Transmission Control Protocol (TCP)* is a connection-based protocol used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP is responsible for the actual delivery of the data, TCP is responsible for dividing data into packets at the sending system and constructing the data message from individual packets at the receiving system.

trap

*A trap* is a message sent by an SNMP agent to a console or network management system (NMS) to indicate that a threshold has been reached or another user-defined condition has occurred. The SystemEDGE agent defines a number of traps for system and application management.
trend line

A trend line is a projection of the future performance of an element based on data from past performance. eHealth constructs the trend line as the best straight line through the data points of the baseline period.

URL

A URL stands for uniform resource locator. It is the specific address for a Web site or file on the Internet.

variable

Variable represents a performance metric for an element. A characteristic or behavior upon which eHealth gathers data and evaluates the performance of the element. SystemEDGE can also monitor local variables to reduce network polls and increase scalability.

Voice over IP (VoIP)

Voice over IP (VoIP) is a set of facilities for managing the delivery of voice information using the Internet Protocol (IP). In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public-switched telephone network.

VoIP

See Voice over IP (VoIP).

WAN

See wide area network (WAN).

Web

See World Wide Web (WWW, Web).

wide area network (WAN)

A wide area network (WAN) is a network that interconnects multiple systems or networks over unlimited distances.

wireless LAN

A wireless LAN is a shared communication medium in which computers and devices communicate over short distances using airwaves.

workstation

A workstation is a powerful computer that is equipped with a fast processor, a large amount of random access memory, and other features such as high-speed graphical rendering that make it suitable for business users such as engineers, graphic designers, and architects.

World Wide Web (WWW, Web)

The World Wide Web (WWW, Web) is all of the resources on the Internet that use Hypertext Transfer Protocol (HTTP). Users of the Web access information through browser software.
Index

A
administration
  AdvantEDGE View • 91
  roles • 89
  tasks • 68
advanced logging • 43
AdvantEDGE View • 12
  administrative tasks • 91
  user tasks • 92
Agent Transaction Viewer • 25
agents
  Application Response • 25
  Cisco IP SLA • 26
  deploying • 12
  Juniper RPM • 26
  SNMP • 72
  SystemEDGE • 21
alarms • 64
  consolidation of • 61
  exporting with integration modules • 14
  Live Exceptions • 61
  SystemEDGE agents • 21
application insight modules (AIMs) • 21
application management • 10, 11, 25
application performance management • 11, 25
Application Response • 25
  agents • 25
  data collection • 19
as-polled data • 27
asset tracking • 21
At-a-Glance reports • 26
automatic notification • 21
auto-registration of elements • 19
B
baseline period • 27
Business Service Console • 58
C
capacity planning
  future capacity • 41
  overutilized resources • 38
  underutilized resources • 35
case study for fault and performance management • 72
Check Point FireWall-1 • 21
Cisco
  IP SLA • 26, 102
  NetFlow • 14, 16
  SA Agent • 26, 107
  VPN Solutions Center • 14
  WAN Manager • 14
Citrix • 25
clusters • 13
Cognos Report Center • 78, 79
command interface • 83
console • 83
consolidating alarms • 61
D
data
  analysis • 27, 48
  collection • 19, 20, 33
  historical • 45
  remote polling • 15
  storage • 27
database
  managing • 35
  roll-up • 27
Deviation From Normal • 61
discover process • 19
Distributed eHealth • 13
drill-down reports • 48
E
elements
  creating • 32
  grouping • 27, 34
  monitoring • 19
end-to-end infrastructure management • 11
exporting alarms • 14
F
fault management • 57
File Transfer Protocol • 21
G
group lists • 27, 86
voice quality • 99
MetaFrame • 25
Micromuse • 14, 21
MOS • 99
My Health reports • 49

N
NavisCore • 14
NavisXtend • 14
Netcool • 14, 21
NetFlow • 16
network
management systems • 21
network management • 9
resources • 26
services • 21
Nortel • 14
notifier • 62

O
OneClick for eHealth (OneClickEH) • 85
online help access • 89
overutilized resources • 38

P
packet loss • 26
passwords • 89
performance management • 57
permissions for Live Exceptions • 63
physical
elements • 19
poller configuration maintenance • 33
profiles for Live Health • 69

Q
QoS-enabled routers • 99

R
real-time data • 58
remote network monitoring • 16
remote polling • 15
reports • 45
Cisco IP SLA • 26
Cognos Report Center • 78, 79
customizing • 49, 81
drill-down • 48
generating • 27
Health • 48
historical analysis • 47
historical data • 45
Juniper RPM • 26
management • 34
MyHealth • 49
Quick Start • 77
scheduling • 48
Service Level • 48, 103
standard • 46, 77
Top N • 46
Trend • 46
viewing • 86
VoIP • 103
resources
discovery • 31
overutilized • 38
underutilized • 35
response time • 25
roll-up process • 27
rules for Live Health • 69
S
scheduling reports • 48
security • 15, 71
Service Availability • 21
service level agreements (SLAs) • 61
Service Level reports • 48
service packs • 44
service profiles • 27
SLAs (service level agreements) • 61
SNMP (Simple Network Management Protocol)
agents • 20
discovering • 19
polling • 19
SystemEDGE • 21
traps • 19
standard reports • 46
system management • 10, 34
SystemEDGE agents
AdvantEDGE View • 12
application insight modules • 21
benefits • 21
Service Availability • 21
T
technology keys • 16
telephones
analog and PBXs • 97
IP • 98
terminal server applications • 25
Terminal Services • 25
Time-Over-Threshold • 61
Top N reports • 46
Top Processes • 21
Traffic Accountant • 16
Netflow collectors • 76
reports • 76
Traffic Accountant • 76
transactions • 25
traps • 19
trends
thresholds • 27
Trend reports • 26, 46
U
underutilized resources • 35
upgrading • 43
user
interfaces • 83
names • 86
V
voice gateways • 97
voice quality and MOS • 101
VoIP reports • 103
W
Web interface
accessing • 89
overview • 85