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

This Product may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Product 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 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 Software are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the Software is limited to the period during which the 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 Product 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 PRODUCT "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 PRODUCT, 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 this Product and any product referenced in the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Product is CA.

This Product is 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 252.227-7013(c)(1)(ii), as applicable, or their successors.

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

Copyright © 2006 CA. All rights reserved.
Table of Contents

Preface

Audience ................................................................. 7
About This Guide ....................................................... 8
Reading Path ............................................................ 8
Revision Information .................................................... 8
Documentation Conventions ......................................... 9
Technical Support ....................................................... 10

Chapter 1  About eHealth  11

eHealth: Your Network Management Solution ................. 11
eHealth: Your Systems and Application Management Solution . 13
eHealth: Your Application Performance Management Solution . 14
eHealth: Your End-to-End Infrastructure Management Solution 16
Where to Go from Here ............................................... 18

Chapter 2  Essential Concepts  19

Components of Your IT Infrastructure ............................. 19
  Networks ............................................................... 20
  Servers and Clients ................................................. 21
  Applications .......................................................... 22
  Local Area Networks ............................................... 23
  Wide Area Networks ............................................... 24
  Network Technologies ............................................. 25
## Table of Contents

- **Modems** .................................................. 25
- **ISDN** ..................................................... 26
- **Remote Access Servers** ................................. 26
- **Modem Pools** .............................................. 27
- **ATM** ........................................................ 28
- **Frame Relay** ............................................... 29
- **Quality of Service (QoS)** ............................... 30
- **Voice over IP (VoIP)** ................................. 31
- **Wireless** .................................................. 32
- **SNMP** ....................................................... 33
- **SNMP Agents** ............................................. 33
- **Using MTFs to Normalize Data** ....................... 33
- **Where to Go from Here** ............................... 34

### Chapter 3  
**How eHealth Works**  

- **Collecting Data** .......................................... 35
- **What Is an Element?** ...................................... 36
- **Specifying the Elements to Monitor** ................. 36
- **Monitoring Elements** ...................................... 37
- **Storing Data in the eHealth Database** ............... 38
- **Generating Reports** ...................................... 39
- **Reporting on Groups of Elements** .................... 40
- **Analyzing Data** ........................................... 41
- **About the Baseline Period** ............................. 43
- **Where to Go from Here** ............................... 44

### Chapter 4  
**Using Agents to Collect Data**  

- **SNMP Agents** ............................................. 45
- **Unicenter NSM Agents** ................................... 46
- **SystemEDGE Agents** ...................................... 47
- **Application Insight Modules (AIMs)** .................. 49
- **Service Availability** ...................................... 52
- **Application Response Agents** ......................... 53
- **Cisco IOS IP SLAs** ....................................... 55
- **Juniper Real-Time Performance Monitoring (RPM)** . 56
- **Where to Go from Here** ............................... 58
Chapter 5  Reporting with eHealth  59

About Historical Data  ....................................................... 60
Standard Reports .......................................................... 60
  Trend Reports ............................................................. 61
  At-a-Glance Reports .................................................... 61
  Top N Reports ............................................................ 63
  What-If Reports .......................................................... 63
Historical Analysis Reports ............................................. 64
  Health Reports ............................................................ 64
  Service Level Reports ................................................... 64
  Running Health and Service Level Reports ..................... 65
Drill-Down Reports ......................................................... 65
MyHealth Reports .......................................................... 66
Where to Go from Here ................................................... 68

Chapter 6  Fault and Performance Management  69

Concepts ................................................................. 69
  Fault Management ...................................................... 69
  Performance Management ........................................... 70
  Real-Time Data ........................................................ 70
Business Service Console ............................................. 71
Live Health .............................................................. 71
  How Live Health Works .............................................. 72
  Live Status .............................................................. 74
  Live Exceptions ........................................................ 75
  Live Trend .............................................................. 78
Live Health — Fault Manager ........................................ 79
Distributed Live Health ............................................... 81
Where to Go from Here ................................................ 82
# Table of Contents

## Chapter 7
**More Features of eHealth** 83
- eHealth Technology Keys .................................................. 84
- AdvantEDGE View .............................................................. 85
- Traffic Accountant ............................................................... 87
- Integration Modules ............................................................. 88
- Distributed eHealth ............................................................. 89
- Remote Polling ................................................................. 91
- Where to Go from Here ....................................................... 92

## Chapter 8
**Using eHealth** 93
- User Interfaces to eHealth ................................................... 93
- Introduction to the eHealth Web Interface ............................. 94
  - Overview of the eHealth Web Interface ............................... 94
  - How to Access the eHealth Web Interface ......................... 95
  - Overview of Web Pages .................................................... 98
  - How to Use Online Help .................................................. 107
- Where to Go from Here ...................................................... 109

**Glossary** 111

**Index** 127
Preface

This guide provides an introduction to and overview of the eHealth® Suite — the comprehensive fault, availability, and performance management solution. It describes eHealth Release 5.7 and later.

Audience

This guide is intended for all potential users of the eHealth Suite, including the following groups of people:

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

This book does not assume any previous knowledge of or experience with eHealth. It does, however, assume a basic understanding of computer terminology and concepts.
About This Guide

This section describes the suggested reading path, revision information, and the documentation conventions used in this guide.

Reading Path

This guide is intended to be read sequentially from Chapter 1 through Chapter 8. Where appropriate, the guide refers you to the Web Help or other areas of the eHealth documentation set for additional information.

Revision Information

This is the fourth release of this guide. It includes the following changes:

- Added section on Unicenter NSM agents to Chapter 4.
- Added section on Juniper RPM to Chapter 4.
- Updated name of Cisco SAA to Cisco IP SLA.
- Updated the glossary with new terms.
# Documentation Conventions

Table 1 lists the conventions used in this document.

**Table 1. Documentation Conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File or Directory Name</td>
<td>Text that refers to file or directory names.</td>
</tr>
<tr>
<td><strong>code</strong></td>
<td>Text that refers to system, code, or operating system command line examples.</td>
</tr>
<tr>
<td><strong>emphasis</strong></td>
<td>Text that refers to guide titles or text that is emphasized.</td>
</tr>
<tr>
<td><strong>enter</strong></td>
<td>Text that you must type exactly as shown.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Text that refers to menus, fields in dialog boxes, or keyboard keys.</td>
</tr>
<tr>
<td><strong>New Term</strong></td>
<td>Text that refers to a new term, that is, one that is being introduced.</td>
</tr>
<tr>
<td><strong>Variable</strong></td>
<td>Text that refers to variable values that you substitute.</td>
</tr>
<tr>
<td><strong>→</strong></td>
<td>A sequence of menus or menu options. For example, <strong>File → Exit</strong> means “Choose Exit from the File menu.”</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td>Important information, tips, or other noteworthy details.</td>
</tr>
<tr>
<td><strong>CAUTION</strong></td>
<td>Information that helps you avoid data corruption or system failures.</td>
</tr>
<tr>
<td><strong>WARNING</strong></td>
<td>Information that helps you avoid personal physical danger.</td>
</tr>
</tbody>
</table>
Technical Support

If you have a Support Contract ID and password, you can access our Support Express knowledgebase at the following URL: http://search.support.concord.com.

If you have a software maintenance contract, you can obtain assistance with eHealth. For online technical assistance and a complete list of primary service hours and telephone numbers, contact Technical Support at http://support.concord.com.
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. The remaining chapters introduce important concepts and describe the components of eHealth.

**eHealth: Your Network Management Solution**

You are responsible for managing and maintaining a large, heterogeneous network. Keeping track of every router, switch, local area network (LAN), wide area network (WAN), and other network components can be challenging. Another challenge is monitoring the performance of the network: You need to know the percentage of time the network components are available; if the current network bandwidth is sufficient; if network traffic is increasing over time.
eHealth is the answer. It 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.
- Perform intelligent capacity planning.
- Manage and document service levels.

Figure 1 illustrates how eHealth collects a wide variety of data from your network infrastructure to generate alarms and reports.
Beyond 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 e-mail, Web servers, and database management systems) perform poorly, user productivity declines. You need to ensure that these systems and applications are always available and performing at their best.

*eHealth* provides integrated fault, performance, and availability management across complex, heterogeneous systems and applications environments. By automatically detecting, isolating, and correcting problems, this solution 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.

Figure 2 summarizes the systems and applications that you can monitor and manage using *eHealth*.
Your ultimate responsibility is making sure that applications are performing properly so that users and customers can do their work. When slow applications interfere with work, 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 allows you to measure and monitor actual end-user application response time for commercial or custom Windows or Web applications that are TCP/IP-based. It also enables you to understand application availability through a synthetic (test) approach from anywhere in the world. With this information, you can ensure that business-critical applications are available and performing well so that users can get their jobs done.

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.

TCP/IP is an acronym for Transmission Control Protocol/Internet Protocol.
- Enhance troubleshooting by drilling down from real-time alarms to historical application performance reports.
- Provide reports for capacity planning and service level documentation.

Figure 3 illustrates how eHealth monitors application performance across the entire IT infrastructure.
**eHealth: Your End-to-End Infrastructure Management Solution**

You are responsible for the health and well-being of the entire IT infrastructure for your organization, from applications to systems to networks. Individual tools to manage different parts of the infrastructure do not offer a single, comprehensive view, nor do they offer the integration you need to understand performance and availability across the organization.

*e*Health is the answer. It 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.

*e*Health 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

Figure 4 illustrates how *e*Health can provide a single, integrated view of the health of your entire IT infrastructure, including networks, systems, and applications.
Automatic impact assessment by customers, regions, and technologies

Identification of trouble spots from personalized business views

Network devices, systems, or response paths

Automatic impact assessment by customers, regions, and technologies

Figure 4. Single Integrated View of Faults and Performance
Where to Go from Here

After reading this chapter, you should have a general understanding of the solutions offered by the eHealth Suite. For an overview of important IT terms and concepts, refer to Chapter 2, “Essential Concepts.” For an overview of how eHealth works, refer to Chapter 3, “How eHealth Works.” The remaining chapters of this book provide more information about the components of eHealth.
This chapter provides an overview of important concepts relating to your infrastructure. You need to understand these concepts to use eHealth effectively.

If you are already familiar with concepts relating to networks and Information Technology (IT), you can skim or skip this chapter and read the next chapter. If you are not familiar with IT fundamentals, read this chapter for an introduction to common terms used throughout the eHealth suite of products.

This chapter covers the following topics:

- Components of your IT infrastructure
- Network technologies
- Simple Network Management Protocol (SNMP)

**Components of Your IT Infrastructure**

As computers and networks become an increasingly essential part of today’s world, it is important to have a clear understanding of the terminology surrounding them. Your **IT infrastructure** consists of the applications, systems, and networks that your organization uses to manage its operations, both for internal use and for interfaces to the outside world.
This section explains the following concepts related to your IT infrastructure:

- Networks
- Servers and clients
- Applications
- Local area networks (LANs)
- Wide area networks (WANs)

**Networks**

A **network** is a group of computers that are linked together to share resources and information, as illustrated in Figure 5. For example, when your computer is networked to other computers, you can do the following:

- Access and use information and applications that reside on other computers.
- Send electronic mail (e-mail) and files to users of other computers.
- Share the same printer, modem, and Internet connection.

The computers connected to a network are sometimes called **nodes** or **network nodes**. Networks can comprise two or three nodes or hundreds of nodes.

![Figure 5. A Simple Computer Network](image-url)
Servers and Clients

In the IT industry, the term server can have two meanings:

- A powerful computer that provides services for other computers connected to the network. For example, a file server usually has a large amount of disk space, and services requests from remote clients to read and write files on its disks.

- A program or a process (on a server computer) that provides a service to other (client) programs. In general, messages are passed between the client program and the server program over the network. For example, a mail server receives a client request for that user’s e-mail, and responds by sending a list of new e-mail messages.

The term client can also have two meanings:

- A personal computer (PC), desktop computer, or workstation that requests services from a server over a network.

- An application or a process (on a client computer) that requests services from an application server or a server process. For example, when you start the e-mail application on your workstation, that application is a client that connects to the e-mail server to retrieve your messages.

In eHealth documentation, server computers and client computers are generally referred to as systems.

In a client/server network, each client computer has access to data and services from one or more centralized servers. These servers can control applications, printing, communications, and administration. Figure 6 shows a client/server network.

Figure 6. A Client/Server Network
Applications

An application is a software program that you use to perform a particular task or type of work. For example, you use a word processing application to write letters and reports; you use an e-mail application to read and send e-mail messages.

In many client/server networks, application servers reside on large powerful computers while application clients reside on your workstation or PC. The application client displays the user interface and can perform some local processing, but the application server performs any major processing required.

One goal of many IT organizations is to maintain quick application response times for users. Response time is the time required to complete a transaction, from the moment you initiate an action until you perceive that the action is complete.

Application response time includes the following components:

- **Client time**: the amount of processing time required by the application client
- **Network time**: the amount of time required to send requests and responses over the network between the application client and server
- **Server time**: the amount of time required for the application server to service the client request

When response time for a particular application is slow, it is useful to break response time down into client time, network time, and server time to help locate the source of the delay, as illustrated in Figure 7.

![Figure 7. Measuring Application Response Time](image-url)
Local Area Networks

When the computers on a network are connected over a relatively small geographical area, it is a local area network (LAN). For example, when all of the computers in one building or location are linked together, it is a LAN.

A device that can be used to connect computers in a LAN is called a switch. A switch can also be used to connect two LANs. The switch passes information across the two LANs so that the two behave as essentially one large LAN. Another device that can link computers together in a LAN is called a hub.

Figure 8 illustrates a LAN that uses hubs to connect the nodes of each building into a small LAN and a switch to connect the LANs in the two buildings. As a result, a user in Building A can communicate with a user in Building B.

![Figure 8. A Local Area Network (LAN)]
Wide Area Networks

When a computer network is spread over a large geographical area, it is known as a **wide area network (WAN)**. A WAN connects large numbers of computers over long-distance communications links such as common carrier telephone lines. A WAN can also connect local area networks together.

Figure 9 illustrates one organization’s WAN that connects its LANs in Chicago, Los Angeles, and New York. Over the WAN, employees in Chicago can communicate and share information with employees in New York or Los Angeles.

![Figure 9. A Wide Area Network (WAN)](image)

A device that directs information from one computer (the source) to another (the destination) between networks is called a **router**. A router uses a networking protocol, such as the Internet Protocol (IP), to determine the best path from the source to the destination. Routers are designed to make intelligent decisions, for example, rerouting network traffic around a failed link to make sure that traffic continues to flow. Routers are typically used to connect LANs together to create WANs.
Network Technologies

Different types of networks often use a wide variety of technologies. This section describes some common technologies you should be familiar with when using eHealth:

- Modems
- Integrated Services Digital Network (ISDN)
- Remote Access Servers (RAS)
- Modem Pools
- Asynchronous Transfer Mode (ATM)
- Frame Relay
- Quality of Service (QoS)
- Voice over IP (VoIP)
- Wireless

Modems

A modem is a device that transmits and receives data through a medium such as a telephone line or cable. You use a modem, for example, to connect your home computer to the Internet.

Suppose you want to send a message across a WAN from your computer to another computer. A modem connected to your computer converts the computer’s digital signal into analog form so the message can be transmitted over standard telephone lines. At the destination, another modem converts the incoming message from analog to digital form before passing the message to the destination computer. Figure 10 shows a modem-to-modem connection through a WAN, which typically consists of a public switched telephone network.

Figure 10. A Simple Modem Connection through a WAN
ISDN

Integrated Services Digital Network (ISDN) is a technology that allows multiple types of communications, including data, voice, and packet services, to travel on a single line. As a completely digital service, ISDN eliminates the need for traditional modems, which perform analog-to-digital and digital-to-analog conversions. As a result, ISDN provides slightly faster connections and transmission speeds than traditional dial-up connections.

ISDN can be used to connect one LAN to another or to connect a LAN to the Internet. ISDN also serves as the basis for other WAN technologies and services, including Frame Relay and Asynchronous Transfer Mode (ATM), which are described in later sections of this chapter.

Remote Access Servers

Suppose you are traveling on business and you want to connect to your organization’s network from a remote location. You can use your laptop computer with its built-in modem to connect to the network over telephone lines. On the other end, your organization typically uses a remote access server (RAS) to manage dial-up connections to its network.

An RAS is a computer (with associated software) that has a set of modems or modem cards. When users dial into the network, the RAS services the connections. The RAS usually includes a router that forwards remote access requests to other parts of the corporate network. Figure 11 illustrates a RAS.
Modem Pools

A **modem pool** is a logical collection of modems and ISDN connections. Modem pools can include modems that reside on the same or different RAS devices. They can be used to reserve modems for a specific group of users.

For example, if an Internet Service Provider (ISP) has several corporate clients, the ISP may create a separate modem pool for each client. Figure 12 illustrates the concept of modem pools.
ATM

Asynchronous Transfer Mode (ATM) is a networking technology that transmits different types of information (such as voice, video, and data) in fixed-length packets called cells. ATM supports high-performance multimedia networking; you can use it in LANs and WANs and in public and private network infrastructures.

ATM is connection-oriented, which means that it establishes a connection across the network before transmitting any data. ATM uses the concept of a virtual channel (VC), which is an end-to-end connection with defined endpoints and routes but without dedicated bandwidth. The network allocates bandwidth on demand as users generate traffic.

In an ATM network, an ATM switch receives a cell and reads the cell header to identify its destination. The switch directs the cell to the next connection on its link. In this way, the cell travels across the network to its ultimate destination. Figure 13 illustrates an ATM network.

**Figure 13. An ATM Network**
Frame Relay

Frame Relay is a WAN protocol that connects LANs. This technology transmits frames across a network between two sites. (A frame is a specially formatted sequence of bits that includes data and control information.) This packet-switching protocol can take advantage of high-speed T1 and T3 lines.

Devices connected to a Frame Relay network can be either of the following:

- **Data terminal equipment** (DTE). These can include terminals, PCs, routers, and bridges. The customer owns the DTE devices that connect to the Frame Relay network.

- **Data circuit-terminating equipment** (DCE). These are internetworking devices (such as packet switches) that actually transmit data through the WAN. The service provider owns the DCE devices.

Figure 14 illustrates a Frame Relay network with DTE and DCE devices.

*Figure 14. A Frame Relay WAN*
To transfer data from one DTE device to another through the network, the Frame Relay devices create a logical connection called a Frame Relay virtual circuit. A virtual circuit provides a communications path from one DTE device to another, passing through any number of DCE devices in the Frame Relay network.

Two types of Frame Relay virtual circuits are available:

- **Switched virtual circuits (SVCs)** are temporary connections between DTE devices.
- **Permanent virtual circuits (PVCs)** are permanently established connections between DTE devices. You can use PVCs for frequent and consistent data transfers across the Frame Relay network.

Frame Relay devices can combine several virtual circuits into a single **physical circuit** for transmission across the network. This capability can reduce the equipment and network complexity required to connect multiple DTE devices.

**Quality of Service (QoS)**

Most networks typically carry different types of traffic: voice, video, and data. Traffic can include critical information upon which a business depends, as well as less critical information. In most cases, network devices such as routers and switches treat all types of traffic equally; that is, all traffic has the same priority and the same chance of being delivered successfully.

**Quality of Service (QoS)** is a technology that allows you to set different levels of service for different types of network traffic. If you have network devices that support QoS, you can configure your routers to recognize different types of traffic, and to treat it differently based on a **Class of Service (CoS)** that you define for each traffic type. You can typically differentiate network traffic based on such factors as its source, destination, port, protocol, packet size, or a value called the IP Type of Service bit contained in the packets.
For example, you might want your highest priority or real-time (voice and video) traffic to have the best service (highest bandwidth, lowest latency, and no discards when congestion problems occur). Your lowest priority traffic might receive the poorest service (less bandwidth, higher latency times, and the first traffic to be discarded when congestion problems occur).

With QoS, you can increase bandwidth for critical traffic, limit bandwidth for non-critical traffic, and provide consistent network response. You can use your network connections more efficiently, and you can establish service level agreements (SLAs) with customers of the network.

**Voice over IP (VoIP)**

In most networks, voice traffic travels over a public switched telephone network (PSTN), while workstation and application data travels over an IP-based WAN. However, some WANs are actually converged networks — they carry both traditional data such as e-mail, 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 ensure that users have clear calls. You need to know about problems with voice quality or outages immediately. You need to know if your network can support the amount of voice traffic you expect.

You also need to ensure that your network can still carry and process your non-voice data traffic. You might also want to ensure that your voice traffic can be routed back into the PSTN if network problems occur. The VoIP management picture is complex.
“Wireless” refers to devices that can transfer signals between them without being connected by wires. A two-way radio is an example of a wireless device; more current examples are mobile telephones, home networks connected via wireless LANs, and personal digital assistants (PDAs). These devices enable users to conduct business and communicate while on the go, eliminating the leash of copper wire.

Several protocols exist for wireless data transfer, including Global System for Mobile Communications (GSM), the main telephone protocol used in Europe; General Packet Radio Service (GPRS), which enables access to the Internet from wireless phones, PDAs, and computers; Enhanced Data GSM Environment (EDGE), a faster variant of GSM; and Wireless Application Protocol (WAP), a set of communications protocols that standardize the way wireless devices, both fixed and mobile, access the Web.

Application servers that support wireless capabilities are being deployed to deliver these new data services — it’s likely that you’ll be responsible to some degree for the performance of these elements.

As part of this evolution, as with VoIP, you are again bringing together your voice and data infrastructures and leveraging new mobile IP devices such as media gateways, content gateways, services gateways, and soft switches. These new devices are key to the reliable delivery of mobile data services — you have to be able to ascertain their availability and performance instantly. You’ll also need to ensure that you have the capability to anticipate and plan for capacity changes and to troubleshoot problems before your end users are affected.

Introduction to eHealth
The Simple Network Management Protocol (SNMP) is an Internet standard that allows you to monitor computers and other network devices and analyze how well they are performing. You can also use SNMP to find and resolve network problems and to plan for network growth.

SNMP Agents

On a network device (such as a router, client system, server system, or switch), a software module called an SNMP agent collects performance, configuration, and status information about that device. The agent stores the data as defined by a management information base (MIB). At any time, a network management system (NMS) can ask the SNMP agent for the current values of particular variables, such as the number of incoming packets and outgoing packets or the total number of errors.

When an important or significant event occurs on a network device, the SNMP agent can report the event to an NMS. This reporting is called sending a trap. Network managers specify the types of events that the agent should report to the NMS. For example, the network manager might want to send an SNMP trap when a process terminates or when an important system resource exceeds a threshold.

Using MTFs to Normalize Data

When collecting performance data from agents, eHealth uses a MIB translation file (MTF) to determine the data that it needs from the agent and how to handle that data. The MTF tells eHealth how to translate MIB variables or use them to calculate other values. In this way, eHealth can normalize (convert) the data so that you can compare the performance of devices from different companies or technologies in reports.
*CPU is an acronym for central processing unit.*

For example, one system vendor indicates how busy a CPU is by storing the *percent* of time that the CPU is busy, while another vendor stores this information as the number of CPU seconds used. To make these different numbers comparable for reporting and analysis, an *eHealth* MTF converts the *percent CPU busy* number into the number of CPU seconds used. When CPU busy time appears in an *eHealth* report, you can easily compare and analyze the performance data from these different sources because all of the data has been normalized.

Figure 15 illustrates how *eHealth* uses SNMP agents, MIBs, and MTFs to collect performance data for IT elements.

![SNMP Agent](image)

**SNMP-managed devices can include client and server systems, routers, switches, bridges, hubs, printers, and other devices.**

**Figure 15. Collecting Data from SNMP Agents**

### Where to Go from Here

After reading this chapter, you should have a basic understanding of the following network and IT fundamentals:

- Networks, servers, clients, applications, LANs, WANs, hubs, routers, and switches
- Network technologies: modems, ISDN, modem pools, remote access servers, ATM, Frame Relay, QoS, VoIP, and wireless
- SNMP, agents, traps, MIBs, and MTFs

Now read Chapter 3 to learn how *eHealth* works.
This chapter describes how eHealth works: how its various components work together to gather information about and report on the performance and availability of the elements of your IT infrastructure. It also describes some fundamental concepts and processes that are referred to in the remainder of this book and throughout the eHealth documentation. To successfully use eHealth, it is important to gain a clear understanding of these concepts.

**NOTE**

This chapter describes how eHealth collects and processes *historical* performance data. Chapter 6 describes *real-time* data collection.

### Collecting Data

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.
What Is an Element?

An element is any part of your IT infrastructure that eHealth is monitoring. 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. For example, eHealth can monitor the network link between Boston and Chicago. This logical element (the Boston-to-Chicago link) does not specify which network devices are used to form the link; instead, it involves the logical connection itself.

Specifying the Elements to Monitor

When setting up the software, the eHealth administrator begins by identifying the elements to monitor for performance and availability. The administrator can specify the elements to monitor in three ways:

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

- **Importing.** 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-registering.** The agents for some eHealth components register automatically with eHealth when they begin monitoring.

Figure 16 illustrates the different ways in which you can identify the elements to you wish monitor.
**Monitoring Elements**

After it knows which elements to monitor, eHealth collects performance data about those elements on a regular basis. eHealth can collect data in the following ways:

- **Polling.** In many cases, eHealth collects performance and availability data about an element from an SNMP agent. (For more information, refer to “SNMP Agents” on page 33.) 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. For example, every five minutes the poller might ask a router how much CPU capacity is in use, and the router’s SNMP agent responds by sending the current CPU utilization.

- **Importing.** In some cases, eHealth can import performance data from an NMS at regular intervals.

- **Pushing.** eHealth Application Response™ uses a special process to send (push) performance data to the eHealth database at regular intervals.
• **Sending traps.** You can configure SNMP agents to send traps to eHealth when certain events occur. Live Exceptions analyzes this data to generate alarms. (For more information about Live Exceptions, refer to Chapter 6, “Fault and Performance Management.”)

Figure 17 illustrates the different ways in which eHealth collects performance data about the elements in your IT infrastructure.

**Figure 17. Collecting Performance Data**

### Storing Data in the eHealth Database

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

Keeping large volumes of as-polled data indefinitely would eventually strain the storage capacity of the eHealth database. To reduce the amount of data it stores, 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 enables you to run detailed reports for today and the past two days.
As the as-polled data ages (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. Figure 18 illustrates the database rollup process.

![Database Rollup Process Diagram](image)

**Figure 18. The Database Rollup Process**

---

### Generating Reports

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.
Reporting on Groups of Elements

To make eHealth reports more meaningful and useful, the eHealth administrator can define groups of elements, and you can then run reports for selected groups. For example, your organization may decide to organize elements by geographic location (Boston, Chicago, Dallas), by department or organization (Sales, Finance, Marketing), by customer or client, and so on.

To further organize elements and groups, the eHealth administrator can create group lists, which are collections of groups. Figure 19 illustrates a simplified example of the use of groups and group lists. In the illustration, each circle represents a group, and each oval represents a group list. With elements organized in this way, you can run a report to show the performance of all routers (in all locations), or of all monitored elements in Boston, or of just routers located in Boston.

![Figure 19. Organizing Elements with Groups and Group Lists](image-url)
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.

**Analyzing Data**

eHealth enables you to run reports on demand or to 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 then 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. Trend thresholds are upper limits on 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 yesterday’s as-polled data. Figure 20 illustrates the process.

Figure 20. The Data Analysis Process
About the Baseline Period

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.

Figure 21 shows the Average Network Volume graph from a sample LAN/WAN Health report. The solid line in the graph indicates the historical volume for the baseline period. The bars show the volume for the specified hour of the day.

For example, an Average Network Volume graph for a group of LAN/WAN elements was generated for the previous Tuesday. The graph compares each hour’s volume to the average volume for the preceding five Tuesdays in the six-week baseline period. 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.

Figure 21. Graph Showing a Historical Baseline
Where to Go from Here

For more information about how eHealth collects, analyzes, and reports on historical performance data, refer to the Web Help or the eHealth Administration Guide. For additional information about reports, read Chapter 5, “Reporting with eHealth,” and refer to the Web Help or the eHealth Reports Guide.

Now that you have a basic understanding of some fundamental concepts and processes of eHealth, read Chapter 4 to learn about the agents that eHealth uses to collect data.
Using Agents to Collect Data

Reports and alarms on the health of your IT infrastructure require accurate data. To provide the information that you need for troubleshooting, analysis, and planning, eHealth uses several different agents to collect data about your infrastructure, including the following:

- 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)

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, refer to http://support.concord.com/devices.

Cisco® IOS IP SLA was previously named the Cisco Service Assurance™ agent (SAA).
Unicenter NSM Agents

Unicenter Network and Systems Management (NSM) agents monitor your critical business systems, allowing you to ensure consistent performance and enhance system management.

You can use the eHealth Suite of software to supplement the robust performance reporting available with Unicenter NSM. Together, eHealth and Unicenter 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’s Live Health solution, you can also generate alarms when system performance is outside the service thresholds that you define.

Figure 22. At a Glance Report for NSM Agent Data
For more information about SystemEDGE agents, refer to the eHealth SystemEDGE User Guide.

SystemEDGE Agents

The eHealth SystemEDGE agent is intelligent and self-managing. It enables you to 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; you can also use it as part of an integrated eHealth solution, as illustrated in Figure 23.

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 autonomously 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.

**Figure 23. Using SystemEDGE Agents with eHealth**

**Automatic Notification and Action.** The SystemEDGE agent can monitor exception conditions automatically, reducing or eliminating the need for constant polling by an NMS. 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 may indicate attempts to compromise system security or poor performance of the Web site) and send an SNMP trap to an NMS.

**Top Processes.** SystemEDGE offers a feature called Top Processes, which enables the agent to 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, ensuring 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 easily 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.** Because it is an SNMP agent, SystemEDGE can provide data to eHealth and network management systems such as HP OpenView or Micromuse® Netcool™, leveraging your return on investment. It is also extremely efficient, using less than 1% of the CPU and about 3 MB of memory. This small footprint means that you can install SystemEDGE agents on server and client computers without affecting performance.
You can deploy, license, and manage SystemEDGE agents with AdvantEDGE View™, a graphical user interface and element manager. For more information, refer to “AdvantEDGE View” on page 85.

**Benefits.** By automating system management with SystemEDGE, IT organizations can scale to managing hundreds or thousands of systems without increasing staff. SystemEDGE enables you to fix problems before they affect users, free up valuable IT human resources, maximize your return on investment, and minimize costs. Figure 24 shows a sample At-a-Glance report that uses information provided by the SystemEDGE agent on a Windows server.

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

**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.

eHealth AIMs allow you to do the following:

- Detect and correct performance problems with mission-critical applications in real-time.
- Ensure sufficient system resources for these applications.
- Track usage statistics for the applications.
- Monitor their effect on critical system resources.
- Determine application configuration information (for use in fine-tuning performance or to train new IT personnel).
At-a-Glance Report
SysEdge NT System Element BOTANYBAY-SH

CPU Utilization by Process Set

Available by Process Set

Server Availability

Physical Memory by Process Set (bytes)

Virtual Memory (bytes)

Page Faults (page faults/sec)

Pages In (pages/sec)

Disk I/O (reads&writes/sec)

Disk I/O Busy Utilization

Disk I/O Queue Length (reads&writes)

Disk Errors (errors/sec)

User Partition Space Used (bytes)

Total Network I/O (frames/sec)

Total Network Errors (errors/sec)

Server Latency (msec)

Figure 24. Sample At-a-Glance Report with Information Sent from SystemEDGE Agent

Introduction to eHealth
eHealth offers a variety of AIMs for SystemEDGE to manage specific applications. Table 2 lists the AIMs currently available.

Table 2. eHealth AIMs

<table>
<thead>
<tr>
<th>Type of Application</th>
<th>AIMs Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail</td>
<td>Microsoft® Exchange</td>
</tr>
<tr>
<td>Web servers</td>
<td>Apache</td>
</tr>
<tr>
<td></td>
<td>Microsoft® IIS</td>
</tr>
<tr>
<td>Databases</td>
<td>Oracle®</td>
</tr>
<tr>
<td></td>
<td>Microsoft® SQL Server™</td>
</tr>
<tr>
<td>Network services</td>
<td>Check Point™ FireWall-1®</td>
</tr>
<tr>
<td></td>
<td>Network Services for UNIX</td>
</tr>
<tr>
<td></td>
<td>Network Services for Windows</td>
</tr>
<tr>
<td>Voice</td>
<td>Voice Quality Monitor</td>
</tr>
<tr>
<td></td>
<td>Cisco® Call Manager™</td>
</tr>
<tr>
<td></td>
<td>Cisco Unity and Unity Bridge</td>
</tr>
</tbody>
</table>

eHealth AIMs can be used with SystemEDGE agents as a stand-alone solution or with eHealth as part of an end-to-end solution, as shown in Figure 25.

Figure 25. Using AIMs with SystemEDGE Agents and eHealth
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
- 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 enables you to 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.
Introduction to eHealth

Application Response Agents

Application Response (AR) is an eHealth application that measures actual, observed response time from the end user’s point-of-view. With 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.
- Proactively manage service levels and perform capacity planning.

To gather application response data, you install AR 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. AR can also track response times for individual transactions and groups of transactions.

The AR agents regularly send the application response time data, along with other aggregated data, to eHealth. (Refer to Figure 27.) eHealth then stores this data in the database and uses the data in reports. eHealth Live Health™ also uses the response data, generating 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 — Response, 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, which 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 described in Chapter 5, “Reporting with eHealth.” Live Health also compares the response data with profiles and generates real-time alarms.

Figure 28 shows a sample Cisco IOS IP SLA Trend report. Trend reports show a historical view of response performance. The sample report shows that, for the specified time period, average response time to ping devices from the router was fairly steady, except for a spike of response time between 2:20 P.M. and 2:50 P.M.; this situation may merit further investigation.
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 allows you to perform service level monitoring, troubleshooting, and resource planning.

You use eHealth—Response 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 described in Chapter 5, “Reporting with eHealth,” 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.

Figure 29 shows sample charts from an At-a-Glance report for a Juniper RPM response path. These charts show metrics for jitter that you can use to monitor and manage attributes of network traffic that affect the quality of voice service.

![Figure 29. Sample AAG Report for Juniper RPM](image)
Where to Go from Here

After reading this chapter, you should have a general understanding of the various agents and plug-in modules that eHealth uses to collect performance and other types of data about components of your IT infrastructure. Now read Chapter 5 to learn about reporting with eHealth.
Using the information stored in the eHealth database, you can run a variety of reports to look at the health of your IT infrastructure from many different perspectives. Depending on the components of eHealth that you purchase, these reports can provide information on the health of applications, systems, and networks.

This chapter describes the nature of eHealth’s historical data and the types of reports that eHealth offers:

- Standard reports
- Historical analysis reports
- Drill-down reports
- MyHealth reports

For information about the real-time fault and performance management capabilities of eHealth, refer to Chapter 6, “Fault and Performance Management.”
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 old to more than one year old.

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, as described in Chapter 8, “Using eHealth.”

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

Because of 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 enables you to 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. Figure 30 shows a sample At-a-Glance report.
Figure 30. Sample At-a-Glance Report
**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 allows you to identify which elements are the source of a performance problem.

**What-If Reports**

What-If reports allow you to change various assumptions to determine how they affect performance. For example, the What-If Capacity Trend report allows you to 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 NMSs when problems are detected.

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.

Four separate Service Level reports are designed to meet the needs of different audiences. The 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.
Running 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, you can take advantage of an eHealth performance feature. For each scheduled Health or Service Level report, eHealth runs a scheduled Data Analysis job that analyzes the data for each element in the report based on the thresholds in the service profile used for that report. eHealth 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 will run faster because eHealth does not need to perform the data analysis for the elements that have existing analyzed summaries for those days.

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. Figure 31 shows an example of drilling down to another report.

---

For more information about data analysis, refer to “Analyzing Data” on page 41, the Web Help, or the eHealth Administration Guide.
When you drill down from one report to another, you do not need to specify report criteria; 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 if critical resources for which you are responsible need attention.

You can view your MyHealth reports from the MyHealth page of the eHealth Web interface, described in Chapter 8, “Using eHealth.” 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. Figure 32 shows a sample MyHealth report.
### MyHealth Report

Lan/Wan Group Mix_Lan_Groups for Yesterday

- **Alignment Errors** 
- **Average Frame Size** 
- **Average Frame Size In** 
- **Average Frame Size Out** (Divide by time)

Alignment Errors /sec
- 0
- 5K
- 10K
- 15K
- 20K
- 25K

Average Frame Size (bytes)
- 0
- 12:00 AM
- 2:00 AM
- 4:00 AM
- 6:00 AM
- 8:00 AM
- 10:00 AM
- 12:00 PM
- 2:00 PM
- 4:00 PM
- 6:00 PM
- 8:00 PM
- 10:00 PM
- 12:00 AM

### Group: ABF_ServerGroup - Top 10 for Previous 7 days

<table>
<thead>
<tr>
<th>Element Name</th>
<th>availability</th>
<th>Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUGUSTA-SH-enet-port-2</td>
<td>100.00</td>
<td>20.00</td>
</tr>
<tr>
<td>BARNEY-SH-enet-port-16777219</td>
<td>100.00</td>
<td>20.00</td>
</tr>
<tr>
<td>FMALI-PC-SH-enet-port-2</td>
<td>100.00</td>
<td>20.00</td>
</tr>
<tr>
<td>speedy-SH-enet-port-2</td>
<td>100.00</td>
<td>20.00</td>
</tr>
</tbody>
</table>

### Lan/Wan Group Mix_Lan_Groups - Bandwidth Utilization - Yesterday

Bandwidth Utilization %
- 0
- 1 - 10
- 11 - 20
- 21 - 30
- 31 - 40
- 41 - 50
- 51 - 60
- 61 - 70
- 71 - 80
- 81 - 90
- 91 - 100
- > 100

### Lan/Wan Group N_Lan_Group for Yesterday

Bandwidth Utilization %
- 0
- 0.5
- 1
- 1.5
- 2
- 2.5

Figure 32. Sample MyHealth Report
Where to Go from Here

After reading this chapter, you should have a general understanding of the reporting capabilities of eHealth. For more information about reports, refer to the Web Help or the eHealth Reports Guide. Now read Chapter 6 to learn about the fault and performance management capabilities of eHealth.
For eHealth, real-time monitoring means that active displays (not static reports) are updated as often as every 30 seconds to show the latest data.

While eHealth reports are useful for troubleshooting, trend analysis, and capacity planning, they do not allow you to anticipate and identify faults and slowdowns that are affecting users now. To address this need, eHealth also provides real-time fault and performance management capabilities for rapid problem diagnosis. This chapter describes the integrated fault and performance management capabilities offered by eHealth.

Concepts

This section describes the following concepts:

- Fault management
- Performance management
- Real-time data

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. Because faults can cause downtime and network degradation, fault management is a high priority for IT organizations. For example, suppose 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, suppose that user response time for a particular application is 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 may 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’s 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. AdvantEDGE View uses this data. For more information, refer to “AdvantEDGE View” on page 85.
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 Business Service Console 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 desktop. The ticker provides a subset of the overall hierarchy represented within the console and easily expands to show the full console. If a critical availability or performance problem occurs that may impact your business, you can quickly determine if someone is addressing it. An acknowledgement 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 Business Service Console provides additional details through pop-ups and navigation buttons, allowing you to 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.

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), allowing them to quickly identify and resolve performance problems.

**How Live Health Works**

Live Health consists of three applications:

- **Live Status®,** which provides a high-level view of the current status of monitored elements in your IT infrastructure
- **Live Exceptions,** which analyzes real-time performance data to detect problems and displays alarms in a browser
- **Live Trend,** a real-time charting tool for monitoring elements of your IT infrastructure

*For more information about Live Exceptions and its algorithms, refer to the Web Help.*

Figure 33 illustrates how Live Health works. eHealth collects performance data across the entire delivery system, including applications and underlying network and system components. Live Exceptions analyzes the data with powerful algorithms to identify outages and delays. These algorithms, including Time Over Threshold and Deviation From Normal, leverage the historical data contained in the eHealth database to identify true problems with greater precision. Live Health eliminates noisy, repetitive traps that provide little or no value.
1. eHealth collects performance data for monitored elements.

2. Live Exceptions analyzes data using algorithms such as Time Over Threshold and Deviation From Normal, watching for performance problems.

3. When Live Exceptions detects a fault or potential outage, it raises an alarm that appears in the Live Exceptions Browser, BSC, Live Status, or an NMS.

4. The operations team drills down from Live Status or the Live Exceptions Browser to real-time Live Trend reports, historical At-a-Glance or Trend reports, or AdvantEDGE View to identify, analyze, and correct the problem.

Figure 33. How Live Health Works

Introduction to eHealth
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.

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 provides a high-level view of the current status of monitored elements in your IT infrastructure. With Live Status, color-coded icons indicate element status, allowing you to quickly determine where the trouble spots are. When you identify a problem, you can quickly drill down for details to determine the source. Figure 34 is a sample Live Status display.

The 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 AdvantEDGE View. IT staff can glance at the display to identify problems and quickly drill down to element-specific information to troubleshoot them.
**Live Exceptions**

Live Exceptions is eHealth’s real-time engine that uses intelligent algorithms to detect brown-outs and service delays. Live Exceptions can detect application slowdowns as well as performance problems with network elements and systems.

**Profiles and Rules**

Live Exceptions provides out-of-the-box profiles (collections of rules) that you can associate with groups 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).
Consider this sample rule:

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

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.

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

Here is another sample rule:

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

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. Because performance is measured against a baseline that is unique to your environment, this is a far more powerful level of analysis than observing a flat threshold.

**The 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. Figure 35 shows a sample display of the Live Exceptions Browser.
In this case, *subjects* refer to groups and group lists.

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 allow you to 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 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.
Live Trend

Live Trend is a real-time charting tool for monitoring statistics elements polled by eHealth. You can chart multiple elements and variables, and eHealth updates each chart with every new poll. Figure 36 shows a sample Live Trend display.

![Sample Live Trend Display](image)

**Figure 36. Sample Live Trend Display**

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. Because 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 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 allows you to 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. Figure 37 illustrates how Live Health — Fault Manager receives traps.
Live Health — Fault Manager receives traps from other sources and sends them to Live Exceptions for processing and analysis of performance data to generate intelligent alarms.

Figure 37. Live Health — Fault Manager

Introduction to eHealth
Distributed Live Health

Distributed Live Health combines the power of real-time performance and availability management offered by Live Health with the scalability of Distributed eHealth. Distributed eHealt allows you to collect data and report on up to one million elements. Distributed Live Health, then, allows you to monitor and manage the alarms raised by Live Exceptions and Live Health — Fault Manager across the same one million elements.

A cluster is a loosely coupled set of eHealth systems that share information for distributed reporting.

From the Live Exceptions Browser running on a Distributed eHealth Console, you can monitor alarms from systems across the cluster. You can also drill down on an alarm to see historical reports automatically from the eHealth system that generated the alarm. This allows you to manage the performance and availability of systems around the world from a single point.

For more information about Distributed eHealth, refer to “Distributed eHealth” on page 89 and the Web Help; for more information about Distributed Live Health, refer to the Web Help.
Where to Go from Here

After reading this chapter, you should have a general understanding of the components of Live Health and how they can help you to monitor the performance of your IT infrastructure in real time.

Now read Chapter 7 to learn about more features of eHealth.
More Features of eHealth

Preceding chapters of this guide describe the agents that eHealth uses to collect data across your IT infrastructure and how eHealth uses that data for historical reporting and real-time fault and performance management. This chapter describes some additional components of eHealth, including the following:

- eHealth technology keys
- AdvantEDGE View
- Traffic Accountant
- Integration modules
- Distributed eHealth
- Remote polling
eHealth Technology Keys

Because 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.

Each technology key enables you to 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 it to Live Health for real-time analysis.

Depending upon the technology keys available, eHealth offers the following:

- eHealth — Network helps you to manage the performance and availability of critical network resources, including LAN/WAN, router/switch, Frame Relay, ATM, remote access, DSL, VoIP, and cable modem technologies. With appropriate licensing, you can also use eHealth — Network to monitor and report on QoS, Storage Area Network (SAN), optical networking, mobile wireless, and wireless LAN technologies.

For more information about eHealth — Network, refer to the Web Help or the Network Health Administration Guide.
For more information about eHealth — System and Application, refer to the Web Help or the eHealth — System and Application Administration Guide.

For more information about eHealth — Response, refer to the Web Help or the eHealth — Response Administration Guide.

- **eHealth — System and Application** enables you to analyze the performance of systems and applications equipped with SystemEDGE, eHealth application insight modules, and third-party SNMP system agents. It provides meaningful, compiled information and analysis about all of your business-critical workstations, servers, and applications.

- **eHealth — Response** collects response time data from a variety of sources for real-time analysis, historical reporting, and service level management. It allows you to detect degrading performance and declining availability of critical services and applications. eHealth — Response can collect response data from Application Response, Service Availability, Cisco IOS IP SLAs, and Juniper RPM.

**AdvantEDGE View**

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 AdvantEDGE View using a standard Web browser, giving you the freedom and flexibility to manage your systems from any location. Figure 38 illustrates the integration between SystemEDGE agents and AdvantEDGE View.

![Figure 38. AdvantEDGE View and SystemEDGE Agents](image)

*Introduction to eHealth*
You can use AdvantEDGE View to do the following:

- Determine the real-time status of critical systems and applications. (Figure 39 shows an example.)
- 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.

![CPU Statistics Information](image)

**Figure 39. Sample AdvantEDGE View Query**

With 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, 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% full?
• Which systems have been upgraded with the new operating system (OS) patch?

AdvantEDGE View provides queries for the following types of information:

• Configuration
• Performance
• Network
• Services

You can use AdvantEDGE View and SystemEDGE separately or with eHealth for integrated performance and availability management across your infrastructure. For more information about AdvantEDGE View, refer to the eHealth AdvantEDGE View User Guide.

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.

In addition, you can ensure that your network resources are well matched to the needs of the users and the demands of applications. Traffic Accountant provides insight on trends and usage patterns that impact the performance of your network. For more information about Traffic Accountant, refer to the eHealth Traffic Accountant Administration Guide.
Integration Modules

Integration modules enable eHealth to 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 NMSs, allowing NOC administrators to troubleshoot problems using the workflow with which they are familiar. In some cases, administrators can drill down from the NMS to eHealth reports to investigate the source of an alarm.

eHealth offers integration modules for some of the major element and network management systems, including the following:

- Alcatel 5620 Network Manager
- Cisco NetFlow FlowCollector
- Cisco VPN Solutions Center
- Cisco WAN Manager
- HP OpenView™ Network Node Manager
- Lucent® NavisCore™ and NavisXtend™ Statistics Server
- Micromuse Netcool
- Nortel® Preside Multiservice Data Manager

Integration modules allow you to obtain as much information as possible about the performance and availability of your network and to view it all in one place. For more information about integration modules, refer to the Web Help or the eHealth user guide for a specific integration module.
Distributed eHealth

Distributed eHealth is a highly scalable solution for managing large infrastructures through a single integrated view across multiple eHealth systems. It allows you to 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 essentially a reporting front end. 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.

Figure 40 illustrates a single Distributed eHealth Console that can report on data from several Distributed eHealth Systems. For more information about Distributed eHealth, refer to the Web Help or the Distributed eHealth Administration Guide.
Figure 40. Scalability and Flexibility with Distributed eHealth
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 the following reasons:

- **Security.** You do not want each remote polling site to have 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.) This may be important for service providers or large corporations with separate divisions.

- **Logistics.** Your infrastructure consists 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.)

**Combining Remote Polling with Distributed eHealth.** 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. This 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.

*For more information about remote polling, refer to Using the eHealth Remote Poller.*
Where to Go from Here

After reading this chapter, you should have a general understanding of eHealth technology keys, AdvantEDGE View, Traffic Accountant, integration modules, Distributed eHealth, and remote polling. Now read Chapter 8 to learn about the user interfaces of eHealth.
Using eHealth

This chapter provides an overview of the ways in which users (IT administrators, report consumers, and others) can interact with eHealth. It includes an introduction to the eHealth Web interface.

User Interfaces to eHealth

eHealth provides three main user interfaces:

- eHealth console
- Command line interface
- eHealth Web interface

The eHealth console and the command line interface are generally used only by eHealth administrators to set up, configure, and manage eHealth operations. Using the eHealth console, the administrator can manage licenses; discover elements; schedule eHealth jobs; manage polling; set options; create groups, group lists, and views; run, schedule, and customize reports; and manage the eHealth database. The administrator can use the command line interface to perform many of the same functions that the console offers. The command line interface also makes available some advanced functions that are not available through the eHealth console.
Only authorized users have access to the eHealth console and the command interface. For details on how to use these interfaces, refer to the Web Help, the eHealth Administration Guide, and the eHealth Administration Reference.

The eHealth Web interface allows users to access eHealth reports and applications using Web browsers on their local systems. With this interface, users can easily view scheduled reports, run reports on demand, or use other authorized functions, regardless of whether they are local or remote.

Introduction to the eHealth Web Interface

This section introduces the Web interface and provides information to help you get started using it. This section describes the following topics:

- Overview of the eHealth Web interface
- How to access the eHealth Web interface
- Overview of Web pages
- How to use online help

Overview of the eHealth Web Interface

Many different groups of users can use the eHealth Web interface, including the following:

- NOC administrators
- System administrators
- Network planners
- CIOs
- Application managers
- Consultants and analysts
- Service providers and their customers
- eHealth administrators
These people can use the Web interface to perform the following tasks:

- View scheduled reports, including MyHealth reports.
- Run and view reports on demand.
- Download Live Exceptions, Live Status, and Live Trend.
- Manage Application Response and AR agents.
- Manage 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.

**How to Access the eHealth Web Interface**

Before you can access the eHealth Web interface, you must obtain the following information. Ask your eHealth Web administrator for these details.

- **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`

  For example, if the eHealth Web server resides on the workstation `chicago` and the domain is `myCompany.com`, your eHealth Web server URL is the following:
  ```
  http://chicago.myCompany.com
  ```

- **Your user name and password** for the eHealth Web interface. When setting up the Web interface, the administrator creates a user account for each user, assigns a password, and defines access settings. Some organizations may choose to disable security for the Web interface, in which case you do not need a user name or password.
When you have this information, you are ready to access the eHealth Web interface.

**NOTE**

The following procedure assumes that eHealth is installed and properly configured and that the eHealth Web interface is established and ready to use.

Also, the remainder of this chapter shows default screens and describes the default behavior of the eHealth Web interface. Your organization may customize the appearance of the screens and the default behavior.

To access the eHealth Web interface:

1. Open a Web browser window.
2. Enter the URL for the eHealth Web server in the **Address** or **Location** field of the browser window.
3. On the eHealth Welcome screen, click **Continue**; see Figure 41.

---

![eHealth Welcome Screen](image)

**Figure 41. eHealth Welcome Screen**

*Introduction to eHealth*
4. If the system prompts you, enter your eHealth Web username and password and click **OK**.

The eHealth Web interface appears, displaying the Organization page for most users or the Administration page for eHealth Web administrators; see Figure 42. (The eHealth Web administrator can specify your initial page.)

![Figure 42. The eHealth Web Interface](image)

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; certain tabs shown in the above illustration do not appear if you are not authorized to access those functions.

Click a tab on the navigation bar to access a Web page or click the Help icon to access online help. The following sections provide descriptions of the Web pages and more information about online help.
Overview of Web Pages

The eHealth Web interface is organized to streamline and simplify your use of eHealth reports and applications. The following sections provide an overview of each Web page.

Gateway

The Gateway page of the eHealth Web interface 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. Figure 43 shows the default Gateway page.

![Figure 43. The Gateway Page of the eHealth Web Interface](image)

Typically, your eHealth Web administrator customizes this page to meet the needs of your organization’s eHealth users. For information on how to customize the Gateway page, eHealth Web administrators can refer to the Web Help.
Organization

The Organization page of the eHealth Web interface allows you to view the structure of your organization and to list available reports based on how elements are organized: by element, node, group, and group list. From this page, for example, you can select a group and view or run reports for that group. This lets you think in terms of the organization of your IT infrastructure, rather than which report you need to access to learn about a certain group of elements.

Figure 44 describes how to use the Organization page. The left frame lists the defined subjects (group lists, groups, elements, and nodes) of your infrastructure. Click a plus sign (+) to the left of a subject to expand the list. For example, clicking the plus sign next to a group list displays a list of the groups that are members of the group list. For information about using and interpreting reports, refer to the Web Help and the eHealth Reports Guide.

Click a report icon to run a report for the selected subject.
Report List

The Report List page of the eHealth Web interface provides a list of all 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 another way, 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. Use the filters at the top of the page to specify your filter criteria and click Redisplay to view the new list.

Figure 45 describes how to use the Report List page to filter, sort, and view available reports. For information on using and interpreting reports to manage your IT infrastructure, refer to the Web Help and the eHealth Reports Guide.
**Run Reports**

Use the Run Reports page of the eHealth Web interface to run reports on demand. Remember that running reports on demand can take time, because eHealth may need to analyze the data that appears in the reports.

To run a report, simply choose the type of report from the left column, complete the report criteria that appear to the right, and click **Generate Report**. (Refer to Figure 46.)

If you plan to run a certain report regularly, you can save the report definition by entering a template name and clicking **Save Report Template**. The report then appears in the left frame as a type of report to run.

For more information about generating reports, refer to the Web Help and the *eHealth Reports Guide*.

---

**Figure 46. How to Use the Run Reports Page**

Choose the report to run.  
Enter report criteria.  
Click here to generate the report.  
Save the report settings, if desired.  

*For information about running Health reports and Service Level reports on demand, refer to “Running Health and Service Level Reports” on page 65.*
MyHealth

The MyHealth page of the eHealth Web interface provides access to your MyHealth reports, each of which contains a series of charts and tables tailored to your specific interests. MyHealth allows you to customize reports to show only the elements and groups that you consider critical. Figure 47 shows a sample MyHealth report.

Figure 47. Viewing a MyHealth Report on the MyHealth Page

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. For more information about MyHealth, refer to “MyHealth Reports” on page 66, the Web Help, or the eHealth Reports Guide.
Live Health

The Live Health page of the eHealth Web interface allows you to download Live Status, Live Exceptions, the Business Service Console, and Live Trend to the client desktop:

- Use Live Status to access a real-time graphical display of the overall health of your IT infrastructure.
- Use Live Exceptions to perform real-time monitoring of your infrastructure and to identify performance problems as they occur. The Live Exceptions Browser can display alarms generated by Live Health — Fault Manager, which receives and processes SNMP traps from other sources.
- Use Live Trend to create and view charts that monitor statistics elements polled by eHealth.

Figure 48 shows the Live Health page. For more information about Live Health, refer to “Live Health” on page 71 or the Web Help.

Figure 48. The Live Health Page of the eHealth Web Interface
**System & Apps**

Figure 49 shows the System & Apps page of the eHealth Web interface. This page provides access to three major eHealth applications:

- AdvantEDGE View, the Web-based user interface and element manager for use with SystemEDGE agents.
- Application Response (AR)
- Service Availability (SA)

![Figure 49. The Systems & Apps Page of the eHealth Web Interface](image)

Figure 50 shows the AdvantEDGE View page. You can use AdvantEDGE View to deploy, manage, and configure SystemEDGE agents and Application Integration Modules (AIMs); query SystemEDGE agents; and search MIBs.

To learn more about AdvantEDGE View, refer to “AdvantEDGE View” on page 85, the Web Help, or the eHealth AdvantEDGE View User Guide.
Application Response allows you to manage AR agents; monitor specific business applications and view transactions of a selected application; identify servers associated with those applications; and download AR tools. Service Availability allows you to create and manage SA tests, SA test agents and test sets, and SA test profiles; and monitor and generate reports on SA agents and tests.
Administration

The Administration page of the eHealth Web interface provides access to administrative functions for authorized users and eHealth Web administrators. Figure 51 describes how to select an administrative function to perform.

Figure 51. How to Use the Administration Page

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 the following functions:
Introduction to the eHealth Web Interface

- **Site management.** Access logs, perform site configuration, perform advanced logging, remove reports marked for deletion.
- **User management.** Manage user accounts, log in to a different user account, set user preferences.

For more information, refer to the Web Help.

**How to Use Online Help**

The eHealth Web interface provides an extensive online help system. To access help relating to a particular page in the eHealth Web interface or a displayed report, click the Help icon on the right side of the page. To access help relating to a particular chart of a report, click the Help icon next to the chart. To access the Web Help Contents page, click the Help icon in the navigation bar. Figure 52 shows the access points for the different levels of help.

![Figure 52. How to Access Different Types of Online Help](image-url)
When you display a Web Help topic, it appears in a separate browser window. Each topic has a similar layout, as illustrated in Figure 53. On the help screen, underlined blue text indicates a hypertext link to another area of the same help topic or to another related help topic.

**Figure 53. Parts of a Web Help Topic**

For more information about online help for the eHealth Web interface, refer to “Web Help and Browser Hints,” which you can access from the Web Help Contents page.
Where to Go from Here

After reading this guide, you should have enough information to begin using the eHealth Web interface to run and view reports generated by eHealth. You should also have a general understanding of the major components of eHealth and which parts of your IT infrastructure they monitor.

For additional information, general users should first access the Web Help. If more information is required, they can also refer to these documents:

- *New Features in eHealth*
- *eHealth Reports Guide*

* eHealth administrators should also refer first to the Web Help; if they need additional information, they can refer to the following documents:

- *eHealth Readme file*
- *eHealth Installation Guide*
- *eHealth Administration Guide*
- *eHealth — Response Administration Guide*
- *eHealth — System and Application Administration Guide*
- *Network Health Administration Guide*
- *eHealth Traffic Accountant Administration Guide*

You can access these guides from the online help system of the eHealth Web interface. In addition, more user guides and documents that describe other parts of eHealth are available. Most of these are available on the eHealth TotalDoc online documentation CD-ROM. To access that information, ask your eHealth administrator for assistance.
Glossary

agent  In network management, 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.

alarm  In Live Exceptions, 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.

AIM  See eHealth application insight module (AIM).

American Standard Code for Information Interchange (ASCII)  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  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  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)  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  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  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.

cable modem  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  A 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 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)  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 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 top-level manager who is ultimately responsible for all information systems in an organization.

CIO  See Chief Information Officer (CIO).

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

console  See eHealth console.

CPU  See central processing unit (CPU).
Database Management System (DBMS)  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  The time required for a packet or frame to travel from the source to the destination.

destination  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).

Digital Subscriber Line (DSL)  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)  The system that locates and translates Internet domain names such as ca.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)  A protocol that enables dynamic allocation of IP addresses so that they can be reused.
**eHealth administrator**  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)**  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 administration and configuration console that allows an administrator to start and stop eHealth, manage the poller and the database, and administer the eHealth system. This is not the same as the eHealth Web interface.

**eHealth Web administrator**  A person responsible for managing and administering the eHealth Web server and eHealth Web interface.

**eHealth Web interface**  The eHealth interface that allows a user to access eHealth reports and applications from a Web browser. See also eHealth console.

**element**  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**  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)**  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 set of selection criteria used to focus a report on the desired data.

firewall  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  A firewall software package developed by Check Point Software Technologies, Ltd. See also firewall.

Frame Relay  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  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)  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)  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  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)  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)  Any operation, program, or device that transfers data to or from a computer.

Integrated Services Digital Network (ISDN)  A high-speed carrier service offered by telecommunications companies.

Internet Information Server  See IIS.

Internet Information Services  See IIS.

Internet Protocol (IP)  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)  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**  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**  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**  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**  *See* Lightweight Directory Access Protocol (LDAP).

**Lightweight Directory Access Protocol (LDAP)**  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, refer to RFC 2251.

**line print (LP)**  A common tool used to print documents over a UNIX network.

**local area network (LAN)**  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**  Megabytes.
mobile wireless  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.

network cloud  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 program that allows users to access file systems over the network.

network information service (NIS)  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)  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)  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  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.

normalize  A 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  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 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 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 (PC)  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  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  The physical (hardware) connection on a device that connects the device to a network.

Portable Document Format (PDF)  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)  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  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  The ability of eHealth to contact an element over the network. eHealth uses ping to determine reachability. See also ping.

real-time  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 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)** 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, refer to RFC 2021.

**report period** 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 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** 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 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** The mail transport agent (MTA) daemon that implements the Simple Mail Transfer Protocol (SMTP) mail protocol on UNIX systems.
service level agreement (SLA)  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)  The Transfer Control Protocol/Internet Protocol (TCP/IP) protocol used for sending and receiving e-mail in data networks. See also sendmail.


SLA  See service level agreement (SLA).

SMTP  See Simple Mail Transfer Protocol (SMTP).


storage area network (SAN)  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 network device that determines the path for sending a frame across a network. It may 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  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  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  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)  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 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 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.

variable  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)**  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 network that interconnects
multiple systems or networks over unlimited distances.

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

**workstation**  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)**  All of the resources on
the Internet that use Hypertext Transfer Protocol (HTTP).
Users of the Web access information through browser
software.
A
Administration page 106
Adobe Acrobat 100
ADSL. See Digital Subscriber Line.
AdvantEDGE Point modules 115
AdvantEDGE View 85
Agent Transaction Viewer 54
agents
  AR agents 53
  Cisco IP SLA 55
defined 111
deploying 86
Juniper RPM 56
SNMP agents 33, 79
SystemEDGE agents and 47
AIM. See eHealth application insight modules.
alarms
  consolidation of 76
defined 111
exporting with integration modules 88
Live Exceptions and 75
SystemEDGE agents and 47
Alcatel 88
alternate latency 118
American National Standards Institute 111
American Standard Code for Information Interchange 60, 111
ANSI. See American National Standards Institute.
Apache 51, 111
application management 13, 14, 53
application performance management 14, 53
Application Response 53
  about 53
eHealth — Response and 85
  sending performance data to eHealth 37
applications 22, 112
AR agents 53
ASCII. See American Standard Code for Information Interchange.
as-polled data 38
asset tracking 48
asynchronous transfer mode 28, 112
At a glance reports 57
At-a-Glance reports 61
ATM. See asynchronous transfer mode.
ATV. See Agent Transaction Viewer.
automatic notification 47
auto-registration of elements 36
availability 112
B
bandwidth 112
baseline 43
baseline period 43
bridge 29
Business Unit report 64

C
cable modems 112
capacity 112
cells 28, 113
central processing unit 113
channels 113
Check Point FireWall-1 51
Chief Information Officer 113
CIO. See Chief Information Officer.
Cisco
  IP SLA 55, 85
  NetFlow 87, 88
  SA Agent 55
  VPN Solutions Center 88
  WAN Manager 88
Citrix 53
Class of Service 30
client time 22
client/server networks 21
clients 21
clusters 89, 113
command interface 93
congestion 113
connect time 113
console 93, 113
consolidation of alarms 76
CoS. See Class of Service.
CPU
  resources 48
  See also central processing unit.

D
data
  analysis 41, 42, 65
  circuit-terminating equipment 29
collection 35
  remote polling 91
storage 38
terminal equipment 29
Database Management System 114
database roll-up 39
databases 38, 51
DBMS. See Database Management System.
DCE. See data circuit-terminating
equipment.
delay 114
destinations 24, 114
Deviation From Normal 76
DHCP. See Dynamic Host Configuration
  Protocol.
dial-up connection 26
Digital Subscriber Line 114
discover process 36
Distributed eHealth 81, 89
Distributed Live Health 81
dns. See domain name system.
domain name system 114
drill-down reports 65
DSL. See Digital Subscriber Line.
DTE. See data terminal equipment.
Dynamic Host Configuration Protocol 114
E

eHealth
   administrators 93, 115
   console 93
   database 38
   how it works 35
   integration modules 88
   reports 59
   solutions 11
   technology keys 84
   user interfaces 93
   Web administrators 95, 106, 115
   Web interface. See eHealth Web interface.
   eHealth — Network 84
   eHealth — Response 85
   eHealth — System and Application 85
   eHealth application insight modules
      about 49
      currently available 51
      defined 115
      eHealth — System and Application 85
   eHealth SystemEDGE
      about 47
      See also SystemEDGE agents.
   eHealth Web interface
      about 94
      accessing 96
      Administration page 106
      defined 115
      Gateway page 98
      introduction to 94
      Live Health page 103
      MyHealth page 102
      Organization page 99
      overview 94
      Report List page 100
      Run Reports page 101
      starting 96
      elements
         about 36
         defined 115
         grouping 40
         monitoring 37
         specifying elements to monitor 36
   e-mail 51
   end-to-end infrastructure management 16
   Exchange 51, 115
   exporting alarms 88

F
   fault management 69
   Fault Manager 79
   File Transfer Protocol 52, 115
   filters 116
   FireWall-1 51, 116
   firewalls 51, 116
   Fixed-Rate DSL 114
   footprint 48
   Frame Relay 29
   frames 29
   front-end 89
   FTP. See File Transfer Protocol.

G
   Gateway page 98
   goals 116
   group lists 40, 99
   groups 40, 86, 99
H
Health Index 41
Health reports 64, 65
help 107
Help icon 107
historical
  analysis reports 64
  data 60
HP OpenView 48, 88
HTTP
  monitoring 52
  See also Hypertext Transfer Protocol.
HTTPS
  monitoring 52
  See also Hypertext Transfer Protocol over Secure Socket Layer.
hubs 23
Hypertext Transfer Protocol
  defined 116
  monitoring 52
  over Secure Socket Layer 52, 116
input/output 117
Integrated Services Digital Network 26, 117
integration modules 88
Internet Information Server 117
Internet Information Services 117
Internet Protocol 24, 117
Internet Service Provider 27, 117
IP. See Internet Protocol.
ISDN. See Integrated Services Digital Network.
ISP. See Internet Service Provider.
IT
  infrastructure 118
  management 16
  See also Information Technology.

J
jitter 55, 56, 118
Juniper RPM 56, 85

L
LAN
  wireless LAN 125
  See also local area networks.
latency 118
Lightweight Directory Access Protocol 118
line print 118
Live Exceptions
  about 75
  browser 76
  installing 103
  overview 74
Live Health
   about 71
   applications 72
   Distributed eHealth and 81
   how it works 72
   page 103
Live Health — Fault Manager 79
Live Status 74, 103
Live Trend 78, 103
local area networks 23, 118
logical elements 36
LP. See line print.
Lucent 88

M
management information base 33
MB 118
MetaFrame 53
MIB
   translation file 33
   See also management information base.
Micromuse 48, 88
Microsoft
   Exchange 51, 115
   IIS 51
   SQL Server 51
   Terminal Services 53
mobile wireless 119
modems 25, 27
MTF. See MIB translation file.
MTTR 16
MyHealth
   page 102
   reports 66

N
NavisCore 88
NavisXtend 88
Netcool 48, 88
NetFlow 87
network file systems 119
network information services 119
network management 11
network management systems 48, 119
Network News Transfer Protocol 52, 119
network nodes 20
network resources 55, 56
network services 51
network time 22
networks
   about 20
   client/server 21
   local area 23
   network cloud 119
   technologies 25
   wide area 24
NFS. See network file systems.
NIS. See network information services.
NMS. See network management systems.
NNTP. See Network News Transfer Protocol.
nodes 20
normal 120
normalize 33, 120
Nortel 88
notification, automatic 47

O
online help 107
OpenView 48, 88
optical networking 120
Oracle 51
Organization page 99
P
packet internet groper 121
packet loss 55
packets 120
passwords
  changing 106
  for the eHealth Web interface 95
paths 120
PC. See personal computers.
PDF. See Portable Document Format.
performance management 70
permanent virtual circuits 30
personal computers 120
physical
  circuits 30
  elements 36
ping 52, 121
poller
  about 37
  remote 91
Portable Document Format 60, 121
ports 121
Post Office Protocol 3 52, 121
Preside 88
profiles 75
protocols 121
PVC. See permanent virtual circuits.

Q
QoS. See Quality of Service.
Quality of Service 30

R
RADSL. See Digital Subscriber Line.
RAS. See remote access servers.
Rate-Adaptive DSL 114
reachability 121
real-time
  defined 121
  monitoring 69
remote access servers 26, 121
remote network monitoring 87, 122
remote polling 91
Report List page 100
reports
  about 59
  At-a-Glance reports 61
  Cisco IP SLA reports 55
  customizing 66, 102
  drill-down reports 65
  generating 39
  Health reports 64, 65
  historical analysis reports 64
  historical data 60
  Juniper RPM reports 57
  MyHealth reports 66
  printing 100
  report periods 122
  running 101
  scheduling 65
  Service Level reports 64, 65
  standard reports 60
  templates 101
  Top N reports 63, 116
  Trend reports 61
  viewing 100
  What-If reports 63
response  
   endpoints 122  
   paths 120, 122  
   time 22, 53  
RMON. See remote network monitoring.  
RMON2. See remote network monitoring.  
roll-up process 39  
runners 24, 122  
rules 75  
Run Reports page 101

S

scheduling reports 65  
SDH 120  
security 91  
sendmail 122  
sender time 22  
servers 21  
Service Availability 52, 85  
service level agreements 31, 75, 123  
Service Level reports 64, 65  
service profiles 42  
Simple Mail Transfer Protocol 52, 123  
Simple Network Management Protocol 33  
site management 107  
SLA. See service level agreements.  
SMTP. See Simple Mail Transfer Protocol.  
SNMP  
   traps 33, 38, 124  
   See also Simple Network Management Protocol.  
SNMP agents  
   about 33  
   discovering 36  
eHealth — System and Application 85  
polling 37  
   SystemEDGE and 48  
source 24  
SQL Server 51

standard reports 60  
subjects 77, 99  
SVC. See switched virtual circuits.  
switched virtual circuits 30  
switches 23, 123  
system management 13  
SystemEDGE agents  
   about 47  
   AdvantEDGE View and 85  
   application insight modules and 49  
   benefits of 49  
eHealth — System and Application 85  
Service Availability and 52

T

T1 29, 123  
TCP. See Transmission Control Protocol.  
TCP/IP. See Transmission Control Protocol (TCP) and Internet Protocol (IP).  
TCP-connect 52  
technical Support 98  
technology keys 84  
templates 101  
terminal server applications 53  
Terminal Services 53  
throughput 124  
Time Over Threshold 76  
Top N reports 63, 116  
Top Processes 48  
traffic 124  
Traffic Accountant 87  
transactions 53  
Transmission Control Protocol 124  
traps 33, 38, 124  
trends  
   about 41  
   trend line 124  
   Trend reports 55, 61  
   Trend thresholds 41
U
URL 95
user interfaces 93
user management 107
user names
  changing 106
  for the eHealth Web interface 95
  logging into a different user account 106
  setting user preferences 106
user preferences 106

V
variables 124
VC. See virtual channels.
virtual
  channels 28
  circuits 30
Voice over IP 84, 125
VoIP. See Voice over IP.

W
WAN. See wide area networks.
Web interface. See eHealth Web interface.
Web servers 51
What-If reports 63
wide area networks 24, 125
wireless LAN 125
workstations 125
World Wide Web 125
WWW. See World Wide Web.

X
xDSD 114