NetIQ® Vivinet® Assessor 4.0

User Guide

June 2018

Legal Notice

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

About This Book and the Library

The *User Guide* provides conceptual information about NetIQ Vivinet Assessor and defines terminology and various related concepts.

Intended Audience

This book provides information for individuals responsible for understanding Vivinet Assessor concepts and for individuals implementing voice over IP (VoIP) or evaluating VoIP performance on a network.

Other Information in the Library

The Vivinet Assessor library provides the following resources:

Performance Endpoints Guide

Explains how to install, configure, and troubleshoot Performance Endpoint software for the platforms that Vivinet Assessor supports.

Messages Guide

Provides the text of messages associated with the Vivinet Assessor Console and the endpoints. Messages include information about why the error occurred and how you can avoid it in the future.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The Vivinet Assessor library is available in Adobe Acrobat (PDF) format from the Vivinet Assessor Documentation page of the NetIQ website.

Contents

1 Introducing Vivinet Assessor

Vivinet Assessor is part of a suite of products designed to test, evaluate, monitor, and manage multi-protocol and multi-platform data network. Vivinet Assessor measures and analyzes the salient factors that affect the performance of call traffic on data networks, thereby determining how well voice over IP (VoIP) is likely to perform on a particular network. With the data you receive from a VoIP Readiness Assessment, you can determine whether the network is ready for a VoIP implementation before you actually roll it out. Or you can make cost-effective decisions about network infrastructure and application traffic once you know which parts of the network are least ready to handle IP telephony.

1.1 Why Assess VoIP Readiness?

A packet network is worlds away from a circuit network. After all, it was designed to carry an entirely different type of traffic. In the U.S. and in many other parts of the world, the public switched telephone network (PSTN) is a triumph of 20th-century circuit-switching technology. We still expect and usually get near-perfect clarity from a telephone call made over the PSTN. But despite the astounding gains data-networking technology has made in the past several years, we do not expect anywhere near the same reliability from our data networks. That kind of reliability is not required for data.

An e-mail message or a file transfer can be delayed by as much as half an hour without exciting anyone's notice, yet delays of a few hundred milliseconds can ruin a VoIP telephone call, making it incomprehensible—or just annoying. When you start to run VoIP across any given enterprise network, delays caused by other applications, overloaded routers, or outdated switches are practically inevitable.

VoIP will undoubtedly be one of your most business-critical applications. An unreliable or poor-quality phone system is a recipe for disaster. But with Vivinet Assessor, you can test and troubleshoot VoIP *before* you roll it out—before you make substantial investments in equipment, software, training, and possibly unnecessary network upgrades. Vivinet Assessor is a vital tool for making smart investments and cost-effective infrastructure adjustments to get your network ready for VoIP.

The concept of "VoIP readiness" is central to Vivinet Assessor. Although it comprises several aspects of network capacity, configuration, and performance, the VoIP readiness of your network is assessed in terms of the following criteria:

- whether your network is ready to carry high-quality voice transmissions in its existing configuration. For more information, see Chapter 3, "Task 1: Performing a Network Inventory," on page 25.
- whether switches and routers have the resources recommended by the VoIP vendor. For more information, see Section 7.11, "Increasing Assessment Accuracy," on page 77.
- whether your network is ready to carry high-quality voice transmissions with its present bandwidth utilization. For more information, see Chapter 5, "Task 3: Assessing Network Utilization," on page 43.
- how much bandwidth you will need for the additional VoIP traffic. For more information, see Chapter 6, "Task 4: Modeling Bandwidth," on page 49.

- how much voice traffic can be added to your network in its existing configuration without significant degradation of call quality. For more information, see Chapter 7, “Task 5: Assessing VoIP Quality,” on page 55.
- how much money your organization stands to lose if call-quality problems on your network are not addressed. For more information, see Section 8.1, “Customizing a VoIP Readiness Assessment Report,” on page 91.

The final criterion listed above is vitally important, especially if you are moving to VoIP as a cost-saving measure. And the bandwidth criterion is similarly important because your implementation will surely expand in the future as new users, new demands, and new equipment are added to the system.

1.2 How Vivinet Assessor Can Help

Vivinet Assessor emphasizes quality in its assessments of VoIP readiness because a low-quality voice transmission is a waste of bandwidth. If VoIP does not perform well, the parties engaged in conversation will not be able to understand each other.

Assessing the quality of voice over IP is crucial at several distinct points in a VoIP implementation:

- When considering a VoIP deployment
- When contemplating upgrades to the network, such as adding bandwidth
- After tuning the network in preparation for VoIP
- When planning to expand your VoIP network for additional users.

The key benefits Vivinet Assessor offers make it truly unique.

It is the leading solution for assessing VoIP quality prior to deployment.

Find out how voice over IP will perform before the first user makes the first VoIP phone call. Once you know how VoIP is likely to perform, you can make well-informed, cost-effective decisions about network infrastructure.

Vivinet Assessor provides a simple, software-only solution.

Complete a series of steps to configure a VoIP Readiness Assessment in a few minutes. There is nothing to plug in to the network, and no hardware to purchase.

Predictive modeling helps with capacity planning.

To find out how much bandwidth you will need on a given link, select a link that Vivinet Assessor has been monitoring for utilization statistics. By calculating the bandwidth needs of the VoIP calls you plan to run, Vivinet Assessor derives the VoIP call capacity of a link based on its present load. You then can make fully informed decisions about upgrades.

VoIP Readiness Assessments also highlight problem areas.

Vivinet Assessor monitors network utilization and shows you exactly which devices and links are too overtaxed to carry additional VoIP packets and deliver high-quality calls. It can analyze the current resources of network devices to ensure they are configured properly for VoIP. And it sends simulated VoIP traffic between pre-selected points on your network to test call quality.

Vivinet Assessor **compares device configuration** to a set of rules you supply to ensure that routers and switches have the most recent operating system revisions, the vendor-recommended modules, and any required patches. Any violations of your rules are clearly flagged so you can make changes.

It accurately **measures current network utilization levels** by sending SNMP queries to network devices. Based on these findings, it assigns a VoIP Readiness Rating to network devices and links. Ratings categories are based on the latest industry research into standards for quality voice over IP transmissions. Results are clearly presented in polished, yet customizable, reports.

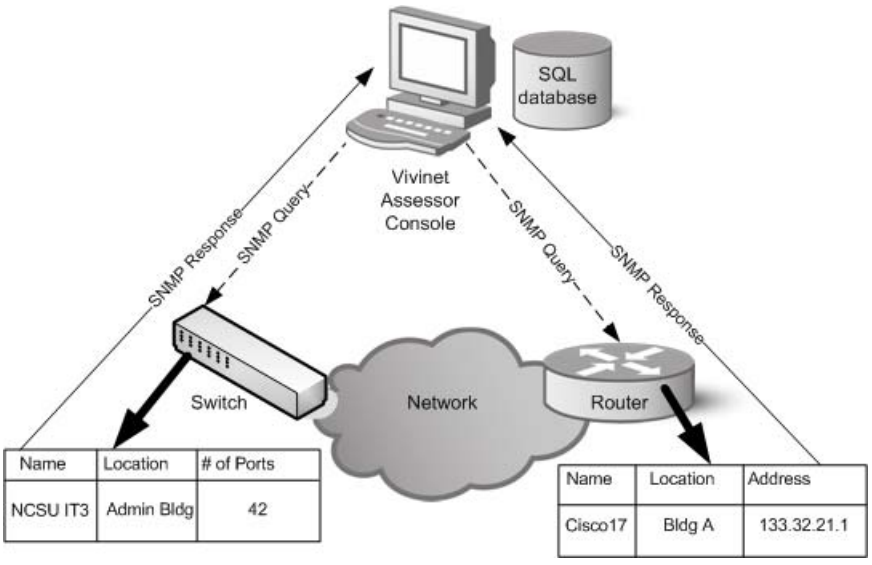
You can use link utilization information to perform **"what-if" analyses**. From the results of bandwidth modeling, you gain insight into potential needs for additional or upgraded devices and bandwidth.

It also **predicts call quality** by precisely emulating voice over IP and evaluating it using innovative patented and patent-pending technology. Vivinet Assessor can calculate an industry-standard **Mean Opinion Score** for a simulated VoIP call, and uses an algorithm derived from the ITU standard E-Model to assess call quality.

Vivinet Assessor relies on unobtrusive software agents to generate VoIP-like traffic according to a set schedule. These agents—called endpoints—can be installed anywhere on the network and eliminate the need to plug in a protocol analyzer. Vivinet Assessor's distributed endpoints mean that a VoIP Quality assessment runs just like a series of VoIP phone calls and encounters the same network conditions. So your results provide **an accurate prediction of the overall call quality** you can expect post-deployment.

1.3 How Vivinet Assessor Works

The Vivinet Assessor architecture consists of a console program with access to a SQL database and distributed endpoints, small software programs used to generate simulated VoIP traffic to send over the network and measure performance. The Console uses SNMP queries to find out device identity, configuration, and utilization information from routers and switches. Router and switch interface data is used to discover WAN and LAN links and access utilization statistics. All information is sent back to the Console, where it is stored in the database and used to create reports.



To assess VoIP quality, Vivinet Assessor communicates with distributed software agents called Performance Endpoints, instructing them to send simulated VoIP traffic across the network and take measurements. Before you run a VoIP Readiness Assessment, you should install NetIQ Performance

Endpoints on every computer you plan to include in the VoIP Quality assessment. For more information, see Section 1.4, “NetIQ Performance Endpoints,” on page 12. Then proceed with each assessment task in order, as directed by the Vivinet Assessor user interface:

1. Click **Inventory Network**. Specify how Vivinet Assessor will discover switches, routers, and links on your network. Once discovered, devices and links are automatically entered into the Assessor SQL database, along with their names, locations, and IP addresses. For more information, see Chapter 3, “Task 1: Performing a Network Inventory,” on page 25.
2. Click **Assess Configuration**. Using the information collected during the Network Inventory and from a configuration rules file you supply, Vivinet Assessor analyzes devices for available resources, such as memory and disk space, software, and updates. For more information, see Chapter 4, “Task 2: Assessing Configuration,” on page 35.
3. Click **Assess Utilization**. With the information collected during the Network Inventory, Vivinet Assessor monitors your network to assess the utilization and rate the VoIP readiness of discovered devices and links. Monitoring proceeds according to a schedule you create. For more information, see Chapter 5, “Task 3: Assessing Network Utilization,” on page 43.
4. Click **Model Bandwidth**. With the link and utilization statistics collected during the Network Inventory and Utilization assessment, Vivinet Assessor helps predict the amount of bandwidth you need on selected links under certain VoIP usage scenarios. For more information, see Chapter 6, “Task 4: Modeling Bandwidth,” on page 49.
5. Click **Assess VoIP Quality**. Design a VoIP Quality assessment based on pairs and groups of computers (endpoints). Vivinet Assessor sends simulated VoIP calls between the endpoints and measures call quality. For more information, see Chapter 7, “Task 5: Assessing VoIP Quality,” on page 55.

At any point during the VoIP Readiness Assessment, you can generate a report of the data collected thus far. Data from all assessment types is compiled into a single VoIP Readiness Assessment report.

1.4 NetIQ Performance Endpoints

Before you begin using Vivinet Assessor, you should install NetIQ Performance Endpoint software on each computer you plan to use in VoIP Quality assessments. Vivinet Assessor ships with the latest endpoints for several operating systems:

- Windows Server 2016
- Windows 10 (32-bit or 64-bit)
- Windows Server 2012 R2
- Windows 8.1 (32-bit or 64-bit)
- Windows Server 2012
- Windows 8 (32-bit or 64-bit)
- Windows Server 2008 R2
- Windows 7 (32-bit or 64-bit)
- Windows Server 2008 (32-bit and 64-bit)
- Windows Vista (32-bit or 64-bit)

NOTE

- Although Vivinet Assessor itself is not supported on Windows NT, Linux, or Sun Solaris platforms, it can gather data from endpoints installed on computers running these operating systems.
- To allow VoIP RTP traffic to run on dynamic ports, **you must disable the Windows firewall** on any computer running Windows 7/Server 2008 computer or later versions of Windows on which Performance Endpoint software is running.

For best results, avoid using Windows Me and pre-ULTRA Sun operating systems. The high-precision clocks on these systems are the least accurate of all the supported endpoint operating systems.

In Microsoft Windows environments, the endpoint runs as a service after you enable it during installation. With other operating systems, the endpoint starts automatically. It functions only during assessments, and should not interfere with other application traffic on your computer.

The Performance Endpoint software can be installed in a matter of minutes; users on the network to be assessed can easily install the software themselves on their desktop computers. They can download it free of charge at the Current Performance Endpoints Product Upgrades page, or you can make it available for installation from a central server.

A web-based endpoint for Windows is also available. It does not have to be installed. Users can run it on their computers from a web browser, and when the assessment is completed, it is not necessary to uninstall anything; the endpoint no longer runs once the computer is restarted.

NOTE: Endpoints are not a prerequisite for running a Network Inventory, for assessing device configuration and device and link utilization, or for performing Bandwidth Modeling.

Plan to deploy the endpoint software on a variety of computers, taking the following into consideration:

- Deploy endpoints both near to and far from the places where you plan to install critical equipment, such as VoIP gateways and Cisco Unified Communication Manager servers. Set up call groups to determine whether location plays a role in call quality.
- Deploy a few endpoints on either side of a WAN link, which should be part of any assessment.
- Deploy endpoints on either side of a firewall to determine how well the firewall will handle VoIP traffic.
- Deploy enough endpoints to get a sense for the geographical distribution of call quality. A single endpoint can perform successfully in up to 50 two-way calls without sacrificing call quality. A two-way call is one in which a phone accepts one call while sending another.

Once you have installed some endpoints or asked users to start running the Web-based endpoint, you can use the endpoint discovery feature to gather information about endpoint network addresses automatically and add it to the assessment database. For more information, see Section 7.3, “Discovering,” on page 57.

For more information about endpoints, see the *Performance Endpoints User Guide*, included with the Vivinet Assessor documentation set.

2 Installing and Registering Vivinet Assessor

This chapter describes system requirements and provides instructions for installing and registering Vivinet Assessor.

2.1 Installation Considerations

To use Vivinet Assessor, you must install two components: the Vivinet Assessor Console and NetIQ Performance Endpoints. For more information, see Section 1.4, “NetIQ Performance Endpoints,” on page 12. Use the topics in this section to help you prepare to install Vivinet Assessor.

2.1.1 Upgrading From Version 3.3 or Earlier

When you upgrade from a previous version to Vivinet Assessor 4.0, the product runs in the demo mode. You need to register Vivinet Assessor 4.0 using a new authorization key to use the full functionality. Please contact the NetIQ Sales representative or login to the NetIQ Customer Center to get the authorization key.

To register Vivinet Assessor 4.0, see Section 2.3.2, “Registering using a License Key,” on page 24.

IMPORTANT: Before upgrading to Vivinet Assessor 4.0 from a previous version, you *must* back up your database files and export them to another location. After you install Vivinet Assessor 4.0, you can import your database files into Vivinet Assessor. For more information, see Section 10.3, “Exporting and Importing Assessments, Scripts, and Definitions,” on page 118.

2.1.2 Security Considerations

Vivinet Assessor uses Microsoft SQL Server 2014 as its database engine.

Vivinet Assessor uses Windows authentication to install the SQL Server named instance. This ensures that anyone seeking access to the SQL Server database on your computer has to be logged in with administrator privileges, restricting access to the user or group who installed Vivinet Assessor. But you may still want to take the following steps to provide extra security:

- Ensure the Vivinet Assessor Console computer is connected only to a trusted network.
- Secure the Vivinet Assessor Console computer behind a firewall.
- Never give an unauthorized user access to the computer where Vivinet Assessor is installed.

You should install any subsequent security updates for this version of Microsoft SQL server as soon as they become available.

Vivinet Assessor installs the SQL Server named instance, `VASSESSOR`, to the location you specify during the Vivinet Assessor installation process. The default location is `c:\Program Files\Microsoft SQL Server`. In this directory, the `VASSESSOR` instance is installed in a subfolder

called `MSSQL##.VASSESSOR\MSSQL\Binn`. The database files are installed in the `MSSQL##\MSSQL\Data` subfolder. In both subfolders, `##` is the major version of the version of Microsoft SQL Server of the `VASSESSOR` named instance.

One essential step in setting up the Utilization assessment and Network Inventory is providing *SNMP permissions*, the security information that allows Vivinet Assessor to contact and query devices on your network. The type of information you configure varies according to the version of SNMP that is implemented on a device. Vivinet Assessor supports SNMP versions 1, 2, and 3. For more information, see Section 3.1, “Setting Up a Network Inventory,” on page 25.

2.1.3 System Requirements

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page. Unless noted otherwise, Vivinet Assessor supports all updates, hotfixes, and service packs for the releases listed below.

Vivinet Assessor has the following system requirements for the computer on which you want to run assessments:

Software/Hardware	Version
Microsoft Windows operating system	You must have Administrator privileges to install and run Vivinet Assessor on one of the following operating systems: ◆ Windows Server 2016 ◆ Windows 10 (32-bit or 64-bit) ◆ Windows Server 2012 R2 ◆ Windows 8.1 (32-bit or 64-bit) ◆ Windows Server 2012 ◆ Windows 8 (32-bit or 64-bit) ◆ Windows Server 2008 R2 ◆ Windows 7 (32-bit or 64-bit) ◆ Windows Server 2008 (32-bit or 64-bit) ◆ Windows Vista (32-bit or 64-bit) **FOR IP Quality of Service (QoS)** Support for Quality of Service (QoS) settings on endpoint computers running Windows 7 and Windows Server 2008 R2 or later versions of Windows requires the NetIQ Performance Endpoints version 5.1.15750.0 or later. You can download the updated Performance Endpoints at the Current Performance Endpoints Product Upgrades page.

Software/Hardware	Version
Microsoft SQL Server	One of the following versions of Microsoft SQL Server: ◆ 2016 ◆ 2014 If SQL Server is not already installed in an instance named VASSESSOR, Vivinet Assessor will install an instance of SQL Server 2014 Express Edition. ◆ 2012 ◆ 2008 R2 ◆ 2008 ◆ 2005 **IMPORTANT:** If you install SQL Server 2012 or later, you must manually configure `NT Authority/SYSTEM`. For more information, see Section 2.2.2, “Installing an SQL Server,” on page 21.
Microsoft Office	One of the following: ◆ 2016 (32-bit) ◆ 2013 (32-bit) ◆ 2010 (32-bit) ◆ 2007 (32-bit) ◆ 2003 (32-bit) **NOTE:** Microsoft Word and Excel are required for generating and printing reports.
Microsoft .NET Framework	2.0 or later
Microsoft Windows Installer 3.1	3.1
NetIQ Performance Endpoints Installed on the computers you want to include in a VoIP assessment. For more information, see Section 1.4, “NetIQ Performance Endpoints,” on page 12.	

2.1.4 Performance Tips for Large Assessments

The following guidelines suggest the maximum number of simultaneous two-way VoIP calls you can run per endpoint during the assessment of VoIP quality before the call load itself begins to induce impairments to the call-quality scores.

In internal testing, two Pentium 800 computers with 256 MB of RAM on Windows Server 2008 R2 served as the endpoints. Although the codec used is the most significant performance factor, the brand of NIC installed in the endpoints is also important. In NetIQ testing, an Intel PRO/100+ Server adapter was used.

Codec	Number of Calls
G.711u; G.711a (64 kbps)	100

Codec	Number of Calls
G.726 (32 kbps)	125
G.729; G.729A (8 kbps)	75
G.723m (6.3 kbps)	125
G.723a (5.3 kbps)	125

2.1.5 Disk Space Considerations

Each assessment you create is stored as a separate database in the system. By default, these databases are all on the same hard drive where you installed Vivinet Assessor. However, you can specify another location for assessments, such as on another hard drive, by using the Assessment Location feature. For more information, see Section 10.2, “Changing the Location of Your Assessment,” on page 117.

Some system-related databases will always reside on the hard drive where Vivinet Assessor is installed. Although most of these databases are negligible in size, one database may present disk-space issues. The system’s temporary database, `tempdb.mdf`, is used internally for processing, committing, and rolling back data in the database system. This database is initially about 3 MB in size, but grows based on activity. The space used by this database shrinks only when the database system is restarted.

The database system is restarted when the computer is restarted. Therefore, if you notice space problems due to the size of this database, you should save your work and restart the system, or restart the `MSSQL$VASSESSOR` system service.

To restart the system service:

1. Navigate to the Control Panel, double-click **Administrative Tools** and then double-click **Services**.
2. Select **MSSQL$VASSESSOR**.
3. On the Actions menu, select **Restart**.

2.1.6 Bandwidth and Performance Considerations

When you perform a Network Inventory and assess Utilization and VoIP Quality, Vivinet Assessor sends SNMP queries or simulated VoIP traffic over your network. In addition, some TCP traffic is generated during endpoint discovery. And for each assessment task, some traffic necessarily passes from the Vivinet Assessor Console to your network devices.

For the Network Inventory, a small amount of traffic is generated for each network device to be discovered. Thus, if you enter a very broad address range for your discovery scan—or several medium-sized address ranges—and if a great many devices share the address ranges to be scanned, be aware of the SNMP traffic that will be generated.

Each time Vivinet Assessor attempts to discover a device at a specific IP address during the Network Inventory, it sends a 100-byte SNMP packet over the network. During inventory setup, you select the number of times this SNMP query will be sent. For more information, see Section 3.1.1, “Editing SNMP Configuration Information,” on page 26. Once a device responds, a separate SNMP query of 100 bytes is sent to obtain each type of information Vivinet Assessor collects for each device type.

Because of the comparatively large amount of data collected about routers, the maximum amount of data sent between the Console and a discovered device, approximately 3500 bytes, is sent when a router is discovered.

When you assess utilization, device and link measurements are collected using SNMP queries. To monitor a large number of devices, be sure the Console has a very fast connection to the network where monitoring is being performed.

Some assessment tasks may be performed simultaneously. Although you cannot perform a Utilization assessment while the Network Inventory is running, you can assess utilization and VoIP Quality simultaneously. And you can set up a Configuration assessment while a Utilization assessment is running, but you cannot run it until the Utilization assessment has completed.

2.1.7 Configuring User Account Control (UAC) Settings

In order for the Vivinet Assessor console to function properly on computers running recent versions of Microsoft Windows operating systems, you must change the User Account Control (UAC) settings from the default.

To change the UAC settings:

1. Navigate to the Control Panel and double-click **User Accounts**.
2. Click the **Change User Account Control Settings** link.
3. Slide the settings selector to the 4th option: **Never notify me when programs try to install software ... I make changes to Windows settings**.
4. Click **OK**.
5. Reboot the computer.

2.2 Installing Vivinet Assessor

Before you install Vivinet Assessor, read Section 2.1.2, “Security Considerations,” on page 15 for important information about authentication on the supported Windows operating systems.

Ensure File and Print Sharing for Microsoft Networks is enabled in the Network Connections Properties dialog box before you begin the installation. Otherwise, the installation process may unexpectedly fail just before it completes.

Vivinet Assessor supports silent installations but does not support advertised installations. For silent upgrades, a silent removal of the old version of the software is required before invoking the silent installation of the new product version.

NOTE

- The installation program verifies that Microsoft Internet Explorer 5.0 or later, Word 2003 or later, and Excel 2003 or later are installed. Vivinet Assessor does not support earlier versions of these applications. If you see requirement warnings for any of these applications, you need to update your computer, but the installation may still complete successfully. Installation fails if Internet Explorer 5.0 or later is absent.
- The installation also checks for enough disk space and displays a message if you need to free some space. If this occurs, you can exit the installation program to free the necessary space, or you can free the space without exiting the installation program. However, if you choose to exit, you should free an additional 15 MB of space above what the installation program reports.

2.2.1 Installing Vivinet Assessor

You can install Vivinet Assessor directly from the NetIQ web site.

When installing Vivinet Assessor, you have the option of:

- allowing Vivinet Assessor to install a SQL using SQL 2014, or
- pre-installing a version of an SQL server and naming the instance VASSESSOR.

NOTE: If you are using Microsoft SQL Server 2012 or later, you must manually grant '`NT Authority\System`' the '`sysadmin`' database role on the `VASSESSOR` named instance. For additional information about this, see Section 2.2.2, “Installing an SQL Server,” on page 21.

Installing Vivinet Assessor

To install Vivinet Assessor, follow the steps below:

1. Navigate to www.netiq.com/products/va/default.asp.
2. When prompted, register or log in.
3. Click the **Vivinet Assessor Trial Package** link.
4. Click **Save**.
5. Select a location in which to save the install package on your computer, and start the download.
6. Navigate to the `vivinetassessor.exe` file you downloaded, and double-click it. This self-extracting ZIP file unpacks itself and automatically launches `maininstaller.exe`. A Welcome dialog box advises you that the installation process installs both Microsoft SQL Server 2014 and Vivinet Assessor.
7. If you wish to pre-install a version of SQL Server yourself, click **Skip SQL Server Installation**.

Installing SQL Server 2014 Express

1. The Microsoft SQL Server 2014 Express dialog box identifies the location in which SQL Server 2014 Express will be installed. To change the location in which SQL Server 2014 Express is installed, click **Browse** and navigate to the new location.
2. Click **Next**.
3. On the License Terms dialog box, click **I accept the license terms**, then click Next.
4. In the Feature Selection dialog box, verify the **Database Engine Services** is selected, then click **Next**.
5. In the Instance Configuration dialog box, verify the named instance is set to **VASSESSOR**, then click `Next`. Do not change this value.
6. in the Server Configuration dialog box, click `Next`.
7. In the Database Engine Configuration dialog box, verify the current logged-on user is listed in the **Specify SQL Server administrators** list. If it is not listed, click **Add Current User**, then click **Next**.
8. On the Error Reporting dialog, click **Next**.

The SQL Server installation program now performs the necessary installation tasks. Once the tasks are completed, you may be asked to restart your computer. If this happens, restart your computer, then re-start the Vivinet Assessor installer. Go to the `C:\Temp\VivinetAssessor` folder, or the location where you extracted the Vivinet Assessor installation files, and click `MainInstaller.exe`.

WARNING: If you only restart your computer and do not restart Vivinet Assessor installation program, Vivinet Assessor will not be installed.

Continuing the Installation of Vivinet Assessor

1. Click **Next** to continue the installation of Vivinet Assessor.
2. Click **I accept the terms in the license agreement**, then click **Next**.
3. Click **Next** to accept the default location in which to install Vivinet Assessor, or click **Change** to select a different folder, then click **Next**. Install Vivinet Assessor on a local hard disk of the computer you are using. Installing on a LAN drive is not recommended; the additional network traffic will influence your results. The default directory is `Program Files\Micro Focus\Vivinet Assessor` or the location where you extracted the Vivinet Assessor 4.0 installation files on your computer.
4. Click **Install** to complete the installation process.

   The Vivinet Assessor installation program creates a NetIQ Vivinet Assessor program icon, which you can access from your Windows **Start** menu.

2.2.2 Installing an SQL Server

If you pre-install SQL Server 2014 or later, after completing the installation, you must manually configure the SQL server.

1. Open the SQL Server Management Studio.
2. Connect to the VASSESSOR instance of the SQL Server.
3. In the Object Explorer pane, select **Security > Logins**.
4. Right-click the NT Authority\System **Account Name** and select **Properties**.
5. In the Object Explorer pane, select **Server Roles > Server Roles**
6. Select the **sysadmin** checkbox.
7. Click **Save**.

2.2.3 Vivinet Assessor Directories and File Types

During installation, a directory structure is created in the Windows Program Files folder. Vivinet Assessor directories contain the following files and file types:

Directory	Contents
Micro Focus\Vivinet Assessor	◆ executable files (`VAssessor.exe` and `varun.exe`) for the Console and Scheduler/run engine. For more information, see Section 2.2.4, “Vivinet Assessor Scheduler Service,” on page 22. ◆ .dll files ◆ Release Notes and PDF versions of Vivinet Assessor documentation: `vivinetassessor_releasenotes.html`, `Messages.pdf`, `VivinetEndpoints.pdf`, and `AssessorUserGuide.pdf` ◆ error log in binary format, `assessor.log`, for all Assessor application errors ◆ error files, if any unexpected errors occur (`assert.err`) ◆ schema rules file (`PropertyRuleSchema.xsd`), which defines the building blocks for valid data and rule files used to perform the Configuration assessment ◆ program `fmtlog.exe`, used to format log files ◆ ASCII data file that contains any QoS definitions you configured (`servqual.dat`)
Micro Focus\Vivinet Assessor\BACKUP	Copies of your assessments for backup when you upgrade or uninstall the software
Micro Focus\Vivinet Assessor\Diagnoses	Vivinet Diagnostics files (`.dgv`) generated during a VoIP Quality assessment. For more information, see Section 7.9, “Working With Vivinet Diagnostics,” on page 72.
Micro Focus\Vivinet Assessor\Help	Help files with file extension `.chm`
Micro Focus\Vivinet Assessor\MIBS	MIB files to help Vivinet Assessor interface with certain types of MIBs
Micro Focus\Vivinet Assessor\Samples	A sample assessment (`Sample.aef`) and a sample Configuration assessment rules file (`SampleRules.xml`) to help you run assessments.
Micro Focus\Vivinet Assessor\Templates	Microsoft Word templates (`.dot`) used to format Vivinet Assessor reports.

2.2.4 Vivinet Assessor Scheduler Service

The Vivinet Assessor Scheduler service (`varun.exe`) runs in the background to schedule and run VoIP Readiness Assessments and process their results. The Scheduler service should always be running. When not actively running an assessment, it waits idle, consuming few system resources. When an assessment is run or verified, the Scheduler is invoked to build and send instructions for the

endpoints, which then run the requested VoIP traffic and send the results back to the scheduler. The Scheduler stores the results in the SQL database. The Vivinet Assessor Console communicates with the Scheduler using system events and status associated with the assessment in the database.

The Scheduler runs as a system service. When you log out, the Scheduler will still be running. Similarly, after an assessment has been started, you can close the Vivinet Assessor Console and the assessment will still run under the Scheduler service. Thus you can close and reopen a running assessment.

For more information, see Section 11.3, “Scheduler Errors,” on page 122.

2.2.5 Uninstalling Vivinet Assessor

When you install a later version of Vivinet Assessor over an earlier version, the setup wizard automatically uninstalls the earlier version after a prompt. If you attempt to reinstall the same version of Vivinet Assessor over an existing copy, the setup wizard helps you perform an upgrade or repair installation.

During the uninstallation process, the following files are removed or remain in place:

- Most Assessor files are removed except files that you created, or edited and renamed, such as assessment database files. The folders containing these files are also preserved.
- The `VAssessor` named instance of a SQL Server *is not* removed when you uninstall Vivinet Assessor. Use the **Add/Remove Programs > Microsoft SQL Server** Control Panel option to remove the `VAssessor` named instance.
- All System Registry entries are removed when uninstalling.
- User Registry entries are not removed. To remove User Registry entries created by the Console and Scheduler components, open `REGEDIT`, highlight the key `HKEY_CURRENT_USER\Software\NetIQ\Vivinet Assessor`, and click **Delete**. All Registry entries are removed.

To uninstall Vivinet Assessor:

1. Navigate to the Control Panel and double-click **Programs and Features**.
2. Select **Micro Focus Vivinet Assessor** and click **Add/Remove**.
3. In the Confirm File Deletion dialog box, click **Yes**.
4. When the uninstallation is complete, click **OK**, and then click **OK** again.

2.3 Registering Vivinet Assessor

Vivinet Assessor runs in Demo mode until you register. Demo mode provides only limited functionality and does not allow you to run an assessment. For more information, see Section 2.3.1, “Reviewing Demo Mode,” on page 24.

To register the software, click **Registration** on the Options menu. For more information, see Section 2.3.2, “Registering using a License Key,” on page 24.

The **Register** button is disabled if multiple assessment windows are active.

Click **Help** in the Registration dialog box for context-sensitive Help.

2.3.1 Reviewing Demo Mode

Register Vivinet Assessor by clicking **Registration** on the Options menu. For more information, see Section 2.3.2, “Registering using a License Key,” on page 24.

A sample VoIP Readiness assessment is included to help you evaluate the product. You can use this assessment to generate sample reports while you are running in Demo mode. To view it, simply open the Console. The sample is loaded automatically when you are running in Demo mode. You cannot run or verify the sample assessment in Demo mode, but you can examine the Design and generate either the Executive Summary or the Complete report. For more information, see Chapter 12, “Working with the Sample Assessment,” on page 127.

2.3.2 Registering using a License Key

You need an authorization key to register Vivinet Assessor 4.0. The authorization key has a validity time. Therefore, you should obtain the appropriate authorization key from the NetIQ Sales representative or the NetIQ Customer Center. For more information, see Section 11.6, “Getting Technical Support,” on page 125.

To register Vivinet Assessor:

1. From the Registration dialog box, click **Register**.
2. In the Authorization Key box, specify the authorization key.
3. Click **Next**.
4. (Optional) To print a copy of your registration, click **Print Registration Info**.
5. Click **Finish**. The Current License Information is displayed.
6. Click **OK**.

3 Task 1: Performing a Network Inventory

The first step in a VoIP Readiness Assessment is determining the current state of the network. To that end, Vivinet Assessor can discover devices and links on your network to create a detailed report of its current configuration.

The Network Inventory starts with setting up *network discovery scanning*. After you select a location (a default gateway router, a subnet, or a series of subnets) where network devices can be found, Vivinet Assessor scans that location, sending out SNMP queries to all devices within the IP address ranges it finds. From the responses, it receives information from device Management Information Bases (MIBs) and enters it in the database for the current VoIP Readiness Assessment.

NOTE: Until you complete the “Inventory Network” task, you cannot run the “Assess Configuration,” “Assess Utilization,” or “Model Bandwidth” tasks

---

3.1 Setting Up a Network Inventory

Use the Set Up view to set the time when network discovery will begin and to select which network devices will be included in discovery scans. To access the Set Up view, expand the **Network Inventory** view tab and click the **Set Up** view tab.

Complete the fields in the Set Up view as described below:

Field	Description
Start discovery immediately upon activation	Tells the Vivinet Assessor Scheduler service to begin discovering devices on your network as soon as you click **Activate Discovery** in the Discover view
After activation, wait until [time of day] before starting discovery	Tells the Scheduler service to begin the process of discovering devices on your network at the specific time of day you entered. To notify the Scheduler, click **Activate Discovery** in the Discover view as soon as you complete the necessary setup tasks in the Set Up view.
SNMP Configuration	Simple Network Management Protocol (SNMP) permissions allow Vivinet Assessor to collect information from SNMP-enabled devices. Until you enter SNMP information into the database, Vivinet Assessor uses the default SNMP community string, `public`, which is probably not the correct one for your network. The type of information you configure varies according to the version of SNMP that is implemented on the network device. Vivinet Assessor supports SNMP versions 1, 2, and 3. The message `"SNMP values are currently set to their defaults"` indicates that you have not entered the SNMP information in use on your network. The Network Inventory probably cannot be performed if you do not enter at least one community string for versions 1 and 2, or security profiles for version 3.
Edit SNMP Configuration	Lets you enter your SNMP information to enable Network Inventory discovery scanning. For more information, see Section 3.1.1, “Editing SNMP Configuration Information,” on page 26.

Field	Description
Use a default gateway	Enables Vivinet Assessor to query the gateway router whose address you specify to discover network devices and links from the gateway's routing tables. This type of discovery is the default method for Vivinet Assessor. For more information, see Section 3.1.3, "Using a Default Gateway," on page 29.
Use specific addresses	Enables Vivinet Assessor to discover network devices and links by performing SNMP discovery scans within an IP network address range you specify. For more information, see Section 3.1.4, "Using Specific Addresses for Discovery," on page 30.
Discover Ethernet links	Tells Vivinet Assessor to include Ethernet LAN links (such as switches with Ethernet cables attached) on your network in discovery scanning. Discovered LAN links appear in the Network Inventory as Ethernet links and can be monitored for utilization and used for Bandwidth Modeling. Some networks contain hundreds of Ethernet links that could potentially be discovered and included in the Network Inventory. If you enable this option, you could quickly exceed the maximum number of database objects your Vivinet Assessor license allows (1000 routers, switches, and links). This limit reflects the maximum number of objects that can be efficiently managed by the Vivinet Assessor database. If you are using a default gateway for discovery, you should leave this option disabled to avoid discovering too many Ethernet links. However, if you want to discover Ethernet links, specify the address ranges you want to discover and then filter the network interface ports to which Ethernet links are connected for the devices in those ranges. For more information, see Section 3.1.4, "Using Specific Addresses for Discovery," on page 30.

3.1.1 Editing SNMP Configuration Information

Vivinet Assessor uses SNMP (Simple Network Management Protocol) to gather important information about VoIP data patterns and performance from your network hardware, including routers and VoIP gateways. You configure SNMP permissions which allows Vivinet Assessor collect information from SNMP-enabled devices.

Enter SNMP information before running a discovery scan for the Network Inventory. Until you enter your information, Vivinet Assessor attempts to use only the SNMP default community string, "public," to query your network devices. However, because the default string is not secure and therefore probably not in use on your network, or because you may have SNMP v3 in use in your environment, the discovery scan will fail unless you configure the proper SNMP information.

The information you configure varies according to the version of SNMP that is implemented on the network device. Vivinet Assessor supports SNMP versions 1, 2, and 3.

Use the Edit SNMP Configuration dialog box to add, edit, and delete SNMP information, and to set SNMP timeout and maximum retries.

Configuration for SNMP Versions 1 and 2

To add configuration information for SNMP v1 and v2:

1. Click **Edit SNMP Configuration** in the **Set Up** view.
2. On the SNMP v1/v2 tab, click **Add**.

3 In the Add Community String dialog box, type the community string in use on your network and click **OK**.

   The SNMP community string acts as a password to yield access to the Management Information Base (MIB) of each VoIP device on your network. You should add each valid community string on your network to the list. Strings are limited to 63 characters.

   Read-only community strings are adequate; Vivinet Assessor does not need write access to SNMP devices. SNMP community strings are case-sensitive.

4 Repeat step 3 for each community string in use on your network. Vivinet Assessor will try each one you enter in turn.

5 To set timeout, click the **Options** tab.

   - In the **SNMP timeout** field, indicate the maximum amount of time (in milliseconds) the Vivinet Assessor Console will wait to receive a response to an SNMP query before sending a new query. Values must be from 500-5000, inclusive. The default is 2000.
   - In the **SNMP maximum retries** field, indicate the maximum number of times the Vivinet Assessor Console will try to reach a device that does not respond to an initial SNMP query. Values must be 0-5, inclusive. The default is 2.

   NOTE: The values for timeout and maximum retries actually apply to the Utilization assessment, which uses the same SNMP information for utilization monitoring. Vivinet Assessor will not keep trying a community string again and again during Network Inventory discovery scans. Instead, it will assume that no devices are present.

   ---

6 Click **OK**. The community string is displayed on the **SNMP v1/v2** tab.

Configuration for SNMP Version 3

Vivinet Assessor supports the following security modes for SNMP v3:

- No authentication; no privacy
- Authentication; no privacy
- Authentication and privacy

In addition, Vivinet Assessor supports two authentication protocols for SNMP v3:

- MD5 (Message-Digest algorithm 5)
- SHA (Secure Hash Algorithm)

and one privacy encryption protocol: DES (Data Encryption Standard).

Your SNMP v3 implementation may support one or more combinations of mode and protocol. That combination dictates the type of information you configure in Vivinet Assessor: user name (or entity), context name, protocol name, and protocol passwords.

Configure SNMP v3 information for each device that you want to include in the Network Inventory.

To add configuration information for SNMP v3:

1 Click **Edit SNMP Configuration** in the **Set Up** view.

2 On the SNMP v3 tab, click **Add**.

   - Select whether you will configure SNMP information for an **IP Address or Range** or a **Hostname**.

- If you select **IP Address or Range**: In the **From** field, type the first IP address in the range. In the **To** field, type the last IP address in the range. To configure one IP address, type the same IP address or hostname in both fields.
- If you select **Hostname**, type the hostname in the field to the right. Enter a fully qualified domain name (FQDN) rather than an IP address.
- In the **User name** field, type the SNMP user name or entity configured for the device.
- In the **Context** field, type the name of a context associated with the user name you entered in the **User name** field. A context is a collection of SNMP information that is accessible by an entity. If possible, enter a context that provides read access to all MIBs for a device.

  Leave the **Context** field blank if no context is associated with the user name.
- For *no authentication/no privacy mode*, no further entries are required.
- For *authentication/no privacy mode*, select **Use Authentication**, select `md5` or `sha` in the **Protocol** field, and then type the associated password in the **Password** field.
- Select **Use Encryption** and type the DES password in the **Password** field.
- Click **OK**. The SNMP configuration information is displayed on the **SNMP v3** tab.

3 Repeat step 2 for each set of SNMPv3 information you need to configure.

4 To set timeout, click the **Options** tab.

- In the **SNMP timeout** field, indicate the maximum amount of time (in milliseconds) the Vivinet Assessor Console will wait to receive a response to an SNMP query before sending a new query. Values must be from 500-5000 ms, inclusive. The default is 2000 ms.
- In the **SNMP maximum retries** field, indicate the maximum number of times the Vivinet Assessor Console will try to reach a device that does not respond to an initial SNMP query. Values must be 0-5, inclusive. The default is 2 retries.

NOTE: The values for timeout and maximum retries actually apply to the Utilization assessment, which uses the same SNMP information for utilization monitoring. Vivinet Assessor will not keep trying SNMP information again during Network Inventory discovery scans. Instead, it will assume that no devices are present.

---

5 Click **OK**.

NOTE: You may notice a temporary spike in processor usage when discovering or monitoring network devices using SNMP v3. SNMP v3 requires additional overhead for authentication or encryption of query requests sent to the SNMP agent on the devices.

3.1.2 Setting Network Discovery Performance

You can complete the Network Inventory more quickly if you set a network discovery performance option before you activate discovery scanning. The Inventory Network task proceeds when Vivinet Assessor sends out a series of SNMP queries or performs a series of tasks, depending on whether you entered a range of IP network addresses or a default gateway router to be used in network

discovery. The Vivinet Assessor Console can break subnets into separate sets of addresses and query them all simultaneously, or it can perform multiple discovery tasks at once. However, in each case, more bandwidth will be taken up with discovery traffic.

Therefore, you can request better performance from Vivinet Assessor network discovery, based on the bandwidth and other resources available on the network to be scanned. The performance option is also recommended in cases where discovery has failed to find any devices that are known to be on the network. In such a case, a slower link may be dropping the SNMP packets used to find devices, and slowing the rate of discovery will solve the problem.

As a rule, the faster discovery is completed, the more bandwidth it requires. However, performance also depends on the available resources on the Console computer (including NIC, memory, and CPU), as well as the speeds, current utilization levels, and maximum allowable utilization levels of all the links and devices in the paths to discovered devices.

To set discovery performance:

1. On the Options menu, click **Performance**.
2. To increase the speed of discovery, move the slider to the right.
3. To decrease the speed of discovery, move the slider to the left.
4. Click **OK**.

TIP: As discovery proceeds, check the Error Log. You set the speed too high if you see any SNMP timeout errors. You should lower the speed if any device known to be active on the network is not discovered.

3.1.3 Using a Default Gateway

If you are not certain of all relevant subnets that should be scanned during Network Inventory discovery scanning, you can instruct Vivinet Assessor to perform device and link discovery based on a “seed” or default gateway (a router) whose IP network address is known. Vivinet Assessor will query the gateway for its routing tables and then attempt to discover every device from the addresses in the tables.

By default, Vivinet Assessor uses the “Use a default gateway” method of discovery. Because using a default gateway requires Vivinet Assessor to learn about the network from scratch and scan many subnets, Network Inventory discovery scanning goes much more quickly if you instead enter specific ranges of IP network addresses in the Set Up view. For more information, see Section 3.1.4, “Using Specific Addresses for Discovery,” on page 30.

To identify a default gateway:

1. Select **Use a default gateway**.
2. In the **Default gateway** field, type the IP network address of the gateway (router) to query during discovery.
3. Use the **Max hops** field to limit the scope of discovery to a certain number of router hops. Values must be 1-20, inclusive.

   NOTE: Discovery considers the gateway router itself to be the first hop. Therefore, a **Max hops** setting of 1 means you will discover only the networks directly connected to the gateway router, and no other routers.

   ---

4. Click **Verify** to run a quick query on the default gateway to ensure that Vivinet Assessor can communicate with the gateway.

If you select **Use a default gateway**, you can exclude certain IP network address ranges from discovery scanning.

To exclude IP address ranges from network discovery:

1. Click **Add**.
2. In the **From** field, type the first IP address in the range that you want to exclude from discovery.
3. In the **To** field, type the last IP address in the range that you want to exclude from discovery.
   - Enter IP addresses in dotted notation, such as 123.45.67.89. Valid address ranges span from 1.0.0.0 to 223.255.255.255. Values higher than 223 in the first octet are reserved for IP Multicast.
   - The value you enter in the **To** field must be greater than the value you enter in the **From** field.
4. To exclude a single address, leave the **From** field blank and enter the single address in the **To** field.
5. Select **Exclude this range from network discovery**. If you perform a subsequent discovery scan, you can include this range by clearing this box.
6. Click **OK**. The range is displayed in the **Excluded Range** list.

3.1.4 Using Specific Addresses for Discovery

If you know the range of IP network addresses or Ethernet network interface ports where device and link discovery should take place, you can specify the ranges in the Add to List of Discovery Ranges dialog box. Vivinet Assessor discovers network devices and links within the ranges you specify.

The IP address range you enter here may also be used later for endpoint discovery as part of the VoIP Quality assessment. For more information, see Section 7.3, “Discovering,” on page 57.

To use specific addresses for discovery:

1. Expand the **Network Inventory** view tab and click the **Set Up** tab.
2. In the Discovery Type section, click **Use specific addresses**.
3. Click **Add**.
4. In the **From** field, type the first IP address in the range that you want to include in discovery.
5. In the **To** field, type the last IP address in the range that you want to include in discovery.
   - Enter IP addresses in dotted notation, such as 123.45.67.89. Valid address ranges span from 1.0.0.0 to 223.255.255.255. Values higher than 223 in the first octet are reserved for IP Multicast.
   - The value you enter in the **To** field must be greater than the value you enter in the **From** field.
6. To include a single address, leave the **From** field blank and enter the single address in the **To** field.
7. Select **Use this range in discovery** if you want discovery scans to look for switches, routers, and links in this range of addresses. If you perform a subsequent discovery scan, you can exclude this range by clearing this box.
8. Use the fields in the Ethernet Links panel to limit the number of Ethernet links that are discovered. Type a range of Ethernet network interface port numbers that you want to discover within the IP address range you specified in the Address Range panel.

   In the first field, type the first port number in the range. In the second field, type the last port

number in the range.

These fields are available only if you checked **Discover Ethernet links** on the **Set Up** tab. For more information, see Section 3.1, “Setting Up a Network Inventory,” on page 25.

9 Click **OK**. The IP address range is displayed in the Range column and the port range is displayed in the Port Range for Ethernet Links column.

3.2 Discovering Network Devices and Links

After you have finished setting up your Network Inventory, you can begin the discovery process. For more information, see Section 3.1, “Setting Up a Network Inventory,” on page 25.

Use the Discover view to initiate discovery and review discovery results. To access the Discover view, expand the **Network Inventory** view tab and click the **Discover** view tab.

To initiate your Network Inventory, click **Activate Discovery**. If you scheduled network discovery to start immediately upon activation, Vivinet Assessor immediately begins sending out SNMP queries within the IP network address range you specified. Or, if you decided to start discovery at a specific time of day after activation, Vivinet Assessor notifies the Scheduler to begin discovery at the time you entered in the Set Up view.

Results from discovery scanning appear on the Discover view and are updated in real time:

Field	Description
Summary of latest discover	The current status of discovery.
Status	The current state of discovery scanning. Once discovery is complete, the Status reads, “Discovery complete.”
Start Time	The time discovery scanning became active.
End Time	The time discovery scanning ended.
Number of addresses scanned / # expected	The number of network discovery scans that have been performed, out of the total number of scans scheduled to be performed. The second value is estimated from the number of addresses in the IP network address ranges you entered. If you are performing discovery based on a default gateway router, only the number of scanned addresses is available. For more information, see Section 3.1, “Setting Up a Network Inventory,” on page 25.
Number of devices and links found	The number of routers, switches, and links already discovered.
Number of errors	The number of errors that occurred during network discovery scanning.
View Error Log	Enabled if any errors occur during discovery scanning. Click to view information about the errors and get help for avoiding them next time.
Discovered Devices and Links table	Shows any switches, routers, or links that Vivinet Assessor discovers on the subnet you specified in the Set Up view. They are also entered into the database. Link information is derived from the router interfaces discovered. Information about each discovered device or link appears as soon as it is available. Click the Routers, Switches, or Links tab to see the information about each component. For more information, see Section 3.3, “Working with Discovered Routers, Switches, and Links,” on page 32.

NOTE

- More information is collected than is shown in the Discovered Devices and Links table. All collected information is shown in the assessment reports.
- Vivinet Assessor discovers all devices on the network; however, some vendors devices are not supported for Network Inventory or for Utilization monitoring. In the table and in reports, unsupported (or unavailable) devices will return no information for some fields.

After you start discovery, the **Activate Discovery** button changes to a **Stop** button so that you can stop discovery scanning at any time.

3.3 Working with Discovered Routers, Switches, and Links

Once network devices and links have been discovered and added to the assessment database, you can add and update information to help you identify them in VoIP Readiness Assessment reports.

In the Discover view of the Inventory Network task, the routers, switches, or links discovered during network discovery scans appear in the Discovered Devices and Links table.

You can change the name of the device, add a comment, and change a link's data rate.

To update discovered device information:

1. Select the **Routers**, **Switches**, or **Links** tab, as appropriate.
2. Select the row that describes the device or link you want to edit and click **Edit**.
3. In the **Name** field, assign a name to the router, switch, or link. The name you supply replaces any name that already is displayed in the Discovered Devices and Links table and will be used in any reports. Names are particularly useful for identifying the links that are discovered. Maximum length is 256 characters.
4. In the **Comment** field, type a text string to further identify this router, switch, or link. The comment you supply here is displayed in reports and in the Discovered Devices and Links table. Maximum length is 256 characters.
5. In the **Speed** field (for the Edit Links only), specify the data rate at which the link is currently operating. You can configure routers to reduce the data rate of a particular link—for example, by setting a maximum speed of 64 kbps on a serial link or ATM PVC that could actually carry 1.5 Mbps. In such a case, the rate Vivinet Assessor would find from polling the routers would be the link's actual capacity: 1.5 Mbps. If actual utilization on such a link were about 56 kbps, or 87% of the rate being allowed, Vivinet Assessor would calculate that link utilization was only about 3.6%. Set the operating speed (in this example, you would enter 64 kbps) to get accurate utilization measurements.

   NOTE

   - Set the speed for links before starting utilization monitoring.
   - Frame-relay links are handled slightly differently than serial or ATM links. Vivinet Assessor can get a frame-relay link's committed information rate (CIR) from the routers and thus calculate the link's utilization based on the CIR.

6. Click **OK**.
7. To delete a device from the table, highlight the device and click **Delete**.

3.4 Best Practices for the Network Inventory

The Network Inventory provides useful information about the equipment currently installed on your network. In addition to discovering switches and routers when they respond to SNMP queries, Vivinet Assessor uses network device interfaces to determine where your WAN and LAN links are located--important information for troubleshooting future VoIP performance problems caused by link failure or over-subscription.

However, the chief object of the Network Inventory is to populate the Vivinet Assessor database with information about your devices and links, information that is required to perform the Configuration and Utilization assessments.

As a secondary goal, the Network Inventory compiles a list of equipment that will be called upon to handle voice over IP traffic and to identify critical links where that traffic could encounter bottlenecks. If no one has kept careful records each time a new device was added or an operating system upgrade installed, you will now be able to improve your record keeping with the information Vivinet Assessor reports.

Before you start running assessments, you need to know several things about your present or planned VoIP network configuration. First of all, you will save a great deal of time during the Network Inventory if you already know the IP address ranges of the subnets where your network devices are installed. If you try to scan too large a range of subnets, the inventory can take a very long time to complete.

You can change the performance options for the Network Inventory to speed things up. But the faster Vivinet Assessor performs device and link discovery, the more network bandwidth is required. For more information, see Section 3.1.2, “Setting Network Discovery Performance,” on page 28.

Do not forget to check the setting for “Max hops” if you decide to perform discovery based on a default gateway router. This setting limits the number of router hops that Vivinet Assessor will query to find network devices and links. For more information, see Section 3.1.3, “Using a Default Gateway,” on page 29.

Also, consider the following tips before and after you perform the inventory:

- Particularly in the weeks before you roll out a VoIP implementation, you need to know precisely what is installed on your network. For each router and switch, it is helpful to know the manufacturer, in case you need to direct VoIP-specific questions to their support personnel, and the level of the device operating system currently running (it may need to be updated). All this information is collected during the Network Inventory.
- It is also important to know exactly where each device is physically located within your campus, building, or site. Such information can be used to construct diagrams of your network’s topology. And those diagrams will be much more helpful to you if you can include the logical identifiers—namely, IP addresses and domain names—of each device, identifiers that are discovered as part of the Inventory.
- If some devices in the Inventory show that no information about device location is available, consider configuring a physical location in the MIB for each device. Location is an important means of identification and could end up saving you a lot of time if you ever have to visit a device at its physical home.
- Take a close look at the operating system level each device reports. If you are not certain that it is the most recent version of the OS, do some checking at the manufacturer’s Web site and make the recommended updates, if necessary.

- Another useful statistic you will find in the Inventory is the Committed Information Rate, or CIR, for discovered frame-relay WAN links. The CIR for your links is an obvious place to begin considering network upgrades if you later find, during the assessment of VoIP Quality, that calls are not performing as well as you would like. The CIR is something you can negotiate with your WAN provider in such a case. Or you can reroute VoIP traffic over faster links.

  In results, the Vendor or Operating System information returned may reflect an OEM or pre-acquisition identity for certain devices. For example, some Alcatel devices may show “Xylan” as the Vendor because Xylan was the original developer of the device or its operating system.

3.5 Network Inventory Serial Numbers

Vendor implementation of device serial numbers can be somewhat unpredictable.

When devices manufactured by Cisco Systems are discovered during the Network Inventory, Vivinet Assessor queries their entity MIBs to collect information about device serial numbers. In our testing, we have found some discrepancies between what is retrieved from the entity MIB and the actual serial number imprinted on the device itself.

In addition, we have seen discrepancies between what the Cisco IOS command `show diag` returns for router serial numbers and what Vivinet Assessor gets when it queries the router MIB. For example, you might use the `show diag` command to get a device serial number and find that the number returned is different from the one that was recorded in the assessment database during the Network Inventory. Or Vivinet Assessor might return multiple serial numbers for a device, including some that are not returned by `show diag`.

4 Task 2: Assessing Configuration

After you complete the Network Inventory, Vivinet Assessor can use the information in the database to perform a Configuration assessment. Although the Configuration assessment is part of an overall assessment of VoIP readiness, you can use it to find and report on any network devices that lack certain resources—resources that are necessary for Voice over IP, for a planned network upgrade, or for any other purpose.

Assessing configuration does not require a scheduling component because it takes place on the spot and usually takes only a few minutes to complete. No testing, querying, or monitoring of devices takes place. Instead, you simply supply a rules file in XML format that summarizes the software and hardware resources that you want your switches and routers to have. Valid rules files use a set of simple operators, such as `LessThan`, `GreaterThan`, `GreaterThanEqualTo`, and `OR`, to define acceptable levels of operating systems, memory, and installed modules. When setting up the Configuration assessment, you import the rules file, and Vivinet Assessor performs a quick validation of the rules file format to make sure it conforms to a schema.

For a full discussion of the rules file format, see Section 4.1.1, “Creating a Rules File,” on page 36.

When you activate the Configuration assessment, Vivinet Assessor examines the information in the database for devices discovered during the Network Inventory. It compares the available information to the rules file. Then it clearly reports any devices that passed or failed rule criteria, along with the applicable rules you specified, on the **Run** tab of the Assess Configuration view. Results can also be included in the VoIP Readiness Assessment report.

4.1 Setting Up the Configuration Assessment

The first step in setting up a Configuration assessment is to create the rules file you want to use and save it to the Vivinet Assessor Console computer. Then, import the file so that Vivinet Assessor can validate and read it. Finally, identify any devices you do not want to include in the assessment.

To set up the configuration assessment:

1. Create a rules file. For more information, see Section 4.1.1, “Creating a Rules File,” on page 36.
2. Expand the **Assess Configuration** view and click **Set Up**.
3. Import the rules file. For more information, see Section 4.1.2, “Importing the Rules File,” on page 38.
4. If necessary, exclude selected devices from the Configuration assessment. All eligible devices from the Network Inventory are shown in the Network Inventory table. Deselect the boxes next to any devices whose configuration you do not want to check.

TIP: You can use the Set Up view to export a configuration rules file that you imported and used in a Configuration assessment. Click **Export** to export the rules to an XML file that will be saved in the `Program Files\Micro Focus\Vivinet Assessor` directory by default.

4.1.1 Creating a Rules File

Before you can assess device configuration, create a valid configuration rules file in XML format. Use the following information to create your rules file and then save it on the Vivinet Assessor Console computer.

When you import a rules file, it is immediately validated against the Vivinet Assessor rules file schema, `PropertyRuleSchema.xsd`, which is installed by default in the `Program Files\Micro Focus\Vivinet Assessor` directory. The schema is an XML definition file that defines the structure, content, and syntax of the XML rules files you can import. It is based on structures in the Vivinet Assessor SQL database so that the data you gather on network devices during the Network Inventory can be analyzed by the configuration rules you import.

If your rules file does not conform to the rule schema, or if it is not in the same directory as the schema, an error is reported when you import it. You will than have to make changes to your XML file or to its directory location and re-import it.

A valid rules file must have a header containing the XML version:

```
<?xml version="1.0" ?>
```

The header also indicates that the schema (`.xsd`) file must be in the same directory as the rules file:

```
xsi:noNamespaceSchemaLocation="PropertyRuleSchema.xsd"
```

A description tag is a recommended, but not a required, element. The text in your description tag appears in the **Rules description** field of the Run view when you run the Configuration assessment. The following is an example of a header containing the previously mentioned elements:

```
<BasicRulesElement xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance" xsi:noNamespaceSchemaLocation="PropertyRuleSchema.xsd"
  Name="SampleRules" Description="NetIQ Configuration Rules">
```

You can see a more specific example by looking at a rule from our `SampleRules.xml` file, located in the `Program Files\Micro Focus\Vivinet Assessor\Samples` directory. This particular rule looks for Cisco routers with an IOS greater than 12.0 and is a good example of how to create a rule in general. We reference it when discussing the various components of a rule. The `SampleRules.xml` is a good starting point for generating your own rules file.

```
<?xml version="1.0" encoding="utf-8" ?>
<BasicRulesElement xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="PropertyRuleSchema.xsd" Name="SampleRules"
Description="Sample Rules">
    <Rule Name="CiscoIOSRule" Description="Cisco IOS downlevel rule">
        <TopRule LogicalOperator="AND">
            <BasicRule ComparisonOperator="EqualTo">
                <!-- Look for all Cisco router devices-->
                <BasicPropertyItem FilterOn="true">
                    <Property>Vendor</Property>
                    <Type>String</Type>
                    <Unit>None</Unit>
                    <Value>Cisco</Value>
                    <DeviceType>router</DeviceType>
                </BasicPropertyItem>
            </BasicRule>
```

```
            <BasicRule ComparisonOperator="GreaterThan">
                <BasicPropertyItem>
                    <!-- Check IOS level greater than 12.0-->
                  <!-- Using Type Integer for an alphanumeric field will typically
yield better results than Type String for GreaterThan/LessThan Comparisons -->
                    <Property>OSRevision</Property>
                    <Type>Integer</Type>
                    <Unit>None</Unit>
                    <Value>12.0</Value>
                    <DeviceType>router</DeviceType>
                </BasicPropertyItem>
            </BasicRule>
        </TopRule>
    </Rule>
```

Each element defined below is a component of the rule described above.

Element	Description
Rule Name and Description	Name and Description are attributes of the Rule element. You should supply names and descriptions indicating what the rule is evaluating as a kind of shorthand for what the XML is doing. These attributes are referenced in the Run view and in the Report.
TopRule and IntermediateRule	Used to introduce a logical operator. If you plan to evaluate multiple properties in one rule, you should use a logical operator. The example above presents a rule that evaluates devices based on the `Vendor` property AND the `OSRevision` property. An IntermediateRule (not shown in the above example) is similar, but allows some flexibility in further defining what a rule evaluates. Rules are generally more effective if multiple properties are evaluated together, as, for example, when you check for a particular vendor, operating system, and installed memory with a single rule.
BasicRule	The element where you can supply the comparison operator to be used on the property you are evaluating with the basic rule construct. The example above looks for two different properties: the property `Vendor EqualTo Cisco` AND the property `OSRevision GreaterThan 12.0`. A complex rule can have several BasicRule elements.
BasicPropertyItem	A complex element comprising the next five basic elements, which define characteristics of the property being evaluated. The following are all required elements.
Property	Several properties are stored for each network device discovered during the Network Inventory. The following are basic device properties you can use a rule to evaluate: `Vendor, Model, OSRevision, InstalledModules, MemoryFlash, MemoryRAM`
Type	A data type. Determines whether the rule should look for a string value or an integer value.
Unit	Determines the units that are applied to a metric. For example, if you want all your routers to have at least 64 MB of RAM, you would supply MegaBytes for the `<Unit>` rule parameter. The following units are valid: `None, Bytes, Kilobytes, and MegaBytes`
Value	Specifies what you are looking for in a given property.

Element	Description
DeviceType	Associates a rule with a particular kind of device to generate more effective rules; expected Basic property values are usually different for different device types. The following types are available: `all, switch, router` Use `<DeviceType>all</DeviceType>` if you want a rule to be applied to both switches and routers.

Operators	*Logical* operators are used to create expressions that evaluate multiple properties in the same rule. The following are available:
	
	`AND, OR`
	
	Comparison operators are used to compare a device's basic property against a known value. The following are available:
	
	`EqualTo, NotEqualTo, LessThan, LessThanEqualTo, GreaterThan, GreaterThanEqualTo, AND, OR, Find`

Find operator	An operator that works similarly to `EqualTo`, `GreaterThan`, `LessThan`, and other operators. It locates a particular value within a property being analyzed by a rule. Useful in instances where an `EqualTo` is not really applicable. For more information, see Section 4.3.2, "Example 2: Installed Modules," on page 40.
FilterOn attribute	FilterOn is a special Property attribute of the BasicPropertyItem that can be used to query only devices with a certain value you are interested in and not create failure results when a device does not meet that criterion. Filtering out all devices except for those made by a particular vendor, for example, can focus the rule on the subset of devices you want to evaluate. For more information, see Section 4.3.3, "Example 3: Filtering Rule Properties," on page 40. The following values are available for the FilterOn attribute: `true, false`

4.1.2 Importing the Rules File

After creating the rules file, import it for use in the Configuration assessment.

To import the rules file:

1. In the **Rules file** field, type the full path to the rules file directory location. Or click the **Browse** button to navigate to the file.
2. Click **Import**.

Vivinet Assessor runs a quick check to ensure the file format is valid for the schema. Any problems are reported so that you can correct them and re-import the file.

4.2 Running the Configuration Assessment

After you create and import a valid configuration rules file, you are ready to run the Configuration assessment.

To run the Configuration assessment:

1. Click the **Run** view tab.
2. Click **Activate Assessment**. Vivinet Assessor parses the data in the database and compares it to the rules file you supplied during assessment setup.

TIP: If you are running a Configuration assessment for a second time on the same assessment database, Vivinet Assessor checks for results from the first assessment, then warns you before emptying the database of any previous Configuration assessment results. Results from other assessments and from the Network Inventory are not discarded.

As soon as the Configuration assessment is complete, results are displayed in the Results table.

A red error symbol identifies devices that have violated a rule. The rule condition that was not met is also shown, along with address information about the device so that you can easily locate it and remedy the condition.

If any errors prevent the Configuration assessment from completing successfully, the **View Error Log** button is enabled. Click the button to open the Log Viewer.

4.3 Best Practices for Assessing Configuration

The engine that drives the Configuration Assessment is a powerful tool, one that places a lot of responsibility on you. Not only do you create the configuration rules file that makes sense for your environment and your goals, but you also need to understand the following:

- how to set up a rules file that will look for certain components and return accurate results.
- how to understand and apply the results you receive.
- how to revise your rules file if the results do not match your expectations.

The topic titled Section 4.1.1, “Creating a Rules File,” on page 36 provides a basic introduction to the rules file format and explains the available parameters. The topics in the current section extend the discussion to special cases and possible pitfalls in running a Configuration assessment.

4.3.1 Example 1: OS Revision

When you create a comparison rule to check the operating system version (“`OS Revision`”) of your devices, you can set the `Type` to be either `string` or `integer`. If you select **string** for the `Type`, a straight comparison is performed on the string values in the rules file and in the database; no conversion is performed. For values that are within the same range of 10’s (for example, comparing 12.1 and 11.0), this approach works fine.

However, for values that are not within the same range of 10’s, such as a comparison of 12.1 and 8.0, this approach gives incorrect results because the comparison is based on the value of each character. When you wrote the rule, you knew that an OS version of 12.1 was greater than a version of 8.0, but when this comparison is performed, Vivinet Assessor finds that 1 is less than 8.

On the other hand, if you had set the `Type` to be **integer**, the comparison is performed on the converted value of the string (Vivinet Assessor converts each string to a double). This type of conversion throws out the text values and only returns their numeric equivalents. In this case, the comparison will work for the comparison of 12.1 and 11.0, as well as 12.1 and 8.0, and even values like 12.1(a) and 12.2(b). However, if the alphabetical portion of the revision is really important, in some cases it is better to set the `Type` to `string`.

A final option is to use the Find feature to search for an exact string of letters, characters, or numbers within a property. For example, you may need to know whether the OS version contains the string "12.3." For more information, see Section 4.3.2, "Example 2: Installed Modules," on page 40.

In the case of OS Revision, you should write the configuration rules file with some prior knowledge not only of the vendor-recommended operating-system levels for VoIP, but also of the OS versions already installed on the network. If you think some devices might have OS Revision values with letters in them, set the Type to string. Or try running the same Configuration assessment with OS Revision Type set to string, and then run it again with the Type set to integer.

4.3.2 Example 2: Installed Modules

For a few device characteristics, such as Installed Modules, the relevant information in the device MIB (and thus, in the Network Inventory for that device) is a complex string of characters and numbers. Sorting through the relevant characters can be tricky, and making a rule that compares it with a `LessThan or GreaterThan` string may be impossible.

The Installed Modules data presents an example where you need to use a `Find` operator in your rules file. (In the rules file, the Installed Modules property appears as `<Property>InstallModules</Property>`.) You may, for example, want to ensure your routers have at least two voice ports.

Here is how the Find feature works:

For Router X, the information stored in the database after the Network Inventory was performed includes the following for the installed modules property:

```
VendorX mainboard, VendorX FSO ethernet 12345, VendorX voice port ABC, mainboard
upgrade 654321
```

To check for these values, you add the property to the rule as follows:

```
<BasicRule ComparisonOperator="Find">
<BasicPropertyItem FilterOn="false">
   <Property>InstallModules</Property>
   <Type>String</Type>
   <Unit>None</Unit>
   <Value>voice port</Value>
   <DeviceType>all</DeviceType>
</BasicPropertyItem>
</BasicRule>
```

In this case, the rule searches the `InstallModules` property for the string "voice port." If the string is located, the result is true (shown as success in the Configuration assessment results); otherwise the result is `false` (the device fails the rule). For the rule shown above, the result for Router X is `true`.

4.3.3 Example 3: Filtering Rule Properties

In some cases, you might want to treat one of the properties of a configuration rule more as a rule detail than as a hard-and-fast configuration requirement. For example, if your environment contains devices from multiple vendors, you will want to include the name of Vendor A in some of your rules.

After all, your rules for those devices should be based on the system resources recommended by Vendor A. However, you will not want to see a failure in the results for every device on the network that was manufactured by Vendor B.

The Configuration assessment offers a filtering feature for just such a case. To enable it, add a `FilterOn` attribute to a `BasicPropertyItemType`. A filtering attribute allows you to exclude certain values from consideration by a single rule without returning a failure result for the rule or excluding that particular value from consideration by any other rule in the rules file.

Unless you add a `FilterOn` attribute to a property item, no filtering takes place. The `FilterOn` attribute type is string, with possible values of "`true`" or "`false`." Any property can have this attribute, and for a given rule, multiple properties can have it set to "`true`." In the results table and VoIP Readiness Assessment Report, any filtering is indicated next to the rule where filtering was applied.

Here is an example of how you might use the `FilterOn` attribute. You discovered six routers by Cisco and six by Nortel during the Network Inventory, and you want to use a single configuration rules file to analyze all 12 of them. For any rule that treats Cisco IOS levels, add the filter to avoid seeing failures for all six Nortel devices.

5 Task 3: Assessing Network Utilization

Vivinet Assessor determines whether your network is VoIP-ready by gathering and assessing utilization statistics for the devices and links on your network. Before you try to assess utilization, you must first perform a Network Inventory to ensure that the devices and links to be queried are already in the database when you commence utilization monitoring. For more information, see Chapter 3, “Task 1: Performing a Network Inventory,” on page 25.

Vivinet Assessor cannot monitor every conceivable router or switch on a given network. The following table summarizes the supported devices:

Vendor	Device	Notes
Switches		
Alcatel	◆ OmniSwitch (6600, 7000, and 8800 series) ◆ OmniStack (6100 series)	
Cisco	All known switches are supported.	
Extreme	Any switch that supports ExtremeWare v6.1.x and later	
Nortel	Baystack 460 series and later	Those with OS version 3.1 lack utilization MIBs; thus, they are not supported.
Routers		
Alcatel	◆ Omni Switch/Router series ◆ OmniAccess (408 and 512)	
Cisco	All known routers are supported.	
Nortel	◆ Access Stack Note (ASN) Series ◆ Backbone Concentrator Node (BCN) Series ◆ Backbone Link Note (BLN) Series ◆ Backbone Node (BN) Series ◆ Passport Series (including 8600 product line and 8300-series switches acting as routers) ◆ Passport Advanced Remote Node (ARN) Series	BayRS version 14.x and 15.x. Other OS versions are also supported, but not all metrics can be collected.

5.1 Setting Up the Utilization Assessment

The main task to complete when setting up utilization monitoring is selecting the time frame when monitoring will take place. To obtain the most accurate, most helpful statistics illustrating utilization on your network, perform the Utilization assessment over a seven-day period.

To set up the Utilization assessment:

1. Ensure the result ranges for Utilization monitoring are appropriate for your network. For more information, see Section 5.2, “Determining Assessment Result Ranges,” on page 44.
2. Expand the **Assess Utilization** view tab and click the **Set Up** tab.
3. Complete the fields in the Set Up view as follows:

Section	Description
Start Time	The time you want Vivinet Assessor to begin monitoring device and link utilization on your network. Choose from the following options: ◆ **Start monitoring immediately upon activation**. Monitoring commences as soon as you activate the assessment from the Monitor view. For more information, see Section 7.7, “Running a VoIP Quality Assessment,” on page 66. ◆ **After activation, wait until [time of day] before starting to monitor**. The Scheduler service will initiate the monitoring of devices on your network at the specific time of day you entered. The Scheduler is notified as soon as you activate the assessment from the Monitor view. For more information, see Section 2.2.4, “Vivinet Assessor Scheduler Service,” on page 22.
Scheduling Options	The number of days and/or hours that Vivinet Assessor will monitor device and link utilization on your network. Valid time frames are 0 days, 1 hour to 7 days, 0 hours.
Interval	Determines the amount of time between device and link queries. Values must be 5 minutes to 60 minutes, inclusive.

4. Click **Validate Schedule** to ensure that Vivinet Assessor can proceed with utilization monitoring using your selected configuration. Validation checks to make sure that the monitoring schedule settings are correct.
5. If necessary, click **Undo Changes** to return all settings in the Set Up view to the previously saved values.

5.2 Determining Assessment Result Ranges

Result ranges for utilization monitoring let you set network- or enterprise-specific standards for utilization levels to determine what is rated “Good,” “Acceptable,” or “Poor” utilization in the final VoIP Readiness Assessment report. Defaults for these ranges have been selected according to IP telephony industry standards, and they differ for each measurement and for each device type. If you are monitoring routers, for example, you can configure result ranges for router-specific metrics, including memory and CPU utilization and buffer errors.

NOTE: You can change result ranges at any time. If you change them during utilization monitoring, the changes should be reflected in the Monitored Devices and Links table.

5.2.1 Changing Result Ranges

As a general rule, run Utilization assessments using the Vivinet Assessor default settings for result ranges. However, some default metrics may not be realistic for the network you are assessing. For example, you may have an overtaxed WAN link through which little VoIP traffic will have to flow. In such a case, you would adjust the average and peak utilization result ranges to higher values.

To increase the average and peak utilization result ranges:

1. Click the **Assess Utilization** view tab.
2. On the Options menu, click **Result Ranges**.
3. Click the **Links** tab.
4. In the **Measurements** list, select **Average Bandwidth Utilization**.
5. Change the **Good: Less than or equal to 30%** metric to a higher percentage, such as 50%.
6. If needed, take the same steps to raise the **Acceptable** metric.

By increasing the average and peak utilization result ranges, the WAN links on this network will be less likely to receive “Poor” readiness ratings in the VoIP Readiness Assessment reports.

For your assessment, adjust the measurement ranges on the **Routers** and **Switches** tabs, as well.

5.2.2 Setting Readiness Ratings

You can also determine how overall network device or link *readiness* ratings are assigned in a VoIP Readiness Assessment Report. Based on measurements taken during the Utilization assessment, these readiness ratings are determined by the percentage of all measurements taken that fell into each ratings category. For example, you may decide that a router’s VoIP readiness will be considered “Good” only if 95% of all its Utilization measurements fall into the “Good” result ranges you set. Therefore, you would set the result range as follows:

To set the “Good” link readiness rating:

1. In the Result Ranges dialog box, click the **Device/Link Readiness** tab.
2. In the **% Good** field, type 95 to indicate that “At least 95%” of all router measurements must fall into the “Good” range for the device itself to be rated “Good.”
3. Click **OK**.

Vivinet Assessor derives the default result range settings from widely accepted industry practices. For example, it is generally agreed that when average link utilization rises above 50%, VoIP quality is very likely to be poor, due to peak usage spikes. Readiness ratings are based on the result ranges that you configure for Device and Link Readiness.

For more information, see Section 8.6, “Reviewing Utilization Assessment Factors,” on page 103 and Section 8.4.2, “Readiness Ratings,” on page 95.

5.2.3 Restoring Default Ranges

You can, at any time, restore the default results ranges for a switch, a link, or a router.

To restore the Vivinet Assessor default settings for an individual measurement:

1. Click the **Assess Utilization** view tab.
2. On the Options menu, click **Result Ranges**.

3 Click the **Switches** tab (or the **Routers** tab or the **Links** tab).

4 Select the measurement in the list, and then click **Restore Defaults for This Measurement**.

5.3 Verifying the Utilization Assessment

After you set up your Utilization assessment, you must verify the configuration you have selected.

To verify the Utilization assessment:

1 Expand the **Assess Utilization** view tab and click the **Verify** tab.

2 Click **Start Verification**. Utilization assessment verification makes a series of quick SNMP queries to the subnets or gateways you specified on the **Inventory Network > Set Up** view tab. Results are displayed in pie charts and a table.

Any problems are reflected on the **Verify** tab as “Unavailable” (shown in black on pie charts). If you have not, for example, configured a valid SNMP community string for the network devices to be monitored, you will see “Unavailable” monitoring results. For more information, see Section 3.1.1, “Editing SNMP Configuration Information,” on page 26.

NOTE: You may also see “Unavailable” in the preliminary results if the devices you are trying to monitor lack some or all of the supported MIBs.

Utilization assessment verification shows preliminary utilization results in the form of pie charts. The charts assign VoIP readiness ratings to all the device and link measurements taken during verification. VoIP readiness ratings are derived from the result ranges configured for the Utilization assessment. The ratings categories, “Good,” “Acceptable,” and “Poor,” are explained in Section 8.4.2, “Readiness Ratings,” on page 95. For more information about setting Utilization result ranges, see Section 5.2, “Determining Assessment Result Ranges,” on page 44.

If any errors occur during verification, the **View Error Log** button is enabled. Click it to view information about the errors and get help for avoiding them in the future.

5.4 Activating the Utilization Assessment

After you set up and verify the Utilization assessment, you are ready to activate monitoring for devices and links. For more information, see Section 5.1, “Setting Up the Utilization Assessment,” on page 44 and Section 5.3, “Verifying the Utilization Assessment,” on page 46.

To activate the Utilization assessment:

1 Expand the **Assess Utilization** view tab and click the **Monitor** tab.

2 Click **Activate Assessment**. Depending on the schedule you entered and validated, activation either starts utilization monitoring immediately or notifies the Scheduler service to wait until the time you selected to start the monitoring process. The **Start time** and **End time** fields indicate the scheduled times that monitoring will begin and end.

The **Status** field indicates whether monitoring is ready to proceed, is proceeding normally, or is complete.

NOTE: You can run utilization monitoring and an assessment of VoIP Quality at the same time. However, you must complete all configuration of each assessment type before you start either one. When either assessment is active, no configuration options are available. For more information, see Chapter 7, “Task 5: Assessing VoIP Quality,” on page 55.

If any errors occur during utilization monitoring, the **View Error Log** button is enabled. Click it to view information about the errors and get help for avoiding them in the future.

Once utilization monitoring begins, rotating green arrows indicate “running,” and the progress bar indicates the percentage of the monitoring schedule that has been completed. Meanwhile, preliminary monitoring statistics are shown in the pie charts and in the Monitored Devices and Links table. Click each of the three tabs on the table to view information about **Routers**, **Switches**, and **Links**.

NOTE: Devices manufactured by Alcatel, Cisco Systems, Extreme Networks, and Nortel Networks can be monitored for utilization statistics. The table will show “Not Supported” for any routers and switches that cannot be monitored.

For more information, see Section 8.6, “Reviewing Utilization Assessment Factors,” on page 103.

The pie charts display preliminary measurement summaries for each device type (that is, routers, switches, and links). The measurements are placed into the Good, Acceptable, Poor, and Unavailable categories configured in the Utilization result ranges.

You can toggle the display for the pie charts and table:

- Click **View summary of most recent queries** to show utilization statistics for the most recent network queries only.
- Click **View summary of all queries** to show utilization statistics for all network queries performed so far during monitoring.

5.5 Best Practices for Assessing Network Utilization

An assessment of network utilization statistics is included in the VoIP Readiness Assessment for one basic reason: your voice over IP traffic will have to share device CPU time and network bandwidth with all your other application traffic. Monitoring network utilization is important for two main reasons:

- The chances are extremely good that your enterprise will exhaust all of its existing bandwidth—and probably sooner rather than later. Even without additional users, there will be new, bandwidth-hungry applications running on your network in the coming months.
- Different types of network traffic not only use widely varying amounts of bandwidth, but they use it in different ways.

For example, when a network user in the CEO’s office downloads an Internet radio broadcast of a baseball game, the traffic flows over the wires in a steady stream and demands a constant amount of bandwidth for several hours; otherwise, the audio would be choppy and difficult to decipher. By contrast, when this same user downloads an `.mp3` file or a large PowerPoint presentation, the traffic grabs a great deal of the available bandwidth for a fairly short period of time. So if this user tries to simultaneously perform both tasks, their differing requirements may clash: the amount of available bandwidth may affect the speed of the download or the quality of the audio stream.

When different types of network traffic compete for bandwidth, VoIP traffic is seldom the victor. The RTP protocol it uses does not resend packets that are lost by the receiver, so lost data may mean a lost syllable. And VoIP traffic is extremely delay-sensitive; your conversation will sound like you are

using a walkie-talkie—or worse—if delay levels are too high. When a phone conversation has to compete in a router queue with the CEO's `.mp3` file, the utilization level of your router may become an issue for your VoIP implementation.

The Utilization assessment is crucial to recognizing places where upgrades will be needed to ensure the network supports high-quality VoIP calls.

One key to getting a helpful assessment of your network's VoIP readiness is correctly setting up the Utilization assessment. First, you may want to check the result ranges for utilization monitoring. These ranges set network- or enterprise-specific standards for peak and normal utilization levels and determine what's rated "Good," "Acceptable," or "Poor" utilization on this particular network. The default selections are appropriate for industry-standard VoIP implementations, but you should check to make sure they are realistic for the network you are assessing.

You can configure Utilization assessment result ranges by clicking **Result Ranges** from the Options menu in the Assess Utilization view. For more information, see Section 5.2, "Determining Assessment Result Ranges," on page 44.

- When you create a schedule for the Utilization assessment in the Set Up view, be sure your schedule will give you an accurate sense for how much of your capacity is already being consumed on a typical workday. Bandwidth Modeling can then help you calculate how much more of your capacity VoIP traffic will demand.
- Set the speed for WAN and LAN links before starting utilization monitoring by editing them in the Inventory Network Discover view. There may be a difference between a link's configured data rate and its actual capacity. With the exception of frame-relay links, Vivinet Assessor finds the link's actual capacity, which may be much higher than the configured data rate, from utilization monitoring. This disparity could skew the utilization results. For more information, see Section 3.3, "Working with Discovered Routers, Switches, and Links," on page 32.
- If you can, perform utilization monitoring on especially busy days, such as the day of the month when the Accounting Department is sending out its payroll updates. You need to know what your utilization is like at your busiest times of day and days of the week—what Cisco Systems calls "Busy Hours Traffic" or BHT—so that you can plan for adequate or, even better, excess capacity to be available if needed, at any time.

  Or run a VoIP Quality assessment while the Utilization assessment is running. The extra traffic from the simulated calls will give you an accurate indication of utilization levels when VoIP is actually deployed.

For more help in capacity planning, see Section 6.1, "Understanding Bandwidth Modeling," on page 49.

6 Task 4: Modeling Bandwidth

The Bandwidth Modeling feature helps you determine how well network links will handle the additional traffic from a VoIP implementation. Bandwidth Modeling works in conjunction with the Network Inventory and Utilization assessment, or it can function as a standalone tool to calculate the potential effects of a configuration change in your network. Bandwidth Modeling helps you:

- Model the effects of different codecs and call volumes
- Model the effects of RTP header compression and silence suppression
- Try out multiple VoIP usage scenarios

Perform a Network Inventory and a Utilization assessment before you model bandwidth. For more information, see Chapter 3, “Task 1: Performing a Network Inventory,” on page 25 and Chapter 5, “Task 3: Assessing Network Utilization,” on page 43.

After discovering devices and links and gathering utilization statistics on your network, Vivinet Assessor can use this information for Bandwidth Modeling. You then select the links you want to model from a table of discovered links whose utilization statistics are known. You cannot make these selections while Utilization monitoring is still active.

You use the **Model Bandwidth** view to model a particular WAN or LAN link.

6.1 Understanding Bandwidth Modeling

Vivinet Assessor’s Bandwidth Modeling feature acts as a bandwidth calculator to aid in capacity planning. By taking into account a particular link’s capacity and utilization, plus optional VoIP parameters to conserve bandwidth, such as the use of RTP header compression (cRTP), Vivinet Assessor determines whether that link would most likely be capable of carrying high-quality VoIP traffic.

One way to use Bandwidth Modeling is to try out different codecs, which are represented by the various Vivinet Assessor call scripts you can select. For more information, see Section 7.11.2, “Reviewing Codec Types,” on page 78. After modeling utilization scenarios with different codecs, you could then run a VoIP Quality assessment that includes call groups using each codec and compare the quality results for each codec.

Vivinet Assessor provides two ways to create models of link capacity and utilization after a VoIP implementation:

- **creating a modeled link based on a monitored link**. Once you run a Utilization assessment, you can use the links whose utilization you monitored to create modeled links. This method provides more information and an accurate link model because it uses a known link name, link type, and real utilization statistics to project bandwidth needs after VoIP traffic is added.
- **creating a generic modeled link from scratch**. A dialog box lets you fill in information to project the necessary link capacity for a VoIP usage scenario. Without utilization information, this link modeling works like a simple bandwidth calculator.

Before you proceed with Bandwidth Modeling, it is helpful to understand some of the concepts used to design this feature. The following topics provide guidance.

6.1.1 Utilization Targets

When you set up Bandwidth Modeling, you are asked to specify the target utilization for the link you selected. A good rule of thumb is to keep the target link utilization for links that will carry VoIP traffic at 75% of link capacity. However, you may adjust this utilization level lower or higher in specific cases.

Vivinet Assessor rates your link utilization according to the utilization thresholds you set, but it uses defaults of 50% (Good) and 75% (Acceptable) for the Peak Bandwidth Utilization statistic. For more information, see Section 5.2, “Determining Assessment Result Ranges,” on page 44.

In the Create Modeled Link dialog box, the default Target Utilization value is equal to 75% of the link’s capacity. For example, 48 kbps on a 64 kbps serial WAN link represents 75% utilization. You might, therefore, want to reduce the Target Utilization data rate to more closely represent average, not peak, utilization.

6.1.2 Call Volumes

When you perform Bandwidth Modeling, you can specify the anticipated number of calls to model for a link using two different units: number of simultaneous calls, and *Erlangs*.

PBX systems can typically generate reports showing call traffic using Erlangs as the units. Named after the Danish telephone engineer A.K. Erlang, the Erlang is a unit of traffic density in a telecommunications system. One Erlang is the equivalent of one call, including call attempts and holding time, in a specific channel for 3600 seconds in an hour. The 3600 seconds need not occur, and generally do not occur, in a contiguous block. An Erlang value of “1” means that the telephone line is 100% busy.

Erlangs are used to show the Busy Hours Traffic, or BHT, a term that refers to link utilization under conditions of stress. If you enter the number of calls to model in Erlangs, Vivinet Assessor also lets you model bandwidth requirements based on the blocking percentage, which refers to calls that cannot be completed. A blocking percentage of 1% indicates that 1 call in 100 is blocked because all lines are busy. This rate can be calculated using *Erlang B*, A.K. Erlang’s calculation that lets you determine any one of the following three factors if you know or can predict the other two:

- Busy Hours Traffic (BHT), or the number of hours of call traffic during the busiest hour of operation. Expressed in Erlangs.
- Blocking %, or the percentage of calls that are blocked because insufficient lines are available
- Lines, or the number of voice paths in a specified trunk group. Vivinet Assessor assumes this is the number of calls.

Based on your input in the **Erlangs** field (for BHT) and in the **Blocking %** field, which defaults to 1%, Vivinet Assessor calculates the amount of bandwidth needed: it finds the number of lines you need for your anticipated traffic on a traditional (PSTN) telephone network and then uses an algorithm to translate the number of lines into the required amount of IP network bandwidth.

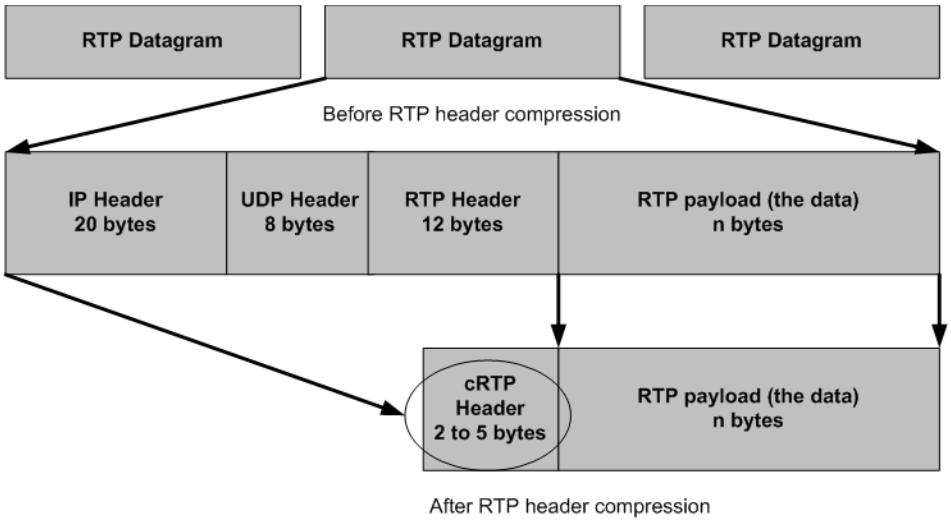
The Vivinet Assessor bandwidth calculations take two-way conversations into account, and if there is not quite enough bandwidth for a call, the call capacity on a given link is rounded down.

6.1.3 RTP Header Compression

If your preliminary results from Bandwidth Modeling indicate that you need more bandwidth, you can try a bandwidth-conservation technique. Vivinet Assessor can help you determine whether such a strategy will help you run high-quality VoIP calls over your existing equipment. One such strategy that is tailor-made for VoIP is RTP Header Compression.

RTP Header Compression, or cRTP, is a technique used by routers on WAN links to compress the VoIP packet header. Because the Realtime Transport Protocol (RTP) rides on top of UDP and IP, the header in a typical VoIP RTP packet often exceeds the payload in size. The combined size of the IP, UDP, and RTP headers, 40 bytes, adds a significant amount of overhead to VoIP transmissions. VoIP packets can therefore consume a great deal of bandwidth on lower-capacity WAN links, especially when you consider that VoIP traffic flows in both directions.

Because most of the RTP header is unnecessary and repetitive, it can be largely eliminated by routers when VoIP packets travel over a WAN. Here is an illustration:



When cRTP is activated, the combined headers are compressed to about four bytes. The bandwidth savings can allow you to put more VoIP calls on a given link. But cRTP exacts a trade-off: the compression consumes more router CPU time and adds latency to the VoIP transmission. Therefore, you should only deploy cRTP on links of 512 kbps or more.

6.2 Creating or Editing a Modeled Link

When you create a modeled link, you select modeling parameters that determine what VoIP network scenario you want to investigate. You can base your selections on the information obtained from the Utilization Assessment task.

After Utilization monitoring is complete, the **Model Bandwidth** view contains a table of all discovered links. For more information, see Section 6.1, “Understanding Bandwidth Modeling,” on page 49.

NOTE: You cannot perform link modeling while Utilization monitoring is active. Wait until Utilization monitoring is complete.

To model a discovered link:

1 Click the **Model Bandwidth** view tab.

2 In the Monitored Links table, highlight the link you want to model.

3 Click **Create Modeled Link**.

4 Complete the fields in the dialog box as follows:

Field	Description
Link name	The name of the WAN or LAN link to be modeled. Can be a link that Vivinet Assessor discovered while performing inventory on your network, or a link that you entered manually. Corresponds to the link you highlighted in the Monitored Links table. Or, if you are creating a generic link to model, enter the link name.
Link type	The type of link to be modeled, such as serial, ATM, or frame-relay. Corresponds to the link you highlighted in the Monitored Links table. Or, if you are creating a generic link to model, select the link type from the list.
Call script	Corresponds to one of the supported VoIP codecs, such as G.729. For more information, see Section 7.10, “Working with Call Scripts,” on page 74.
Compress RTP headers	Refers to a bandwidth-conversion technique: RTP header compression (cRTP). Compression can reduce the size of the RTP header, which otherwise takes 40 bytes. For more information, see Section 6.1.3, “RTP Header Compression,” on page 51.
Number of calls to model	Can be specified in Erlangs or in number of calls. If you specify Erlangs, then the corresponding number of calls appears. If you specify Erlangs you also must specify the blocking percentage, which is the percentage of calls that are blocked because not enough lines are available. An Erlang is a unit of traffic density in a telecommunications system. One Erlang is the equivalent of one call (including call attempts and hold time) in a specific channel for 3600 seconds, which need not occur in a continuous block. An Erlang value of "1" means that the telephone line is 100% busy. For more information, see Section 6.1, “Understanding Bandwidth Modeling,” on page 49.
Link speed	The absolute throughput capacity of this link, as determined during discovery scanning. Can be expressed in kbps.
Target utilization	Ideal target for bandwidth utilization. Expressed as a percentage of link capacity. For more information, see Section 6.1.2, “Call Volumes,” on page 50.

5 Click **OK**. The results of the modeling are displayed in the Modeled Links table.

For more information, see Section 6.3, “Understanding Results from Bandwidth Modeling,” on page 53.

In addition to modeling discovered links, you can run a limited set of bandwidth calculations on a link that Vivinet Assessor has not discovered and monitored. Simply click **Create Generic Modeled Link** and select the modeling parameters as described in “To model a discovered link:” on page 51. Bandwidth utilization information is *not* available for models that are not based on discovered links.

To change any model parameters and re-run the modeling scenario, highlight a link in the Modeled Links table and click **Edit**.

To remove a link, highlight a link in the Modeled Links table and click **Delete**.

6.3 Understanding Results from Bandwidth Modeling

Any modeled link that you create is displayed in the Modeled Links table in the Model Bandwidth view. The table displays not only the information that you entered in the Create a Modeled Link dialog box, but also the following information:

Result	Description
Average Utilization	The average utilization of this link, based on the monitored results. Not applicable to generic modeled links.
Added Call Bandwidth	The total bandwidth required for calls on this link after VoIP traffic is added, expressed in kbps. For more information, see Section 6.4, “Understanding VoIP Header Overhead,” on page 53.
Percent Above Target	The percentage of times that the total utilization—composed of the average utilization for a particular polling interval plus the additional call traffic—exceeded the target utilization.
Call Capacity	The number of calls that can travel on this link simultaneously, given the known utilization, target utilization, and per-call bandwidth.

For more information, see Section 6.1, “Understanding Bandwidth Modeling,” on page 49.

6.4 Understanding VoIP Header Overhead

The total required bandwidth shown in the “Added Call Bandwidth” field of the Modeled Links table is probably considerably larger than the codec would seem to need. The “Added Call Bandwidth” calculation includes not only the bandwidth the codec requires, but also any overhead associated with the protocol used (RTP), plus Layer-3 overhead (the IP and UDP headers), and the overhead associated with the network architecture. For example, a PPP link adds 56 extra bits.

Thus, when you select the G.729 codec, for example, the codec itself purports to use only 8 kbps (8,000 bits) of bandwidth. However, 320 bits of overhead must be added to each packet, as discussed in Section 6.1.3, “RTP Header Compression,” on page 51. And then, to calculate the bandwidth, you must add the header size associated with the link type. The following tables provide details:

Link Type	Header Size
PPP	56 bits
DS1	40 bits
E1	40 bits
DS3	40 bits
Prop PointToPoint Serial (Cisco HDLC)	56 bits
Serial	56 bits
Frame Relay	56 bits

For ATM links, a separate calculation must be performed to account for the requirements specific to ATM. When VoIP data travels over ATM, each packet is placed into 53-byte ATM cells, of which 48 bytes are payload data. No partial ATM cells are sent, so if a VoIP packet requires multiple ATM cells, any remaining cell space is padded with unused data. A 40-bit header is assumed for the ATM

architecture. The calculation then uses default packet sizes based on the selected codec, breaks them into the 48-byte ATM payload size, and rounds up the number of bytes based on the ATM header and the extra cells needed to transport the data, with padding.

The following is an illustration of bandwidth usage over a PPP link:

Codec	Data Rate	Total Bandwidth
G.711u, G.711a	64 kbps	82.8 kbps
G.726	32 kbps	50.8 kbps
G.729, G.729A	8 kbps	26.8 kbps
G.723.1 MPMLQ	6.3 kbps	18.7 kbps
G.723.1 ACELP	5.3 kbps	17.7 kbps

Other factors such as silence suppression and the number of packets sent per second, controlled by the “Delay between datagrams” parameter defined in Section 7.10.1, “Adding a Call Script,” on page 75, are used in these bandwidth calculations as well.

7 Task 5: Assessing VoIP Quality

The VoIP Quality Assessment task is a multi-part process that you perform from the Assess VoIP Quality view. Consult the topics in this chapter in the order listed to set up and complete a VoIP Quality Assessment.

7.1 Planning a VoIP Quality Assessment

Before you design your first assessment of VoIP Quality, research your network and your proposed VoIP implementation. First, look at existing network documentation to find peak and average usage statistics. For instance, telephone records are a good source of data about the likely call volume your network will have to handle. Then check the vendor data sheets to answer the following questions:

- What type of codec will you be using?
- Will this codec use silence suppression or packet loss concealment?
- How many simultaneous calls need to be supported?
- Can your network currently support QoS for VoIP?
- What size jitter buffer will be used?

You should emulate these factors as closely as possible when you design VoIP Quality assessments.

To configure and run a VoIP Quality assessment, take the following steps:

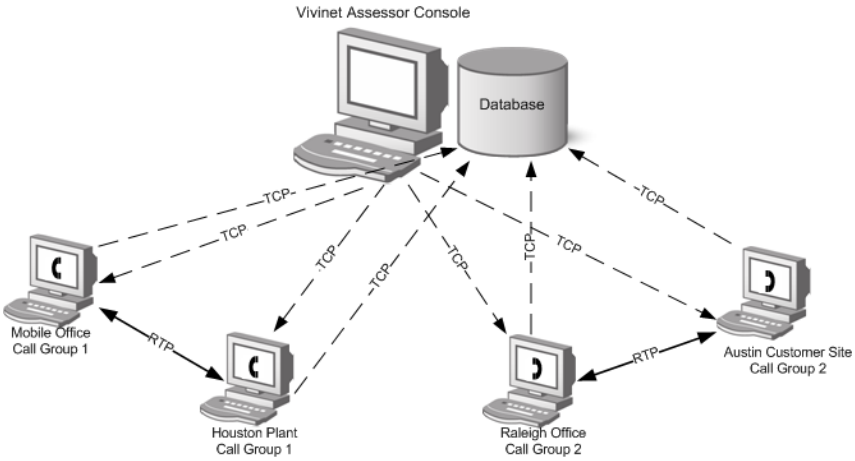
Step	Description
Step 1	**Discover** the endpoints installed in your network. You specify a range of IP addresses to scan. Endpoints that are discovered are added to the database and available in the Design view. For more information, see Section 7.3, “Discovering,” on page 57.
Step 2	**Design** the assessment schematically in the Design view. Choose the computers where the simulated voice over IP traffic will run and connect them using VoIP connectors. For more information, see Section 7.4, “Designing a VoIP Quality Assessment,” on page 58. Create endpoints to represent the different areas of your network. Create at least one call group that spans a WAN link, assuming your deployment will include one. When creating connectors, create only one connector for each call script (representing a codec type) you want to include in the assessment. To add more calls, change the “Connector Multiplier” in the Create a Connector dialog box. The multiplier corresponds to the number of simulated calls that will be sent simultaneously over the connection between the endpoints in the call group. If your network contains a firewall, you need to do some extra configuration, both in Vivinet Assessor and at the firewall itself. For more information, see Section 7.8.2, “Working with Firewalls,” on page 69.

Step	Description
Step 3	**Schedule** the assessment in the Schedule view. The scheduling parameters for a VoIP Quality assessment allow you to run a quick call-quality check by sending a single set of simulated calls over the network and measuring the resulting MOS, or to send and measure calls periodically over the course of up to a week. A typical assessment runs for about seven days, enough to get plenty of data from different days of the week when network traffic conditions are different. However, for your first assessment, run for a few hours and then scan your results. You can then reset the schedule for a longer time period if the assessment is providing meaningful results and including enough representative endpoints The schedule interval determines how heavy the simulated VoIP traffic will appear to your network equipment. To simulate heavier traffic (more frequent calls), choose a smaller interval. You should already have some idea of what peak and average utilization on your network will be; if not, do some traffic analysis to find out. For more information, see Section 7.5, “Scheduling a VoIP Quality Assessment,” on page 65.
Step 4	**Verify** that the computers you selected can be reached, and that they have Performance Endpoint software installed. Verification runs a mini-assessment to determine whether your assessment is ready to run successfully as completed. Experiment with different configurations at this stage and correct the causes of any errors you see before you run the assessment. For more information, see Section 7.6, “Verifying a VoIP Quality Assessment,” on page 65.
Step 5	**Run** the assessment. While the assessment is running, your presence is no longer required. However, you should plan to check the assessment periodically to make sure no major errors have occurred that might interfere with results. For more information, see Section 7.7, “Running a VoIP Quality Assessment,” on page 66.
Step 6	**Generate** reports. Reports contain much more useful information if you have followed the advice offered above. They are also more useful if you assign helpful endpoint names to the endpoints You will notice that by default, the reports label the results according to the call group names, which are combinations of the ’ names. Another option is to assign a Connector Comment to each connector to achieve the same purpose—identifying the call groups in reports and in charts. Names that describe the locations of the endpoints are perhaps the most helpful. For more information, see Chapter 8, “Generating Reports,” on page 91.

7.2 Understanding How VoIP Quality is Assessed

To assess VoIP quality, Vivinet Assessor sends realistic traffic across your network and measures the resulting flows. You set up an assessment of VoIP Quality by selecting the type of traffic to send, including the codec used and some other VoIP-specific parameters, and creating call groups to act as senders and recipients of this traffic. A call group consists of two endpoints connected by a VoIP

connector, which defines the type and number of calls to be sent between the endpoints on a specified schedule. The following diagram illustrates how Vivinet Assessor and the endpoints work to measure VoIP quality:



In the diagram above, endpoints that belong to call groups are designated by a telephone receiver symbol. All assessment parameters, including, for example, the codec to be emulated, are saved to an assessment within the Assessor SQL database. This database also contains any results from an assessment after it is run.

When you run an assessment, the Console contacts all the endpoints in each call group. The Console sends the endpoints a call script to use, along with the schedule configured for the assessment that is stored in the database. In the drawing above, dashed lines indicate these setup flows. The endpoints then send the information to their partner endpoints within each call group.

As the assessment runs (solid lines in the drawing), the endpoints take measurements and periodically return results to the Console, which stores them in the database (dashed lines, with arrows pointing back to the Console, indicate reporting flows in the drawing). The endpoints always report results using the connection-oriented TCP protocol so that results are not lost. Simulated VoIP traffic uses the RTP protocol.

7.3 Discovering

The VoIP Quality assessment requires you to select the locations on the network where simulated VoIP calls will run. These locations, or , are computers that have NetIQ Performance Endpoint software installed. You should install Performance Endpoints now, if you have not done so already. The endpoints are not required for the Network Inventory or Utilization Assessment or for Bandwidth Modeling. For more information, see Section 1.4, “NetIQ Performance Endpoints,” on page 12.

As a first step in setting up a VoIP Quality assessment, you can instruct Vivinet Assessor to discover all the endpoints on the network and add them to a list. Then when you design your VoIP Quality assessment in the Design view, you simply click and drag endpoints from the list onto a network diagram. The ’ network addressing information is automatically entered into the database as they are discovered.

NOTE: Perform a Network Inventory before discovering Performance Endpoints That way, endpoint discovery can use the same IP network address ranges you already configured for the Network Inventory. For more information, see Chapter 3, “Task 1: Performing a Network Inventory,” on page 25.

To discover endpoints installed on your network:

1. Expand the **Assess VoIP Quality** view tab and click the **Discover Endpoints** tab.

   The ranges of IP network addresses you entered when setting up the Network Inventory appear in the Performance Endpoint Discovery Ranges table. By default, all are selected for endpoint discovery scanning.
2. To exclude any ranges from discovery, clear the boxes in the “Use in Discovery” column.
3. To add a new range of IP network addresses, click **Add**.
4. Click **Activate Discovery**. When discovery is complete, the Summary of Latest Discovery panel provides the following information:

Field	Description
Status	The current state of endpoint discovery scanning. Once discovery is complete, the Status reads, “Discovery complete."
Start time	The time discovery scanning became active.
End time	The time discovery scanning ended.
Number of addresses scanned / # expected	How many endpoint discovery scans have been performed of the total number of scans scheduled to be performed. The second value is estimated from the number of addresses in the IP network address range(s) selected for endpoint discovery scanning.
Number of endpoints found	The number of endpoints already discovered and added to the Endpoint and Group List in the Design view.
Number of errors encountered	The number of errors that occurred during endpoint discovery scanning. Click **View Error Log** to view information about the errors and get help for avoiding them in future scans.

5. After endpoint discovery is complete, click the **Design** view tab to see the complete list of endpoints available for the VoIP Quality assessment.

7.4 Designing a VoIP Quality Assessment

To begin designing your assessment, click the **Design** view tab. The Using the Design View window provides a brief tutorial. Clear **Show this upon entering Design view** if you do not want to see the tutorial anymore. Re-invoke it anytime by clicking **Help > Using the Design View**.

The Design view offers five tools for building VoIP Quality assessments. Mouse over a tool button to view the tool name.:

Tool	Description
Selection tool	Lets you select and manipulate Design tools.
Endpoint	Creates an endpoint and places it on the network diagram. Endpoints are computers on which Performance Endpoint software is installed.
Endpoint Group	Creates a group of endpoints and places it on the network diagram. Endpoint groups let you create multiple call groups with fewer connectors.
VoIP Connector	Connects two endpoints to form a call group. Specifies the type and quantity of calls to be sent between the endpoints

Tool	Description
Background Traffic Connector	Sends TCP/IP data between two endpoints Specifies the data rate for this network traffic.

To design a VoIP Quality assessment, first use the **Endpoint** tool to add an endpoint or group to the Network Diagram. The Create an Endpoint dialog box lets you enter an IP network address to represent a VoIP-enabled computer on your network. For more information, see Section 7.4.2, “Creating an Endpoint,” on page 59.

Next, connect two endpoints or endpoint groups using the **VoIP Connector** tool. The Create a VoIP Connector dialog box lets you select key parameters for the voice traffic that will be sent between the, including the type of codec emulated and the number of simultaneous calls represented. The combination of two endpoints or endpoint groups and a VoIP connector makes a call group, the basic unit of a VoIP Quality assessment.

7.4.1 Reviewing Design Features

Vivinet Assessor offers several features that help you design and run a VoIP Quality assessment:

Feature	Description
Drag-and-drop interface	After an endpoint appears in the Endpoint and Group List, you can drag it to the diagram and drop it. This action opens the Create an Endpoint dialog box and places an icon for the endpoint on the diagram.
Disable Connector option	To exclude a call group or background traffic from an assessment without deleting the connector, click to select a VoIP or Background Traffic connector, then right-click and select **Disable Connector**. You can enable it again later.
Endpoint verification	Save time by making sure endpoints are available before trying to verify or run the VoIP Quality assessment. To verify an endpoint, select it in the Endpoint and Group list. Then right-click and select **Verify Endpoint**. A green check mark appears next to any endpoint that has been successfully verified. If the endpoint cannot be reached, a red X appears.
Endpoint Information	Once an endpoint has been successfully verified, information is available about the computer where it is installed. Click to select any verified endpoint in the Endpoint and Group list. Right-click and select **Endpoint Information**. A dialog box provides information about the operating system and memory on the endpoint computer, the version of the endpoint software, and whether any verification errors have occurred.

7.4.2 Creating an Endpoint

You use the **Endpoint** tool to add an endpoint to the Network Diagram.

To create an endpoint:

1 Drag the **Endpoint** tool to the Network Diagram.

2 Complete the fields in the dialog box as discussed below:

Field	Description
Endpoint name	The name of the endpoint computer. Can designate an actual computer on the network, or a network location.
Address type	The network addressing scheme that applies to this endpoint computer's network interface card (NIC). A single computer can be assigned multiple IP addresses for advanced assessments. Choose from **Single IP Address** or **Range of Virtual IP Addresses**. Choose **Range of Virtual IP Addresses** to create assessments with many simultaneous calls using different addresses, but with only a few computers to represent those calls. Provide the first and last IP addresses in the range in the **To** and **From** fields. If necessary, use the **Increment by** field to delineate separate subnets or classes of address within a single range.
Network address	An endpoint computer's network address, or a set of addresses assigned to that computer's NIC. Type a DNS hostname, such as `headquarters`, or the IP address of the endpoint computer in dotted notation, such as `135.25.25.5`.
Advanced	Provides more options for testing through a NAT-enabled device or using an alternative network for test setup flows.
Setup Address (optional)	The network address at which the Vivinet Assessor Console should contact an endpoint. The Console sends the endpoint setup information about the type of VoIP traffic to simulate. It can send these setup flows over a different connection from the one specified in the **Network address** field. This is the address by which Vivinet Assessor identifies the endpoint containing the virtual addresses, if any are used. You should also enter a setup address if the Console must contact an endpoint behind a NAT-enabled firewall.
Contact endpoint using setup address	Instructs the Console to use an alternative IP address to contact this endpoint. If this box is checked, you must also enter a **Setup address**. The **Network address** you entered for this endpoint will still be used for test traffic between the endpoints
Network Address Translation (NAT) Information	If an endpoint is located behind a router or firewall that performs NAT, you need to do some extra configuration to allow the VoIP Quality assessment to proceed. For more information, see Section 7.8.2, "Working with Firewalls," on page 69. Be sure to read the section titled Section 7.12.5, "Performing Assessments with NAT," on page 85 before you configure a VoIP Quality assessment through a NAT-enabled device.
Contact endpoint behind NAT device	Signals to the Console that this endpoint must be contacted at the IP address provided in the **NAT address** field.
NAT address	The endpoint IP address that is used on the public or non-secure side of a network protected by a firewall that performs network address translation.

3 Click **OK**. An icon for the new endpoint is displayed on the Network Diagram.

7.4.3 Creating an Endpoint Group

You can organize your endpoints into endpoint groups. Endpoint groups are particularly useful if you are trying to assess the performance of VoIP calls between two sites—over a WAN link, for example. With groups of , you spend less time creating endpoints and VoIP connectors if you want to emulate multiple calls. You can even add existing endpoint groups to new endpoint groups.

To create an endpoint group:

1. Drag the **Endpoint Group** tool to the Network Diagram.
2. Complete the fields in the dialog box as discussed below.

Field	Description
Endpoint group name	The name of the group of endpoints you are creating. Identifies the icon that appears on the diagram after you add endpoints to the group. Required field.
Available endpoints and groups	A list of endpoints and endpoint groups that you have already created. Highlight the endpoint or groups you want to add to the new group you are creating and click **Add**. Your selection is displayed in the **Endpoint group members** list.
Remove	Removes an endpoint or endpoint group from the endpoint group you are creating. Does not delete the endpoint from the Endpoint List.
Endpoint Quick Add	Lets you add a new endpoint to your list of endpoints It is “quick” because you do not have to open a separate Create an Endpoint dialog box. This method of creating a new endpoint does not allow you to choose a different IP address for assessment setup.
Add Endpoint	Adds the endpoint you just created using **Endpoint Quick Add** to the endpoint group you are creating.

3. Click **OK** to save the endpoints in the **Endpoint group members** list. Their group name appears in the **Available endpoints and groups** list, and a set of grouped icons is displayed on the Network Diagram.

7.4.4 Creating a VoIP Connector

By connecting two , VoIP connectors create call groups that emulate VoIP calls between endpoint computers on your network. The Create a VoIP Connector dialog box lets you select the parameters that match your VoIP application.

To create a VoIP connector:

1. Click the **VoIP Connector** tool.
2. Click an endpoint or endpoint group icon on the Network Diagram and drag the solid arrow to another endpoint or endpoint group.

3 Complete the fields in the dialog box as discussed below.

Field	Description
From Endpoint or Endpoint Group	The first endpoint in the call group. Endpoints are computers that initiate and receive bi-directional, simulated VoIP calls during the assessment. Designated as Endpoint 1 in the Call Groups--MOS Summary of Verification Calls table in the Verify view.
To Endpoint or Endpoint Group	The second endpoint in the call group. Designated as Endpoint 2 in the Call Groups—MOS Summary of Verification Calls table in the Verify view.
Call Script	The type of codec used to send VoIP datagrams, plus any additional parameters that affect the calls that are sent on the network. Choose one of the supported call scripts from the list. For more information, see Section 7.11.2, “Reviewing Codec Types,” on page 78.
View this Call Script	Click to view details about the codec selected in the **Call Script** list.
Connector multiplier	The number of times the identical connector will be represented in the assessment. This value corresponds to the number of simultaneous calls Vivinet Assessor will emulate between these endpoints Values must be between 1 and 1,250, inclusive. The default value is 1. For more information, see Section 7.1, “Planning a VoIP Quality Assessment,” on page 55.
Connector Comment (optional)	Identifies the VoIP connector on the Design diagram.
Use default comment	By default, the Connector Comment is the call script selected, plus the names of the endpoints Endpoint 1 is listed first.
Port Range (optional)	A range of ports to use for the simulated VoIP traffic sent between the endpoints Remember that RTP uses even-numbered ports. This port range will override the one you set on the **Firewall** tab of the Assessment Options dialog box. Accepted values are 1 - 65535, inclusive. The first value must be less than the second value. **NOTE:** If the Port Range you set here does not include Port 10115 (endpoint-to-endpoint configuration traffic) and Port 10116 (endpoint-to-Console results traffic), these ports will still be used, and so need to be configured at the firewall. For more information, see Section 7.8.2, “Working with Firewalls,” on page 69.

4 Click **OK**. After you create a call group, the Call Count in the lower right of the assessment window shows you how many VoIP calls will be emulated.

NOTE: Any VoIP connector you create is enabled by default. To disable a connector for a particular assessment run, select the connector on the diagram. Then click **Disable Connector** on the Edit menu.

7.4.5 Creating a Background Traffic Connector

Background Traffic connectors send TCP/IP packets between the endpoints on a particular network segment. Select the data rate to match an expected or projected level of network bandwidth utilization for that segment. The extra network traffic helps you test the effects of QoS, or it shows how VoIP quality is affected when small VoIP packets get behind larger TCP/IP packets in the network.

To create a background traffic connector:

1. Click the **Background Traffic Connector** tool.
2. Click an endpoint or endpoint group icon on the Network Diagram and drag the dashed arrow to another endpoint or endpoint group.
3. Complete the fields in the Create a Background Traffic Connector dialog box as discussed below.

Field	Description
From Endpoint or Endpoint Group	The endpoint that will send the TCP packets. Designated as Endpoint 1 in the Background Traffic -- Summary table in the Verify view.
To Endpoint or Endpoint Group	The endpoint that will receive the TCP packets. Designated as Endpoint 2 in the Background Traffic -- Summary table in the Verify view.
Connector Comment (optional)	Identifies the connector on the Design diagram.
Use default comment	By default, the Connector Comment consists of the data rate and the names of the endpoints Endpoint 1 is listed first.
Data Rate	The rate at which packets will be sent between the —the throughput to be attempted. Should match an expected or projected level of bandwidth utilization. Default is 28.8 kbps (modem).
Custom	Lets you define a custom data rate, including the number of bytes to send (the packet size), the number of times to send a packet, and an interval between SENDs (in seconds). For more information, see Section 7.4.6, “Setting a Custom Data Rate,” on page 64.
Port Range (optional)	A port or range of ports to use for the TCP traffic sent between the endpoints Accepted values are 1 - 65535, inclusive. Enter the same value in each field to specify a single port.
Initial Delay	Optional parameter. Set a value for the endpoints to wait before beginning to send background-traffic data. Select the **Type** of delay, and then indicate the **Value** for the length of the delay. For more information, see Section 7.10.2, “Setting the Initial Delay,” on page 76.

4. Click **OK**.

NOTE: Any Background Traffic connector you create is enabled by default. To disable a connector for a particular assessment run, right-click the connector on the diagram and select **Enable Connector**.

7.4.6 Setting a Custom Data Rate

The custom data rate option is particularly useful for testing VoIP QoS at slower link speeds. You determine how often the endpoints send a data packet or packets, and you set the number of packets to send and the number of bytes in each packet. When they compete with the VoIP packets, larger data packets may cause certain VoIP performance metrics to degrade each time they are sent, showing the effects of queuing in the network.

Fill in each field on the Background Traffic Connector dialog box to set a custom data rate for background network traffic. The first field determines the number of bytes to be sent in each data packet. The second field determines how many packets to send at the same time. The third field determines how often a packet is sent while simulated calls are running, or, technically, how frequently the endpoints issue a SEND command.

Background traffic runs only as long as the call duration you set in the Schedule view. For more information, see Section 7.10.2, “Setting the Initial Delay,” on page 76.

The following is an example of how you might set a custom data rate. To send two packets of 1500 bytes each every five seconds during each set of calls, you would enter the following:

Send **1472** bytes **2** times, every **5** seconds.

Headers will add a few bytes to the number of bytes you set. Thus in our example, the actual datagram size would be 1500 bytes after the addition of a

- 20-byte IP header, and an
- 8-byte UDP header.

NOTE: Background Traffic connectors normally send data using TCP. However, when you specify a custom data rate, the data is sent using UDP so that the endpoints can generate the exact packet size requested. Otherwise, TCP buffering would prevent the endpoints from sending packets of the specified size.

7.4.7 Viewing Network Diagram Objects

Vivinet Assessor includes standard Windows options for viewing and organizing the endpoints and call groups you have added to the Network Diagram. You can also control how open windows are displayed.

Tool	Description
Draw menu	Lets you change your network diagram organization.
Order	When your network diagram contains many , you can place their icons over each other by clicking and dragging. To view an endpoint or group icon that is partially obscured, first click it to select it. Then choose one of the following menu items: ◆ **Bring to Front** — Places a selected icon in front of another icon. ◆ **Send to Back** — Places a selected icon behind another icon.
Zoom In or Out	Gives a closer or broader view of the network diagram objects. Correspond to “**+**” and “**-**” buttons on the Design toolbar.
View menu	Lets you switch between views. Each view provides access to different menus and functionality as you design and run an assessment.

7.5 Scheduling a VoIP Quality Assessment

To determine when the assessment will run, click the **Schedule** view tab.

Throughout a VoIP Readiness Assessment, Vivinet Assessor typically starts a run of simulated VoIP calls every few minutes and measures the performance of the simulated traffic. You can choose to do a quick check of VoIP quality by running a single set of calls and viewing the results.

To schedule a VoIP Quality assessment:

1. Select the time of day when the VoIP Quality assessment will start. You can choose to **Start VoIP quality assessment immediately upon activation**, or you can select a specific time using the **After activation, wait until ...** option.
2. Select the **Duration** of each simulated call in **minutes** and **seconds**.
3. Select whether to run **One set of calls** or to **Run a series of calls** for a specific number of **Days**/**Hours** at selected **Intervals**.

   The number of simulated calls that run during an assessment can be determined by dividing the **Duration** of the assessment by the **Interval** between the calls for a series of assessments. Thus, if your assessment runs for an hour and you schedule calls to run every 20 minutes, Vivinet Assessor sends three sets of simulated VoIP calls between the endpoints in your call groups during the assessment.

   The minimum interval between call start times is six minutes. Use the minimum interval to emulate heavier call traffic. Or increase the interval to determine how well VoIP performs when traffic is lighter. You can set an *initial delay* before sending call data, which effectively staggers the sending of call traffic among all the call groups. For more information, see Section 7.10.2, “Setting the Initial Delay,” on page 76.

   NOTE: The endpoints need some time to report the results of the simulated calls to the Console. Therefore, the minimum length of time between the duration and interval you set must be five minutes. For example, if you set a call duration of five minutes and a calling interval of six minutes, you will be prompted to increase the interval or decrease the duration of the calls. In this case, you could simply increase the calling interval to ten minutes.

   ---
4. If necessary, click **Undo Changes** to discard your changes and revert to the previous schedule.
5. Click **Validate Schedule** to apply your selections to the current assessment and commit them to the database.
6. Click **Save** on the File menu to save the assessment in a location of your choice.

You can create or change a stop-assessment threshold for this assessment. For more information, see Section 7.8.3, “Configuring Stop-Assessment Thresholds,” on page 71.

7.6 Verifying a VoIP Quality Assessment

Click the **Verify** view tab to verify your assessment before you run it.

Verification is required before an assessment can begin because Vivinet Assessor must contact each of the selected endpoint computers and send them the schedule and scripts.

Verification is like a mini-assessment. You will receive some preliminary results after you verify your assessment, which let you see right away whether you need to make any changes to the assessment Design. For more information, see Section 11.1, “Verification Errors,” on page 121.

To verify an assessment:

1. Click **Start Verification**. The **Status** fields indicate verification progress, start time and end time. When verification is complete, the Summary tables display the results.
2. Click the **VoIP** tab to view the Call Groups—MOS Summary of Verification Calls table.
3. Click the **Background Traffic** tab to view the Background Traffic—Summary table.
4. If any errors occur during verification, a warning icon appears next to the affected endpoint in the Summary tables. Click **View Error Log** to see what happened and which endpoints were affected.
   - If Performance Endpoint software was not detected by one of the computers in the assessment, install the software. For more information, see Section 1.4, “NetIQ Performance Endpoints,” on page 12.
   - Return to the Design view and make the necessary changes to assessment configuration to avoid repeating the error. For more information see Section 11.1, “Verification Errors,” on page 121 and Section 7.4, “Designing a VoIP Quality Assessment,” on page 58.

7.7 Running a VoIP Quality Assessment

In the Run view, start the VoIP Quality assessment by clicking **Activate Assessment**.

The status and the preliminary results are continually updated and indicate how the assessment is proceeding. Large assessments—that is, assessments with many call groups that are collecting timing records—take longer to process than smaller ones. When an assessment collects many timing records, even after all calls have completed, the Running indicator may still be spinning and the Status may still read “Calls running...” until results have been processed and entered into the database.

Field	Description
Status	The current status of the assessment. The assessment is ready to run when the status reads “Verified.”
Start time	The time you started the assessment.
End time (estimated)	The time you have scheduled the assessment to end. The end time is “estimated” because the run interval and call duration you specified, plus the time needed for the endpoints to report results, cannot be exactly calculated. The actual end time is set when the assessment is stopped or completed.
View Error Log	Accesses the Log Viewer, which lets you sort and filter errors and analyze their causes. For more information, see Section 11.3, “Scheduler Errors,” on page 122.
View summary of most recent calls	Shows quality results only for the last set of simulated calls sent during the assessment.
View summary of all calls	Shows quality results for all simulated calls sent during the assessment.

Field	Description
VoIP tab	Contains the “Call Groups—MOS Summary of All Calls” table, a table of preliminary results for each call group: ◆ Errors—Indicates whether any errors occurred during calls run between the endpoints in this call group. ◆ Endpoint 1—The computer acting as Endpoint 1 in the call group. Initiates the calls and reports results back to the database. ◆ Endpoint 2—The computer acting as Endpoint 2 in the call group. ◆ Script—The script used. Generally refers to the codec, but some optional parameters can be altered. For more information, see Section 7.11.2, “Reviewing Codec Types,” on page 78. ◆ # Concurrent Calls—The number of concurrent voice over IP calls represented by the connector of the current call group. ◆ Total Calls Simulated—The number of simulated VoIP calls sent over the network between the endpoints in the call group. ◆ %Good, %Acceptable, %Poor—Percentage of calls whose quality scores fell into the range of scores considered “good,” “acceptable,” or “poor” performance.
Background Traffic tab	Contains the “Background Traffic—Summary” table, which presents the configured and actual data rates for each call group.
Analyze and Chart Results button	Click to review the results of your assessment in Vivinet Assessor Analysis Console. For more information, see Chapter 9, “Working with Analysis Console,” on page 105.

If an error occurs, click **View Error Log** to find out what happened. At any time, you can stop the assessment and change configuration parameters before starting it again. Simply click the **Stop Assessment** button.

Although the Run view lets you stop an assessment, the Vivinet Assessor Scheduler component will also stop the assessment when the time period you entered in the Schedule view has passed.

NOTE

- You can run an assessment of VoIP Quality and monitor Utilization at the same time. However, you must complete all configuration of each assessment type before you start either one. Once any assessment is active, no configuration options are available.
- When you run an assessment again, all results from a previous assessment run are removed from the database.

7.8 Setting Assessment Options

Now that you have learned how to design, schedule, verify, and run a VoIP Quality assessment, you are ready to try out some of the extra features of Vivinet Assessor. If you have Performance Endpoints installed, Vivinet Assessor offers extensive options for customizing your VoIP implementation. You can also try out different VoIP optimizations, such as QoS, silence suppression, and jitter buffer sizes.

Assessment Options let you control how data is shown in VoIP Readiness reports, how the VoIP Quality assessment runs through a firewall on the network, and whether the Scheduler service should stop the assessment if the returned results are poor enough.

To set assessment options:

1. In the Assess VoIP Quality view, click Assessment Options on the Options menu.
2. Set the **report parameters** that determine quality standards for voice over IP on your network. For more information, see Section 7.8.1, “Setting Result Ranges,” on page 68.
3. Set the Vivinet Assessor **reporting port**, the port used when the endpoints report results back to the Console. For more information, see Section 7.8.2, “Working with Firewalls,” on page 69.
4. Determine whether, and how quickly, the Scheduler should **stop a running assessment** if preliminary results are extremely poor. For more information, see Section 7.8.3, “Configuring Stop-Assessment Thresholds,” on page 71.
5. Set thresholds that determine when additional diagnostic information will be automatically gathered for a call group. For more information, see Section 7.9.3, “Configuring the Vivinet Diagnostics Integration,” on page 74.
6. Control how measurements are taken and reported during the VoIP Quality assessment. For more information, see Section 7.8.4, “Setting Assessment Run Options,” on page 72.
7. To revert changed fields to their default values, click **Restore Defaults**.
8. Click **OK**.

7.8.1 Setting Result Ranges

You can control how Vivinet Assessor evaluates the quality of VoIP calls on your network.

To set reporting result ranges:

1. From the Assess VoIP Quality view, click **Assessment Options** on the Options menu, and then click the **Result Ranges** tab.
2. Set one or all of the ranges for the different reporting parameters:

Parameter	Description
Call Quality	Determines how MOS estimates are mapped to VoIP quality ratings. The MOS scale runs from 1 to 5, with 1 representing the lowest quality. Vivinet Assessor rates call quality as Poor, Acceptable, or Good. Enter numbers from 1 to 5, inclusive, to determine which Mean Opinion Scores are rated Good and Acceptable; all lower scores are then rated Poor. For more information, see Section 8.5.1, “Mean Opinion Score,” on page 98.
Delay	Determines how delay (latency) is mapped to VoIP quality ratings. Set the maximum amount of delay (in milliseconds) that a call can have if its quality is rated Good or Acceptable. Any call with higher delay is then rated Poor. For more information, see Section 8.5.2, “Delay,” on page 100.

Parameter	Description
Lost data	Determines how data loss is mapped to VoIP quality ratings. Set the maximum amount of datagrams lost (in % of total datagrams sent) that a call can have if its quality is rated Good or Acceptable. Any call with a higher percentage of data loss is then rated Poor. For more information, see Section 8.5.5, “Lost Data,” on page 102.
Jitter Buffer loss	Determines how datagrams lost due to jitter buffer overruns or underruns are mapped to VoIP quality ratings. If jitter is detected, jitter buffer loss becomes a MOS impairment. Set the maximum amount of jitter buffer loss, expressed as a percentage of all datagrams sent, that a call can have if its quality is rated Good or Acceptable. Any call with higher jitter buffer loss is then rated Poor. For more information, see Section 8.5.3, “Jitter,” on page 101.

7.8.2 Working with Firewalls

If there is a firewall on your network, you need to ensure that simulated traffic, plus flows carrying assessment setup information and assessment results, are allowed through the firewall.

Running any version of Windows where the Windows Firewall feature is installed is equivalent to running with a firewall, so the steps detailed below apply to this configuration. For more information, see “Windows Firewall Feature” on page 71.

Vivinet Assessor uses RTP, which is equivalent to UDP for many firewalls, for simulated VoIP call traffic, and uses TCP for setup and reporting. For more information, see Section 1.3, “How Vivinet Assessor Works,” on page 11.

The extra configuration you do at the firewall depends on the type of firewall you are using and whether the firewall is located between the Vivinet Assessor Console and the , or between the endpoints in a call group.

From the Assess VoIP Quality view, click **Assessment Options** on the Options menu, and then click the **Firewall** tab. Use the information in the following topics to make sure your firewall and Console settings are in agreement.

NAT-Enabled Firewalls

Network Address Translation (NAT) can be disruptive in VoIP networks because the addresses the firewall needs to translate are hidden within the payload of each VoIP packet. One workaround is to use static NAT, which maps each IP address for points on the secure side of the firewall to its own static IP address on the public or non-secure side.

NOTE: If a device is performing dynamic NAT, or “overloading,” you cannot run VoIP Quality assessments through the firewall. With dynamic NAT, private and public addresses are not statically mapped. Protected nodes may be assigned IP addresses randomly, when they make a request to send data to a public node, or they may share the same public IP address but receive different port assignments dynamically. This routing technique is called overloading. For a VoIP Quality assessment, the endpoints used in call groups must maintain the same addresses throughout.

With a NAT device active between the endpoints in a call group, enter the IP address of the endpoint as the **Network address** when you create the endpoint. Then enter a NAT address—the IP address assigned to this endpoint for network address translation—in the **NAT address** field on the Create/ Edit an Endpoint dialog box. The NAT address allows the endpoints to find each other through the firewall.

See Section 7.4.2, “Creating an Endpoint,” on page 59 for more information about creating endpoints where a NAT-enabled device is active. Then consult Section 7.12.5, “Performing Assessments with NAT,” on page 85.

If the NAT-enabled firewall is located between the Console and the , continue reading in the “All Firewalls” on page 70 topic for more information about the necessary configuration. Then consult Section 7.4.2, “Creating an Endpoint,” on page 59.

All Firewalls

The **Firewall** tab lets you configure a Reporting Port and a Call Traffic Port range. Reporting refers to TCP communications, setup and reporting information, between the Console and the endpoints Call Traffic refers to bi-directional endpoint-to-endpoint VoIP traffic using RTP, recognized as UDP by many firewalls.

NOTE: A NAT-enabled firewall requires special configuration when you create the endpoints in the Design view. For more information, see Section 7.4.2, “Creating an Endpoint,” on page 59.

The necessary firewall and Console configuration depends on the location of the firewall in your network:

Location	Configuration
Firewall located between Console and	First, your firewall needs to be configured to pass TCP streams from the Console through Port 10115 to the , and from the endpoints to the Console through Port 10116. On the **Firewall** tab, enter a **Reporting port** for the endpoints to use when reporting results back to the Console, or leave the default at 10116. Choose **AUTO** to let the Console choose the port dynamically; this means you will not know which ports to open at the firewall. **NOTE:** After you set or change the reporting port, you must stop and restart the Vivinet Assessor Scheduler service. For more information, see Section 11.3, “Scheduler Errors,” on page 122.
Firewall located between the	First, your firewall needs to be configured to pass bi-directional VoIP (RTP) streams through one particular range of ports. And it also needs to pass bi-directional TCP and UDP streams through Port 10115 because the endpoints need to be able to send setup and clock-synchronization messages to each other through the firewall. On the **Firewall** tab, enter as the **Call Traffic** port the range of ports you configured at the firewall for VoIP RTP (UDP) flows between the endpoints Within any range of ports you set, the endpoints will only use even-numbered ports (which is what real VoIP RTP streams use). The default Call Traffic setting, AUTO, lets the endpoints choose the port dynamically. For VoIP traffic, they use even-numbered ports between 16384 and 65534.

Windows Firewall Feature

If you are running Vivinet Assessor on Microsoft Windows Server 2008 or later, you are running with a firewall and may find that assessments of VoIP Quality do not run properly. You must perform one of the following tasks:

- Disable the firewall option in **Control Panel > Windows Firewall**.
- Create two inbound rules for the following Assessor executables: `Varun.exe` and `Vassessor.exe`

To create inbound rules for Assessor executables:

1. Navigate to Administrative Tools in the Control Panel and click **Windows Firewall with Advanced Security**.
2. Select Inbound Rules and New Rule.
3. Click Next.
4. Click Browse and navigate to `varun.exe` in the file system.
5. Click Next.
6. Click Next.
7. Click Next.
8. Provide a **Name** for the rule, such as `Allow Varun.exe`.
9. Click Finish.
10. Repeat this process for `Vassessor.exe`.

7.8.3 Configuring Stop-Assessment Thresholds

A stop-assessment threshold allows the VoIP Quality Assessment to stop sending simulated VoIP traffic over your network if call performance is consistently poor. In the event of a prolonged network outage or extraordinary congestion, the Assessor Scheduler service will stop an assessment from adding its simulated traffic to the mix. By default, no stop-assessment threshold is configured for a new assessment.

From the Assess VoIP Quality view, click **Assessment Options** on the Options tab, and then click the **Stop-Assessment Threshold** tab to select the conditions that determine when Vivinet Assessor automatically stops a running assessment.

A stop-assessment threshold does not stop an assessment immediately. As the assessment runs, results from each set of simulated calls are checked as soon as the set is completed. The Scheduler checks the percentage of results that indicate Poor call quality or show that a call group or endpoint was Unavailable. It will not start the next set of calls if results exceeded your threshold. For example, if you configure your stop-assessment threshold to stop after collecting **25**% Poor and Unavailable results in **3** consecutive sets of calls, the stop-assessment threshold kicks in if the Scheduler detects that the percentage or Poor and Unavailable results was 26% or higher during three consecutive calling intervals.

In the Run view, the status of an assessment that has been stopped by a stop-assessment threshold will read, “Assessment stopped by Scheduler. Threshold exceeded.” For more information, see Section 2.2.4, “Vivinet Assessor Scheduler Service,” on page 22.

7.8.4 Setting Assessment Run Options

When assessing VoIP Quality, Vivinet Assessor runs simulated VoIP calls between the endpoints you selected for your call groups in the Design view. To measure the performance of these simulated calls, the endpoints generate *timing records* containing performance data and periodically send these records in batches back to the Vivinet Assessor, which uses them to calculate the metrics shown in reports and in Analysis Console for each call group. By default, a new timing record is produced every five seconds.

You can change two default settings that control how measurements are taken and reported during the VoIP Quality assessment.

To change run options:

1. From the Assess VoIP Quality view, click **Assessment Options** on the Options menu, and then click the **Run Options** tab.
2. To set the run option, select **Override timing record duration** and enter a new value. Accepted values are 1-60 seconds, inclusive.

   Some caveats apply, however. No timing records should be returned while simulated calls are running on the network because the batch file transfer traffic interferes with call performance and skews results. The five-second default avoids this situation, particularly if you also accepted the default options for the call traffic on the **Schedule** view tab. Calls that last one minute are sent between the endpoints every 15 minutes.

   If you try to set a timing record duration that will send timing record batches while calls are running, you will see a warning message.

   It is also important to ensure the assessment does not return too many results. The smaller the timing record size you select, the more records must be stored in the database. That is why five seconds is the recommended setting. If you select a setting that may return more than 3.6 million results for the VoIP Quality assessment, you will see a warning message.
3. To see more detailed assessment results in Analysis Console, select **Collect call details (timing records) when running a series of calls**. This option affects the level of granularity of the data you collect. When this box is checked, the VoIP Quality assessment collects and stores individual timing records for an assessment in which you run a series of calls.

   When timing records are not collected for series of calls, results per call direction, per call group are totaled and stored in the assessment database instead.

   Timing records are always collected and stored when you run a *single set of calls*. When you create a new assessment, timing records are collected by default. For assessments created with an older version of Vivinet Assessor and upgraded to the current format, timing records are not collected by default.

For more information about timing records and how they are used in Analysis Console, see Section 9.4.2, “Understanding Data Streams,” on page 112.

7.9 Working With Vivinet Diagnostics

When you run a VoIP Quality assessment, you can perform some real-time troubleshooting if you are also running NetIQ Vivinet Diagnostics on the same computer. Vivinet Diagnostics diagnoses problems with the routing, connections, and performance of VoIP phone calls on your network.

7.9.1 Overview

By default, Vivinet Assessor automatically invokes Vivinet Diagnostics version 1.1 (or later) during the VoIP Quality assessment if it detects call quality that falls below a certain threshold. In such cases, Vivinet Diagnostics runs in the background, while the VoIP Quality assessment is still visible.

Poor MOS values calculated for the simulated calls sent between the endpoints determine whether Vivinet Diagnostics runs during an assessment. A MOS value is considered Poor if it falls into the Poor result range you configured for the assessment. For more information, see Section 7.8.1, “Setting Result Ranges,” on page 68.

For any given call group, Vivinet Assessor distinguishes between a single instance of poor call quality and a potential problem by keeping track of the number of times the poor performance was detected. You can determine the number of times that a low MOS must be reported for a call group before Vivinet Diagnostics will be launched. For more information, see Section 7.9.3, “Configuring the Vivinet Diagnostics Integration,” on page 74.

All the information Vivinet Assessor has gathered about a particular call group is saved in separate Vivinet Diagnostics-compatible files (`.dgv` format), which are stored in the `Vivinet Assessor\Diagnoses` folder. You can view these files by calling them up in Vivinet Diagnostics. If you run an assessment again (thus clearing its results), associated Diagnosis files are deleted unless you save them with new names, or to a new location.

The filenames assigned to `.dgv` files are a combination of the assessment name, the call group’s index (a value identifying it in the assessment database), and the time the Diagnosis was completed. If you run a Diagnosis again based on one of these associated files, you will be prompted to save it with another name first.

If you use the Save As or Export commands to create a copy of an assessment that has associated `.dgv` files, the new assessment will not have associated `.dgv` files.

7.9.2 Viewing Diagnoses in the Run View

When Vivinet Assessor and Vivinet Diagnostics are installed on the same computer, you will automatically gather diagnostic information to aid in troubleshooting the VoIP network. Diagnostic information is gathered by default during the VoIP Quality assessment. Once this information has been gathered and analyzed for a call group, you will see an indication in the Call Groups table of the Run view. Click the **Diagnoses** column to sort the table by call groups for which diagnostic information is available.

To view a diagnosis, right-click the relevant call group in the table and select **View Diagnoses with Vivinet Diagnostics**. Vivinet Diagnostics launches and displays the available diagnoses.

When multiple diagnoses exist for a single call group, you can select the diagnosis you want to view from a list that is available when you right-click on the call group. The existence of multiple diagnoses is indicated by a value next to the diagnosis icon.

In Vivinet Diagnostics, a particular diagnosis may be distinguished by its timestamp, which indicates the time a problem was detected on the network.

7.9.3 Configuring the Vivinet Diagnostics Integration

You can disable the Vivinet Diagnostics integration without uninstalling Vivinet Diagnostics. You can also determine the circumstances under which Vivinet Diagnostics is launched.

To configure the Vivinet Diagnostics integration:

1. From the Assess VoIP Quality view, click **Assessment Options** on the Options menu, then click the Vivinet Diagnostics tab.
2. Set the following parameters as necessary:

Field	Description
Use Vivinet Diagnostics to analyze the causes of poor call quality for a call group	Enables and disables the diagnostic feature. By default, Vivinet Diagnostics will be invoked automatically if poor call quality is detected for a call group.
Invoke Vivinet Diagnostics for a call group when	Thresholds that control the circumstances in which diagnostic information will be made available for a call group.
The call group's MOS is poor at least N times	The number of simulated calls that must report poor performance (as determined by low MOS values) before Vivinet Diagnostics will be invoked.
In the previous N calls	The number of previous simulated calls to consider when counting calls with poor performance (as determined by low MOS values).
Do not analyze the same call group more than N times per day	Limits the number of times Vivinet Diagnostics will diagnose a VoIP problem between the endpoints in a single call group each day.

7.10 Working with Call Scripts

Call scripts are collections of parameters set to recommended values that you assign to call groups when you design your VoIP Quality assessment. Each default call script is configured for assessing a typical voice over IP implementation based on a supported codec. For more information, see Section 7.11.2, “Reviewing Codec Types,” on page 78.

When you create connectors in the Design view, you can quickly configure parameters for an assessment by choosing a call script from the list.

You can customize a call script, although you must assign it a name to distinguish it from the default call script it was based on. A call script you modify and rename is later available in the Call Scripts List dialog box.

You can export call scripts from other assessments, including assessments you created with an earlier version of Vivinet Assessor, and then import them into new assessments. For more information, see Section 10.3, “Exporting and Importing Assessments, Scripts, and Definitions,” on page 118.

7.10.1 Adding a Call Script

By default, call scripts correspond to codecs, as indicated by their names. Default call scripts cannot be changed or deleted; instead, you must add new call scripts based on the default scripts. Once you add a call script with customized settings, you assign it a name to distinguish it from the default call script it was based on. Any call script you modify and rename is later available in the Call Scripts List dialog box and can be edited.

To add a call script:

1. From the Assess VoIP Quality view, click **Call Scripts** on the Options menu.
2. *To add a call script*, click **Add**. Complete the fields as discussed below and then click **OK**.
3. *To change a call script*, select a non-default call script in the list and click **Modify**. Complete the fields as discussed below and then click **OK**.
4. *To copy a call script*, select a call script in the list and click **Copy**. Complete the fields as discussed below and then click **OK**.

Field	Description
Call Script Name	By default, the same as the codec. Enter a new name to distinguish a call script you modified.
Codec	The type of codec used on your network. Choose one of the supported codecs from the list. For more information, see Section 7.11.2, “Reviewing Codec Types,” on page 78.
Packet Loss Concealment	Packet Loss Concealment (PLC) is enabled by default in version 3.2 of Vivinet Assessor; it was disabled by default in previous versions. Most G.711 codecs implement this feature. For more information, see Section 7.11.2, “Reviewing Codec Types,” on page 78.
Use silence suppression	Emulates the effects of silence suppression (also called voice activity detection) on the line during the VoIP Quality assessment. Disabled by default; when enabled, uses a 50% voice activity rate. For more information, see Section 7.11.5, “Understanding Silence Suppression,” on page 80.
Voice activity rate	The percentage of time during a simulated call that talking seems to occur. Silence suppression means that during periods of silence in a conversation, no data is sent. The activity rate determines how much actual voice data the simulated call contains. Default is 50% voice activity; accepted values are 1% to 100%, inclusive.
Override delay between voice datagrams	Determines the datagram size to be used in the assessment. VoIP applications break voice data into chunks based on delay, or the amount of time, in milliseconds (ms), between successive datagrams. For the G.723 codecs, the default value is 30 ms; for all other codecs, the default is 20 ms. Values entered must be between 10 and 200 ms. Vivinet Assessor may adjust values slightly after you enter them so that no partial buffers are sent. For more information, see Section 7.11.4, “Setting Datagram Sizes,” on page 79.
QoS name (optional)	Emulates the effects of a Quality of Service (QoS) scheme on call quality. If you enable a quality of service, you must select a pre-configured QoS definition that determines how the traffic will be marked. QoS is not supported by all endpoint operating systems. For more information, see Section 7.11.7, “Reviewing Quality of Service,” on page 81.
Advanced	Reveals more call script parameters for advanced users to configure.

Field	Description
Initial delay type	Introduces delays between the start of each call in a set of calls. Instructs the endpoints to delay sending RTP datagrams for slightly different amounts of time while preserving the interval specified in the schedule. The type of initial delay refers to the distribution algorithm the endpoints use to calculate it. The initial delay parameter and the algorithm choices are explained in Section 7.10.2, “Setting the Initial Delay,” on page 76. Select **Constant Value** to set your own initial delay value. All the endpoints in all call groups will then pause for the same amount of time before starting to send call traffic.
Additional fixed delay	Lets you add a delay value from a known, constant source. For example, if you are testing equipment that adds 10 milliseconds of delay to each datagram, enter 10 ms here. Range is 0-300 ms.
Jitter buffer	Emulates the effects of jitter buffering on your VoIP network. Jitter buffers may be configured based on time (called an “absolute” jitter buffer) or based on number of datagrams (a “frame-based’ jitter buffer). All call scripts have a default jitter buffer of **2** voice datagrams. For more information, see Section 7.11.6, “Understanding Jitter Buffers,” on page 80.

5 *To delete a call script*, select a non-default call script in the list and click **Delete**.

6 Click **OK**.

7.10.2 Setting the Initial Delay

You use the **Initial delay type** call script parameter to introduce variations among simulated calls or streams of background traffic in order to realistically emulate traffic on a VoIP network. To better represent the random way in which data is sent over a VoIP network, the initial delay parameter instructs the endpoints to delay the start of calls (or, for background traffic, the sending of TCP/IP datagrams) for slightly different amounts of time while preserving the scheduled call duration you specified in the Schedule view. For more information, see Section 7.5, “Scheduling a VoIP Quality Assessment,” on page 65.

When you configure an initial delay value in a call script, you actually introduce variations in the length of each call as well, which means that the amount of data sent by the calls will not be exactly the same. No matter what initial delay you set, all calls stop running at the same time, when the call duration timer expires.

The call duration also controls the amount of TCP/IP data sent by Background Traffic connectors. The variability introduced by setting an initial delay for background traffic affects the timing of `SEND` commands. Just as with calls, when the call duration timer expires, all background traffic stops running at the same time.

For example, you set an initial delay of between ten and 25 seconds using a Uniform distribution. Calls at the lower limit of the distribution will send data for as much as 15 seconds longer than those at the upper limit of the distribution because the delay before they start to send data will be 15 seconds shorter, yet they will stop sending data at the same time as the calls with longer initial delays.

Despite any initial delay that is configured, all calls are connected immediately. The endpoints then either sleep or begin to send data according to the initial delay value and distribution selected.

The type of initial delay refers to the distribution algorithm the endpoints use to calculate the delay. The initial delay distribution choices are as follows:

Algorithm	Description
Uniform	Distribution of initial delay times between the upper and lower limit you set is completely uniform. Any number within the upper and lower limits is as likely to be used for the delay value as any other number.
Normal	Distribution of initial delay times between the upper and lower limits you set is a normal distribution, plotted with a bell curve. The Marsaglia-Bray algorithm is used to generate the normal distribution.
Poisson	Distribution of initial delay times between the upper and lower limit is a Poisson distribution; most values occur within +/-3 standard deviations with respect to the average. The incomplete gamma function is used to generate this distribution.
Exponential	Distribution of initial delay times between the upper and lower limit you set is an exponential distribution. If you plot the (descending) times against the number of occurrences, the graph's maximum will be at the upper limit and the minimum will be at the lower limit.

For more information, see the discussion of the **Initial delay type** field in Section 7.10.1, “Adding a Call Script,” on page 75.

7.11 Increasing Assessment Accuracy

A VoIP Quality assessment increases in accuracy if you run simulated traffic that closely resembles the actual VoIP traffic you will be running once your VoIP implementation is operational. And you can also increase assessment accuracy if you add background traffic when you design your assessment.

Installing VoIP equipment entails a series of choices that affect voice traffic and how the network must handle it. Therefore, before you select VoIP Quality assessment parameters, acquaint yourself with the following options and how they can affect VoIP network performance:

- Seven different codec types, emulating different compression algorithms, data rates, and datagram sizes
- Packet loss concealment for G.711 codecs
- Voice datagram sizes
- The ability to use silence suppression
- A jitter buffer
- Any additional, fixed delay values that apply
- The typical amount of TCP/IP application, or “background,” traffic that will share the network with VoIP
- Quality of Service

Once you understand these conditions and parameters, you will be better equipped to determine which ones your VoIP implementation will deploy. Or you can experiment with them to see if the VoIP Quality of the simulated traffic improves.

7.11.1 Understanding Background Traffic

Find out how good VoIP calls will sound on the network during times of heavy or average network usage by adding background traffic to your VoIP Quality assessment. The Background Traffic Connector in the Design view lets you add a specific amount of TCP/IP traffic to emulate network utilization levels.

Background Traffic Connectors send TCP/IP packets between the endpoints in your network. You select a connector's data rate to match an expected or projected level of network bandwidth utilization for that path. For example, if you want to assess the VoIP readiness of a T1 line (1.544 Mbps), you would probably select 128 kbps (Fractional T1/ISP) to simulate heavy network traffic, or 64 kbps (Fractional T1) to simulate lighter network utilization. You may want to select a data rate based on the results from the Utilization assessment.

You can also set a "custom" data rate for background traffic. For example, you can send a single packet of a specific size every few seconds. For more information, see Section 7.4.6, "Setting a Custom Data Rate," on page 64.

The extra network traffic generated by a Background Traffic Connector helps you test the effects of QoS, or it shows how VoIP quality is affected when small VoIP packets get behind larger TCP/IP packets in the network.

For information about adding background traffic to a VoIP Quality assessment, see Section 7.4.5, "Creating a Background Traffic Connector," on page 63.

For more information about the background traffic results you can view in Analysis Console, see Section 9.2.6, "Background Traffic Tab," on page 110.

7.11.2 Reviewing Codec Types

In a VoIP transmission, the codec samples the sound and determines the data rate. You can perform voice over IP assessments using seven codec types, represented by seven call scripts. For more information, see Section 7.10, "Working with Call Scripts," on page 74.

Codec	Description
G.711u	ITU standard for H.323-compliant codecs. Uses the u-law for companding, the most frequently used method in the USA. PLC is enabled.
G.711a	ITU standard for H.323-compliant codecs. Uses the A-law for companding, a popular standard in Europe. PLC is enabled.
G.726	A waveform coder that uses Adaptive Differential Pulse Code Modulation (ADPCM). ADPCM is a variation of pulse code modulation (PCM), which only sends the difference between two adjacent samples, producing a lower bit rate.
G.729	High-performing codec; offers compression with high quality. Optimized for voice over frame relay, teleconferencing, and other applications.
G.729A	Also known as G.729 Annex A. High-performing codec; offers compression with high quality. Same as G.729, but less complex to implement.
G.723.1-MPMLQ	Uses the multipulse maximum likelihood quantization (MPMLQ) compression algorithm.
G.723.1-ACELP	Uses the conjugate structure algebraic code excited linear predictive compression (ACELP) algorithm.

7.11.3 Reviewing Packet Loss Concealment

Packet loss concealment (PLC) is an option if you are using the G.711u or G.711a codecs. PLC describes a number of techniques for minimizing or masking the effects of data loss during a VoIP conversation. When PLC is enabled (the default setting), Vivinet Assessor assumes that the quality of your conversation would be improved, but this improvement is only factored into the MOS estimate calculation if any data is lost.

In the table below, “packetization delay” refers to the delay this codec introduces as it converts a signal from analog to digital; this delay is included in the MOS estimate, as is the *jitter buffer delay*, the delay introduced by the effects of buffering to reduce interarrival delay variations. For more information, see Section 8.5, “Reviewing VoIP Quality Assessment Factors,” on page 98.

Codec	Default Data Rate	Default Datagram Size	Packetization Delay	Default Jitter Buffer Delay	Theoretical Maximum MOS
G.711u G.711a	64 kbps	20 ms	1.0 ms	2 datagrams (40 ms)	4.40
G.726	32kbps	20 ms	1.25 ms	2 datagrams (40 ms)	4.22
G.729 G.729A	8 kbps	20 ms	35.0 ms	2 datagrams (40 ms)	4.07
G.723.1-MPMLQ	6.3 kbps	30 ms	67.5 ms	3 datagrams (60 ms)	3.87
G.723.1-ACELP	5.3 kbps	30 ms	67.5 ms	3 datagrams (60 ms)	3.69

7.11.4 Setting Datagram Sizes

With each new call script you add, you can choose to **Override delay between voice datagrams**. This option is recommended only for advanced users, and it is not likely that you will need to set it.

However, the following is an explanation of what happens when you choose to override the delay associated with the codec you are using.

The delay between datagrams determines the datagram size to be used in the simulated VoIP calls. VoIP applications break voice data into chunks based on delay, or the amount of time between successive datagrams. Each call script uses a delay value appropriate to its codec: the faster codecs use 20 ms and the G.723.1 codecs use 30 ms. This means, for example, that every 20 milliseconds, the VoIP application adds a header to any voice data it has received and places the datagram on the wire. Smaller delay values mean that the header-to-payload ratio is larger; more, smaller datagrams are sent, which increases processing overhead. Greater delay values mean that fewer, larger datagrams are sent, and that delay is probably higher.

Some VoIP equipment refers to the delay between voice datagrams as the “speech packet length.” For example, at 64 kbps, a “20-millisecond speech packet” implies that the sending side creates a 160-byte datagram payload every 20 ms. A simple equation relates the codec speed, the delay between voice packets, and the datagram payload size.

Datagram payload size (in bytes) equals:

```
Codec speed (bits/sec) x packet delay (ms) / 8 (bits/byte) x 1000 (ms/sec)
```

In this case:

```
160 bytes = (64000 x 20)/8000
```

For a given data rate, increasing the delay increases the datagram size because datagrams are sent less frequently. A delay of 30 ms at a data rate of 64 kbps would mean sending 240-byte datagrams.

Unless you are an equipment manufacturer, you are much better off leaving the datagram sizes at their default values. These values were selected because they match those of the codec being emulated and allow for realistic simulation of VoIP datagram traffic.

Values for **Override delay between voice datagrams** must be between ten and 200 ms. Vivinet Assessor may adjust values slightly after you enter them so that no partial buffers are sent.

For more information, see Section 7.10.1, “Adding a Call Script,” on page 75.

7.11.5 Understanding Silence Suppression

When you edit a call script for an assessment, you can enable silence suppression in the voice over IP call traffic Vivinet Assessor sends on the network. The codec performs silence suppression, also known as voice activity detection. By default, silence suppression is disabled in all call scripts.

When you enable silence suppression, no data is sent on the network during periods of call silence, that is, when no one is talking. Enabling it means that each simulated call contains less data. For all call scripts, the silence suppression option uses a default voice activity rate of 50%, which means that data is being sent during 50% of each simulated call’s duration. You can set a voice activity rate to include more or less data in calls using silence suppression.

For more information, see Section 7.10.1, “Adding a Call Script,” on page 75.

7.11.6 Understanding Jitter Buffers

To minimize call disruptions from delay and jitter, VoIP phones and gateways typically have jitter buffers. A jitter buffer can be either frame-based or absolute: a *frame-based* jitter buffer will hold a given number of voice datagrams, while an *absolute* jitter buffer is based on time. For example, a frame-based jitter buffer might hold two datagrams, buffering them until a segment of the voice transmission can be reassembled to reduce inter-arrival time variability. An absolute jitter buffer, on the other hand, might be set to 43 ms, and, given a typical 20-ms speech frame, could hold two speech frames and allow for an extra three milliseconds of variability.

Jitter buffers may also be static or dynamic. Each buffer implementation has its strengths. But buffering adds delay while smoothing out variability; therefore, one goal of VoIP network tuning must be to minimize jitter buffer sizes while maintaining call quality.

By default, all the call scripts used in VoIP Quality assessments emulate a frame-based jitter buffer of two datagrams. You can configure buffers based either on time (in milliseconds) or on number of datagrams. Configure your own jitter buffers by clicking **Call Scripts** on the Options menu. The supported range of values is 10-1600 ms for an absolute jitter buffer, and 1-8 for a buffer configured in number of voice datagrams. For more information, see Section 7.10.1, “Adding a Call Script,” on page 75.

NOTE: The Vivinet Assessor jitter buffer call script option does not smooth out jitter. Instead it provides a more accurate Mean Opinion Score (MOS) by better accounting for datagrams that would have been lost due to underrun or overrun of the jitter buffer. In addition, the delay incurred by using a jitter buffer is factored into the MOS. For more information about how Vivinet Assessor uses jitter buffer sizes to assess call quality, see Section 8.5.3, “Jitter,” on page 101.

7.11.7 Reviewing Quality of Service

Using a prioritization or QoS scheme can make a significant difference in call quality, particularly if you are running VoIP on a crowded enterprise network. Vivinet Assessor ships with a default QoS definition that was designed to emulate the QoS used in typical VoIP implementations. The **VoIPQoS** definition specifies that each voice datagram

- is assigned a priority that makes it unlikely to be queued or dropped
- is flagged to receive the lowest possible delay

When you select **VoIPQoS** from the **QoS name** list in the Adding a Call Script dialog box, Vivinet Assessor sets the three IP Type of Service (TOS) precedence bits in the IP header, using the "CRITIC/ECP" setting (`101` or value 5). These same bits are known as the Expedited Flow (EF) setting in the Differentiated Services (DiffServ) standard. More recent DiffServ implementations use all six DiffServ Code Point (DSCP) bits, so this definition has been supplemented by 13 new DiffServ settings you can select when configuring QoS definitions.

To run assessments using other types of QoS, click **QoS Definitions** on the Options menu. In the QoS List dialog box, definitions are listed according to type. Click **Add** to create a new definition. A menu lets you add an **802.1p Definition** or a **DiffServ Definition**.

If you have not tried QoS for your VoIP traffic, you can set up a few call groups that use QoS and a few that do not. Depending on your routers' ability to process requests for QoS, you should see a difference in the groups' Call Quality scores when you compare the results.

802.1p Definitions

IEEE 802.1p is an OSI Layer 2 standard for prioritizing and queuing network traffic at the data link/MAC sub-layer. It can also be defined as best-effort QoS at Layer 2. 802.1p traffic is classified and sent to the destination with no bandwidth reservation.

To run a VoIP Quality assessment using 802.1p, add a QoS definition as instructed below, and then add or copy a Call Script, using the new QoS definition. For more information, see Section 7.10, "Working with Call Scripts," on page 74.

To add an 802.1p QoS definition:

1. Click the **Assess VoIP Quality** view tab.
2. On the Options menu, click **QoS Definitions**.
3. Click **Add** and then click **802.1p Definition**.
4. In the **QoS name** field, assign a name to your definition. You use this name to identify your settings when you apply QoS to a Call Script.
5. In the **Priority** field, select the desired priority setting:
   - **000**--(0) for lowest-priority traffic. Equivalent to no QoS.
   - **011**--(3) for medium-priority traffic. Often used for call setup packets.
   - **101**--(5) for high-priority traffic. Recommended for VoIP data packets.

The three-bit **Prioritization** field in the 802.1p tag establishes eight levels of priority, similar to the IP Precedence bits. A level-eight priority is the highest, and is thus reserved for router-update traffic. However, Vivinet Assessor only supports three priority levels, two of which are appropriate for VoIP traffic.

Network adapters and switches route traffic based on the priority level. The hardware itself-usually a NIC card or an IP phone-does the tagging. Many recently developed IP phones are marking voice packets with a priority of five (101).

NOTE

- Definitions to simulate 802.1p QoS can be used only in call scripts running to Windows 2000 and Windows XP endpoints
- Some older switches support just two or three priority queues, so their implementation of 802.1p does not actually support all of the eight priority levels in the IEEE 802.1p specification. Such switches place 802.1p values of 0 through 3 in a low-priority queue, and priority levels 4 through 7 in a high-priority queue, using only two different priority levels.

DiffServ Definitions

The DiffServ standard for QoS defines an individual packet's per-hop behavior (PHB), or the treatment it receives from routers. PHB depends on a packet's likelihood of being dropped in congested conditions (its "drop precedence") and the amount of forwarding resources—buffer space and bandwidth—that will be devoted to it.

DiffServ-enabled routers can subdivide networks into DiffServ (DS) domains, within which all IP traffic competes for a finite share of bandwidth determined by a committed information rate, or CIR. To ensure that traffic that exceeds the CIR is still delivered without compromising the performance of high-priority traffic, packets within a DS domain are placed into PHB groups, including Expedited Forwarding and Assured Forwarding. Of these two groups, Expedited Forwarding receives slightly lower drop precedence and slightly higher bandwidth allocation than Assured Forwarding.

These groups allow for very exact policy-based QoS: they can be further subdivided to determine which packets are least likely to be dropped and most likely to be forwarded quickly despite congestion. Assured Forwarding includes four classes, AF1-AF4. Within each class, three subclasses may be defined, with increasing drop precedence. For example, AF1 may be the highest class of traffic, but within that class, AF13 will be dropped before AF11 or AF12.

Two DiffServ settings once used as part of the standard implementation may soon be deprecated, or rendered obsolete. Those settings, Expedited Flow and Assured Flow, used only the first three bits of the DiffServ codepoint, the type of service (TOS) bits. More recent DiffServ implementations use all six bits, for a total of 64 possible settings.

The predefined QoS definition that ships with Vivinet Assessor, **VoIPQoS**, is a DiffServ definition that marks bits for Expedited Flow, highest-priority service.

To run a VoIP Quality assessment using your own DiffServ settings, add a QoS definition as instructed below, and then add or copy a Call Script, using the new QoS definition. For more information, see Section 7.10, "Working with Call Scripts," on page 74.

To add a DiffServ definition:

1. Click the **Assess VoIP Quality** view tab.
2. On the Options menu, click **QoS Definitions**.
3. Click **Add** and then click **DiffServ Definition**.
4. In the **QoS name** field, assign a name to your definition. You use this name to identify your settings when you apply QoS to a Call Script.

5 To use a **Predefined DiffServ codepoint**, select bit settings from the list. When you make your choice from the list, the graphic illustrating the **Bit field settings** changes to reflect these choices.

6 To create a **User-defined Diffserv codepoint**, click the buttons for customized **Bit field settings**. The following table shows the DiffServ choices that are available in Vivinet Assessor. TOS-only settings are still supported:

Bit Settings	PHB Class
000000	Best Effort. Default settings in IP. No special treatment given.
101000	Expedited Flow (TOS). Highest-priority service.
101110	Expedited Forwarding. Highest-priority (premium) service. Recommended for VoIP.
011000	Assured Flow (TOS). Medium-quality service.
001010	Assured Forwarding (AF11).
001100	Assured Forwarding (AF12).
001110	Assured Forwarding (AF13).
010010	Assured Forwarding (AF21).
010100	Assured Forwarding (AF22).
010110	Assured Forwarding (AF23).
011010	Assured Forwarding (AF31).
011100	Assured Forwarding (AF32).
011110	Assured Forwarding (AF33).
100010	Assured Forwarding (AF41).
100100	Assured Forwarding (AF42).
100110	Assured Forwarding (AF43).

7 Click **OK** to save your new QoS definition.

NOTE: Some endpoint operating systems require extra configuration to support DiffServ bit settings. For more information, see Section 7.12.1, “Configuring Endpoints for Assessments with QoS,” on page 84.

7.12 Advanced Configuration

Vivinet Assessor is designed to run highly accurate assessments right out of the box—with no extra configuration necessary. However, you may have special requirements in your own environment. The following topics briefly discuss some of the advanced VoIP Quality assessment parameters you can configure.

7.12.1 Configuring Endpoints for Assessments with QoS

You may have to perform some extra configuration at the endpoint computers to allow for VoIP Quality assessments that use QoS. Some endpoint operating systems supported by Vivinet Assessor do not allow for setting the necessary bits for DiffServ and 802.1p QoS. The following table provides a summary:

Endpoint Operating System	Supports DiffServ?	Supports 802.1p?	Notes
Windows Server 2003 Windows XP Windows 2000	Yes	Yes	**DiffServ**: Requires a change in the Registry setting. For more information, see Section 7.12.2, “Changing the Registry Setting,” on page 84. **802.1p**: Requires the Packet Scheduler. For more information, see Section 7.12.3, “Installing the QoS Packet Scheduler,” on page 84. May also require configuration for NIC support. For more information, see Section 7.12.4, “Enabling NIC Support for 802.1p,” on page 85.
Linux	Yes	No	
Sun Solaris	Yes	No	

7.12.2 Changing the Registry Setting

To allow for assessments with DiffServ definitions on Windows 2000 and Windows XP, an addition to the Registry is required. Add the following `DWORD` value at the :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableUserTOSSetting = 0
```

Restart the endpoint computers after you edit their Registry settings. Then run the assessment.

7.12.3 Installing the QoS Packet Scheduler

On Windows 2000 and Windows XP, the QoS Packet Scheduler provides functionality to support 802.1p, although it may not be installed as part of the basic operating system installation. The Packet Scheduler marks the bit settings based on the QoS service type requested by the application. Currently, the Packet Scheduler performs only three different settings.

To install the Packet Scheduler on Windows 2000 or Windows XP:

1. Right-click **My Network Places** and select **Properties**.
2. Right-click **Local Area Connection** and select **Properties**.
3. Click **Install**.

4 Select **Service** and then click **Add**.

5 Select **QoS Packet Scheduler** and click **OK**. The QoS Packet Scheduler appears in the list of installed components in the Local Area Connection Properties dialog box.

6 Restart your computer to ensure that the QoS Packet Scheduler is properly initialized.

7.12.4 Enabling NIC Support for 802.1p

Even though most of the latest NICs (network interface cards) support 802.1p, this support is usually not enabled at the endpoints by default. Perform the necessary configuration as follows (this example is from Windows XP):

1 From the Start menu, click **Settings** and then click **Network Connections**.

2 Right-click **Local Area Connection** and select **Properties**.

3 Click **Configure**, and then click the **Advanced** tab.

4 In the **Property** list, select **802.1p Support**. If it is supported by the NIC card, the **Value** field will read "**Enable**."

5 If the **Value** field reads "**Disable**," select **Enable** and then click **OK**.

NOTE

- Some of the NICs that support 802.1p may require updated driver software to enable it. These drivers are usually available from the NIC vendor.
- If you set up a call group with an 802.1p-enabled host talking to a host that is not 802.1p-enabled, communication errors will be registered in the Error Log.

7.12.5 Performing Assessments with NAT

Devices performing network address translation (NAT) on your network can disrupt VoIP traffic because of the way VoIP packets conceal addressing information. Therefore, if VoIP calls are going to pass through a NAT-enabled device, usually a firewall, you should plan to create at least a couple of call groups with endpoints on either side of the NAT device to check the performance of calls as they pass through it.

Read the topic titled Section 7.8.2, "Working with Firewalls," on page 69 before you try to run a VoIP Quality assessment through a firewall. That topic outlines setup at the firewall and at the Vivinet Assessor Console to allow the assessment to proceed. In addition, the steps to take in creating the endpoints and call groups are slightly different, depending on whether the firewall is located between the Console and the , between the endpoints in a call group, or some combination. In other words, the Console and some of the endpoints in your call groups are on one side of the firewall, and some are on the other side. Basically, the proper configuration depends on whether the simulated calls between the endpoints will cross the NAT device.

Before you set up the call groups, spend some time creating a schematic diagram that includes the NAT device. Then use the diagram when you design the VoIP Quality assessment.

Configuring Endpoints for NAT

“Static” NAT, or “inbound mapping,” refers to scenarios where the firewall device maps the private addresses of all the nodes on the private network to public IP addresses on a one-to-one basis. If an endpoint has a statically assigned NAT address, you should enter that address as the endpoint’s Network Address when you create the endpoint, except where noted in the examples provided below. Devices performing “dynamic” NAT are not supported for VoIP Quality assessments.

To assess VoIP Quality between endpoints on either side of a device performing NAT, you must define a **NAT address** for the endpoints on the private network. This mechanism instructs the endpoints where to send the test VoIP traffic that flows between them during an assessment. And depending on where the Console is located relative to the endpoints and to the NAT device, you may also need to define a **Setup address** for each endpoint. If no **Setup address** is defined, the Console can use the **NAT address** for setup.

To configure endpoints for NAT:

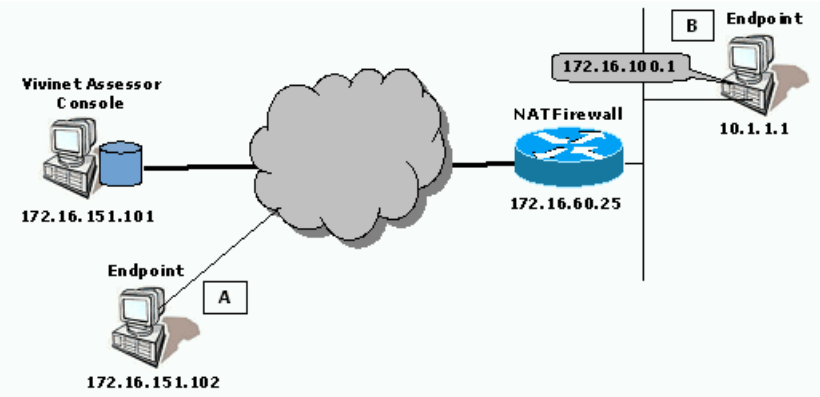
1. Expand the **Assess VoIP Quality** view tab and click the **Design** view tab.
2. On the Create menu, click **Endpoint**.
3. Complete the fields as necessary, using the information in the following topics as a reference.
   - “Scenario 1: One Endpoint behind NAT Device” on page 87
   - “Scenario 2: Both Endpoints behind NAT Device” on page 87
   - “Scenario 3: Endpoints behind Separate NAT Devices” on page 88
   - “Scenario 4: Console and One Endpoint behind NAT Device” on page 89
   - “Scenario 5: Console behind NAT Device, Endpoints with Public Addresses” on page 89
   - “Scenario 6: Console with Public Address; Endpoints on Either Side of NAT Device” on page 90
4. Click **OK**.

Examples of VoIP Quality Assessment with NAT

To see how to set up VoIP Quality assessments that run through a NAT-enabled device, look at the following diagrams of specific network topologies. In the following scenarios, data that travels from the protected or private network outward to the Internet are *outgoing* data, while data traveling from the Internet to the private network are *incoming* data. The firewall treats the UDP and RTP protocols as the same protocol.

Scenario 1: One Endpoint behind NAT Device

In this scenario, the Vivinet Assessor Console and Endpoint A are located on the public Internet, while Endpoint B is located on a private network, behind a NAT firewall. The firewall has 172.16.100.1 as the public address for Endpoint B.

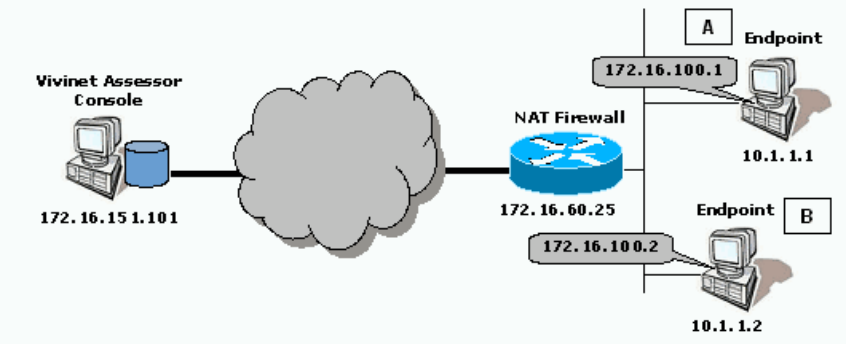


A VoIP connector creates a call group between Endpoint A and Endpoint B. The firewall is configured to allow bi-directional TCP and UDP flows on Port 10115, and bi-directional UDP flows on a selected port for the test call traffic. It is also configured to allow outgoing TCP flows on Port 10116.

Endpoint A	Endpoint B
Network address: 172.16.151.102	**Network address**: 10.1.1.1
	NAT address: 172.16.100.1

Scenario 2: Both Endpoints behind NAT Device

In this scenario, the Vivinet Assessor Console is installed on a computer on the public Internet. Both endpoints A and B are behind a firewall performing network address translation. The firewall has 172.16.100.1 as the public address for Endpoint A, and 172.16.100.2 as the public address for Endpoint B.

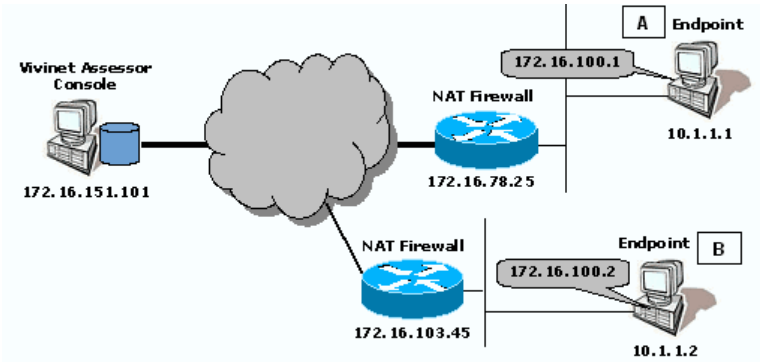


A VoIP connector creates a call group between Endpoint A and Endpoint B. The firewall is configured to allow bi-directional TCP flows on Port 10115, and outgoing TCP flows on Port 10116. With the following configuration, call traffic does not travel through the NAT device:.

Endpoint A	Endpoint B
Network address: 10.1.1.1	**Network address**: 10.1.1.2
Setup address: 172.16.100.1	**Setup address**: 172.16.100.2

Scenario 3: Endpoints behind Separate NAT Devices

In this scenario, the Vivinet Assessor Console is installed on a computer on the public Internet. Endpoint A is behind a firewall performing network address translation. Endpoint B is behind a second NAT firewall. The firewalls have 172.16.100.1 as the public address for Endpoint A and 172.16.100.2 as the public address for Endpoint B.



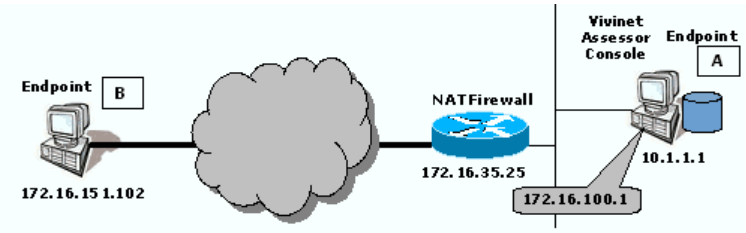
A VoIP connector creates a call group between Endpoint A and Endpoint B. Both firewalls are configured to allow bi-directional TCP and UDP flows on Port 10115, bi-directional UDP flows on a selected port for the test call traffic between the , and outgoing TCP flows on Port 10116.

Endpoint A	Endpoint B
Network address: 10.1.1.1	**Network address**: 10.1.1.2
NAT Address: 172.16.100.1	**NAT address**: 172.16.100.2

Scenario 4: Console and One Endpoint behind NAT Device

In this scenario, the Console and Endpoint A are behind a firewall performing network address translation. Endpoint B is located on the public Internet. The firewall has a public IP address of 172.16.100.1 for Endpoint A.

In most cases with this configuration, depending on the type of firewall used, the Console and endpoint would have to be installed on the same computer because most firewalls would not be able to forward traffic on a certain port to multiple endpoints

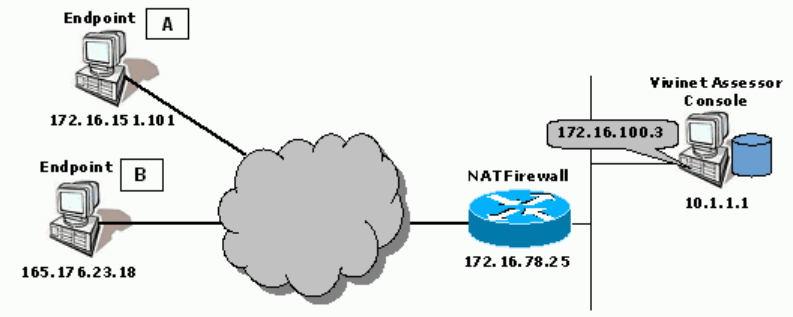


A VoIP connector creates a call group between Endpoint A and Endpoint B. The firewall is configured to allow bi-directional TCP and UDP flows on Port 10115, bi-directional UDP flows on a selected port for the test call traffic, and incoming TCP flows on Port 10116.

Endpoint A	Endpoint B
Network address: 10.1.1.1	**Network address**: 172.16.151.102
NAT address: 172.16.100.1	
Setup address: 10.1.1.1	

Scenario 5: Console behind NAT Device, Endpoints with Public Addresses

In this scenario, the Vivinet Assessor Console has a private address, behind a firewall performing network address translation. Both endpoints in a call group have public IP addresses on the Internet. The firewall has 172.16.100.3 as the public IP address for the Console computer.

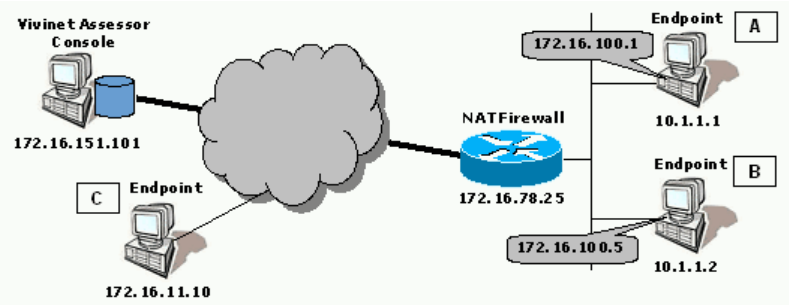


A VoIP connector creates a call group between Endpoint A and Endpoint B. The firewall is configured to allow outgoing TCP flows on Port 10115 for Console-to-endpoint setup communications, and incoming TCP flows on Port 10116 so that the endpoints can send results back to the Console.

Endpoint A	Endpoint B
Network address: 172.16.151.101	**Network address**: 165.176.23.18

Scenario 6: Console with Public Address; Endpoints on Either Side of NAT Device

In this scenario, the Vivinet Assessor Console is located on the public Internet. Two of the three endpoint computers are located behind a NAT device. One of these , labeled B in the diagram below, is used in more than one call group. It is paired with an endpoint on the private side for Call Group 1, and paired with an endpoint on the public side for Call Group 2. The firewall has 172.16.100.1 as the public IP address for Endpoint A, and 172.16.100.5 as the public IP address for Endpoint B.



The endpoint with IP address 10.1.1.2 is created twice, using two different names.

Endpoint B is in the database with Network Address 10.1.1.2 and Setup Address 172.16.100.5 (Endpoint Name is B), and also with the same Network Address, no Setup Address, and NAT Address 172.16.100.5 (Endpoint Name is B-NAT).

NOTE: Vivinet Assessor allows you to create two endpoints with the same IP Network Address only if they have different names and different configurations for their Setup address or NAT address.

VoIP connectors create Call Group 1 between Endpoint A and Endpoint B and Call Group 2 between Endpoint B-NAT and Endpoint C. Call Group 2 tests the NAT device.

When sending test traffic through the firewall to Endpoint B-NAT, Endpoint C uses the NAT Address. However, with Call Group 1, the public addresses shown in the diagram above are only used for assessment setup between the Console and endpoints The call traffic between Endpoint A and Endpoint B will use the Network Addresses, bypassing the NAT firewall. This is important because actual VoIP calls between these network nodes will not cross the firewall.

The firewall is configured to allow bi-directional TCP and UDP setup flows on Port 10115, and bi-directional UDP flows on a selected port for the test call traffic between the endpoints in Call Group 2. It is also configured to allow outgoing TCP flows on Port 10116 so that the protected endpoints can send results back to the Console.

Here is a summary of the configuration for this scenario:

Endpoint Name	Network Address	Setup Address	NAT Address
Endpoint A	10.1.1.1	172.16.100.1	
Endpoint B	10.1.1.2	172.16.100.5	
Endpoint B-NAT	10.1.1.2		172.16.100.5
Endpoint C	172.16.11.10		

The Setup Addresses configured for endpoints A and B are required; they allow the Console to contact those endpoints with assessment setup information through the NAT device.

8 Generating Reports

After an assessment has run on your network, you use the Report view to customize and generate two different reports of the results: the *Executive Summary Report* and the *Complete Report*.

By default, reports include information about all the assessments that you have completed. However, you can selectively filter some of the information to be included.

Some reporting parameters are dependent on result ranges you can configure. For example, Vivinet Assessor calculates Mean Opinion Score (MOS) estimates for each call group and rates each group's overall performance as "Good," "Acceptable," or "Poor" based on its average MOS. The result ranges determine how scores are rated. For more information, see Section 7.8.1, "Setting Result Ranges," on page 68.

You can generate reports while any assessment is still running. But be aware that this action might alter your results slightly. For example, depending on exactly when you click the **Generate Report** button, some call groups in the VoIP Quality assessment might include results from a few more simulated calls than others. And some polling intervals for the Utilization assessment may be incomplete. You are especially likely to interfere with the results if you generate a report from a large assessment—monitoring 25 devices and links, for example—while utilization monitoring is still proceeding.

Do not try to generate and display reports from multiple assessment databases simultaneously, or you will receive an error.

8.1 Customizing a VoIP Readiness Assessment Report

For the Executive Summary and Complete reports, you can add customized information to the cover page, such as your name, your customer's name, and even a logo. If you ran a VoIP Quality assessment, you have the further option of adding Potential Lost Revenue information to a report. Potential lost revenue, which gives you a sense for the likely return on investment (ROI) of your VoIP

deployment, is calculated as lost revenue per hour, per employee. By incorporating lost revenue information in your report, you will be able to estimate the financial impact of poor VoIP quality for the assessed network.

To customize a VoIP Readiness Assessment Report:

1. Expand the **Report** view tab and click the **Set Up** view tab.
2. In the fields in the Cover Page and Potential Lost Revenue sections, supply the appropriate information as described below. You do not need to supply information in all the fields—only those that you want on the cover page or in the Potential Lost Revenue summary.

Field	Description
Report prepared by	Your name, or the name of the person preparing the report.
For	Name of your internal or external customer.
Logo for report	Click **Browse** to navigate to and select a graphic file of your logo, such as a .bmp or .jpg, to place on the cover of the report.
Based on VoIP Quality assessment data, project revenue loss	Check this box to include the Potential Lost Revenue section in your report and calculate potential revenue loss due to Poor and Unavailable calls in the VoIP Quality assessment.
Industry of assessed network	Select the industry for which you are assessing network functions. If the appropriate industry type is not shown in the list, select **Other**.
Use currency from regional settings	By default, lost revenue calculations are done in US dollars. To use the local currency setting of the computer that is generating the report, check to enable this option.
Exchange rate from US ($) to local ($)	Required if you selected **Use currency from regional settings**. Enter a recent exchange rate to convert US dollars ($) to the currency setting of the local computer that is generating the report.
Lost revenue rate of industry	This field is automatically populated when you select any industry type except **Other**. If you selected **Other**, enter the average lost revenue rate for your customer's industry. The figures for average revenue loss for each industry were calculated by TeleChoice, Inc., a leading telecom consulting and analyst firm. The figures were derived based on specific and factual industry information provided by select US companies in each segment as well as from US government-compiled information. Information was collected and analyzed in 2002, although much of the underlying data was from 2000 and 2001.
Number of employees using assessed network	Enter the number of employees that are represented by the VoIP Quality assessment—the number of people who will be making VoIP calls on the network you are assessing. Assume a one-to-one employee-to-phone relationship, so if you ran the VoIP Quality assessment for 120 phones, enter `120` in this field.

3. After you set up your report, you can generate it. For more information, see Section 8.2, "Generating an Executive Summary Report," on page 93 and Section 8.3, "Generating a Complete Report," on page 93.

8.2 Generating an Executive Summary Report

The Executive Summary Report provides a summary, with relevant charts and graphs, of the results that most directly affected the overall quality of voice over IP calls on your network.

Reports may take several minutes to compile and display. The fewer days and hours you filter out of the Executive Summary Report, the longer it takes.

To generate an Executive Summary Report:

1. Expand the **Report** view tab and click the **Generate** view tab.
2. Select **Executive Summary**.
3. Use the **Filter Results** fields to control the results that display in the report. You can choose to include only those assessment results that occurred during a specific range of hours or a specific range of days. To filter results, select **Include only results between these times** or **Include only results between these day**s, and then provide the appropriate time range.
4. Click **Generate Report**. The Executive Summary is generated in Microsoft Word. For more information, see Section 8.4, “Understanding Report Content,” on page 94.

8.3 Generating a Complete Report

The Complete Report provides information, charts, and graphs about every type of data collected during every day of the assessment.

The Complete Report is very comprehensive and may take several minutes to compile and display. Be aware that, depending on the number of devices and call groups in your assessment, the report could contain up to 300 pages. The fewer days, hours, and detail sections you filter out of the Complete Report, and the more devices and links you monitored and call groups you included in the VoIP Quality assessment, the longer it takes. Although filtering helps, in many cases, the Executive Summary Report provides more than enough information to determine a network’s ability to handle voice traffic.

To generate a Complete Report:

1. Expand the **Report** view tab and click the **Generate** view tab.
2. Select **Complete Report**.
3. Use the **Filter Results** fields to control the results that display in the report. You can choose to include only those assessment results that occurred during a specific range of hours or a specific range of days. To filter results, select **Include only results between these times** or **Include only results between these day**s, and then provide the appropriate time range. This option lets you see only the compiled results that apply to the days and hours considered significant to your organization.

   NOTE: The Filter Results option differs from the Filter Content option in a significant way: when you filter the results, you actually alter the data that appears in the report. For example, when you choose to show only the data gathered on weekdays, the results may not include a particular router’s poor performance during a weekend outage. Filtering the content, on the other hand, can exclude information without altering the data shown. You could, therefore, include the day of the week that the outage occurred but exclude detailed information about that particular router.

   ---

4. Use the Filter Content tree and tabs to control the sections of content that are included in the report.

You can apply more filtering to the report by excluding any content sections that are not applicable to your situation. Click the **Sections** tab and clear any box for a section you want to exclude from the report. Or check a box to include any section that is not included by default. The selections on the **Sections** tab correspond to the Table of Contents that will appear in the Complete Report.

For even more comprehensive filtering, click the **Details** tab and select the specific routers, switches, links, modeled links, and call groups that you want to exclude from or include in the report.

Filtering by device does not affect the results you see in measurement charts, which show results for all monitored devices or links. For example, if you clear the boxes next to every router except the one at Corporate Headquarters, the device details for all the excluded routers will be excluded, but their utilization statistics will still be included in the measurements shown in the charts.

5 Click **Generate Report**. The Complete Report is generated in Microsoft Word. For more information, see Section 8.4, “Understanding Report Content,” on page 94.

8.4 Understanding Report Content

Although the Executive Summary and the Complete VoIP Readiness Assessment reports contain introductory and explanatory text, the topics in this section provide a few helpful tips for understanding the various charts and tables, as well as the data and device readiness metrics you see.

8.4.1 Working with Microsoft Word and Excel

Vivinet Assessor invokes Microsoft Word and Excel to interact with the database and produce charts, graphs, and detailed explanations of the data in a formatted report. It may take some time to compile and generate a report, depending on the size of your assessment and the amount of data collected.

Although you can create your own custom reports by reading an assessment database using Microsoft SQL Server Management Studio Express, another option is to edit the Complete Report in Microsoft Word after it is generated, removing the sections you do not need from the Word document. For more information, see Section 10.1, “Using SQL Server Management Studio Express,” on page 117.

Configuring Microsoft Word Security Settings

Before generating a report in Microsoft Word, check your Word security settings. Vivinet Assessor cannot generate reports unless your settings allow templates from a trusted source.

To configure your security settings in Microsoft Word 2007 and later versions:

1 In Word, click the **Microsoft Office** button, and then click **Word Options**.

2 Click **Trust Center**, and then click **Trust Center Options**.

3 Select **Enable all macros**.

4 Click **OK**.

Configuring Date Formats

Reports automatically use the Windows date format configured on your computer. For example, if you selected one of the “Short Date Formats” for dates in your Windows Regional settings, Vivinet Assessor reports will show “15-Oct-02” or “15-10-02,” depending on which format you selected.

To change the format:

1. Navigate to the Control Panel and double-click **Regional Options**.
2. Click the **Date** tab. Click **Customize** on the Regional Options dialog box to see the **Date** tab.
3. Select **Short Date Format** or **Long Date Format** from the lists, and click **Apply**. But be aware that the “Long Date Formats” might not wrap neatly in most Excel data tables. To get “15-Oct-02,” select the **Short** format **dd-MMM-yy**.

Configuring Footers For Printing

If report footers are not printing correctly, the problem may be that your printer has a bottom edge requirement that is greater than the “From edge” setting for footers configured in the Microsoft Word report template. The template by default supplies a value for the “From edge: Footer” setting.

To prevent footers from being cut off by your printer:

1. From the report document, click **Page Setup** on the File menu.
2. On the Margins tab, find the **Footer** field and increase the value slightly.
3. In the **Apply To** list, select **Whole Document**.
4. Print a test page to make sure you increased the footer distance enough for your printer.

8.4.2 Readiness Ratings

During the Utilization assessment, Vivinet Assessor rates the VoIP readiness of individual monitored components. The VoIP readiness ratings Vivinet Assessor assigns are derived from result ranges you can configure, and they comprise four categories:

Category	Explanation
Good (green)	At least 99.00% of collected measurements rated Good. Component is voice-ready, or else device or call-quality statistics are within acceptable parameters.
Acceptable (yellow)	At least 98.00% of collected measurements rated Good or Acceptable. Reconfiguration or an upgrade is necessary to achieve voice compliance or good call quality.
Poor (red)	Any lower value. The device or link may not be ready to carry additional VoIP traffic.Component is not voice-ready, or else device or call-quality statistics are not within acceptable parameters.
Unavailable (black)	No results were available to report.

In the VoIP Readiness Assessment reports, the colors are assigned to routers, switches, and links based on the Utilization assessment. Note that they correspond to the colors that are used to report the Call Quality results of the VoIP Quality assessment. For more information, see Section 8.5, “Reviewing VoIP Quality Assessment Factors,” on page 98.

Readiness ratings are based on the result ranges you configured for Device and Link Readiness. For more information, see Section 7.8.1, “Setting Result Ranges,” on page 68.

8.4.3 VoIP Quality Charts

Just like jitter, delay, and lost data, call quality is measured in units. In the case of call quality, the units are points on the five-point Mean Opinion Score (MOS) scale. This means that in bar charts showing call quality, the line graph shows the average MOS of all calls made between the endpoints in a call group. And the bars are further broken down into call-quality mappings to show the percentage of all calls that were rated as having Good, Acceptable, and Poor quality or were Unavailable.

You can set the mappings for call quality and for all result metrics to determine how collected results translate into VoIP readiness ratings. For more information, see Section 7.8.1, “Setting Result Ranges,” on page 68.

On charts that break out specific impairment factors by day or by hour, a line graph of that factor’s values is superimposed over a bar graph. For example, a line graph of Lost Data Evaluation by Day gives you a quick overview of the lost data results averaged for each day of the assessment. The bars show what percentage of the lost data values fell into the Good, Acceptable, and Poor ranges.

For charts that show results broken out by hour of the day, it can be difficult to see all the values that extend to two decimal places. When you add all the values in a column, it can, therefore, appear that the values total only 99%. To see the full values, including the decimal places, double-click any chart to launch Microsoft Excel. You then have access to the spreadsheet containing your data.

8.4.4 Data Tables

In Vivinet Assessor reports, bar charts are paired with data tables so that you can quickly scan the results and see the specific values. Different colors in the bar charts provide an overview of the data, while the tables provide the specifics.

Most values shown are based on averages. For example, when you look at the charts that break out Call Quality by time of day (“Call Quality Evaluation by Hour,” for example), you seeing quality averages for all simulated calls that were sent over the network during a certain hour of the day over the course of the entire assessment.

8.4.5 Device and Link Availability

During the Utilization assessment, Vivinet Assessor sends out SNMP queries to the network devices and links you discovered during the Network Inventory to gather data on network utilization. Responses to these queries do not always make it back to the Console. For various reasons, including network congestion or link failure, the responses are lost, and Vivinet Assessor receives no data from a device or link during a polling period. This fact is recorded in the reports; the device or link is said to be “Unavailable,” and the measurement that could not be obtained is said to be “n/a” (not available).

In the VoIP Readiness Assessment reports, statistics on “Unavailable” measurements for devices and links are shown separately from the utilization measurements used to determine their readiness rating. Look at the Router Utilization Details chart in the Sample report for an example. For more information, see Section 12.6, “Sample Reports,” on page 132.

No readiness rating is given at all if a device was completely “Unavailable” during the assessment. The “Unavailable” results are shown separately within the table because they are not folded into the measurements for each device and link. After all, it is entirely possible that the devices in question never actually went down during the assessment, so no values were recorded in order to avoid

skewing the results. However, this method of reporting can in itself be misleading: keep in mind that the more frequently a device was “Unavailable” during polling intervals, the fewer samples were used to determine the results. Assuming, for example, that a certain switch was “Unavailable” for 90% of the polling intervals in the assessment, that switch’s “Good” readiness rating is not very impressive.

NOTE: Another reason for “Unavailable” results is that Vivinet Assessor cannot always get information about every utilization measurement from every device. Some device MIBs do not support certain utilization measurements.

You should investigate when a device or link has high unavailability.

8.4.6 Endpoint Availability

If endpoints were found to be “Unavailable” in the initial VoIP Quality Summary, generate the Complete Report to find out what went wrong. In the sections that recap the assessment of VoIP Quality, the Complete Report offers an Availability Summary that breaks out all availability issues into specific categories. This summary supplements the error information you can view in The Log Viewer.

The explanations listed in the table below may not cover all instances in which the endpoints return the specified error to the Console. Be sure to check the Log Viewer for the assessment and click the Help for Message button to find out more. For more information, see Section 11.5, “The Log Viewer,” on page 123.

An endpoint may be “Unavailable” due to any of the following errors, shown in the Availability Summary as percentages of all “Unavailable” endpoints The CHR# error messages you are likely to see are also indicated:

Error Type	Likely Explanation	Error Messages
Endpoint Unavailable	An endpoint was not installed, or was not started, or else the endpoint version does not support a requested function, such as QoS.	CHR0125 CHR0204
Network Connectivity	A network problem is preventing the Console from contacting the , or preventing the endpoints from contacting the Console. Or a network problem is preventing the endpoints from contacting each other.	CHR0200 CHR0201 CHR0202 CHR0225 CHR0142 CHR0144 CHR0373
Clock Sync	The endpoints in a call group were unable to synchronize their high-precision clocks. A firewall may have prevented clock-synchronization flows between the endpoints For more information, see Section 7.8.2, “Working with Firewalls,” on page 69.	CHR0371
Assessor Unavailable	The Console lost contact with the endpoints The Scheduler service may have gone down, or the Console computer may have been powered off. For more information, see Section 11.3, “Scheduler Errors,” on page 122.	CHR0372
Test Timeout	Calls were interrupted; Endpoint 2 was no longer receiving data sent by Endpoint 1 and notified the Console.	any other message

8.5 Reviewing VoIP Quality Assessment Factors

During the VoIP Quality assessment, Vivinet Assessor calculates Call Quality based on a set of factors known to affect the perceived quality of voice over IP transmissions. Just as device and link utilization is measured and rated for VoIP readiness, Call Quality is also rated, and the results of the ratings are broken out in detail in the final VoIP Readiness report.

A subjective factor is necessarily part of evaluating VoIP because a listener must be able to understand the received transmission, and both talkers must be able to tolerate the amount of delay between speaking and being heard (called “the walkie-talkie effect”), lost or fractured syllables, and echo that often impede the conversation.

To determine the relative quality of each simulated VoIP call made during a VoIP Quality assessment, Vivinet Assessor measures the following quality impairment factors:

- Section 8.5.1, “Mean Opinion Score,” on page 98
- Section 8.5.2, “Delay,” on page 100
- Section 8.5.3, “Jitter,” on page 101
- Section 8.5.4, “Jitter Buffers and Datagram Loss,” on page 101
- Section 8.5.5, “Lost Data,” on page 102
- Section 8.5.6, “Time Zone Considerations,” on page 102

Each factor is measured, and the results are evaluated for VoIP readiness. You can determine how any of these factors are rated by changing the result ranges for the VoIP Quality assessment. For more information, see Section 7.8.1, “Setting Result Ranges,” on page 68.

8.5.1 Mean Opinion Score

The chief unit of measurement for Call Quality in Vivinet Assessor VoIP Quality results is an estimated Mean Opinion Score, or MOS. The E-Model, ITU Standard G.107, quantifies what is essentially a subjective judgment: a user’s opinion of the perceived quality of a voice transmission. After much study, the ITU determined which impairment factors produced the strongest user perceptions of lower quality. The E-Model thus includes factors for equipment and impairments and takes into account typical users’ perceptions of voice transmissions affected by jitter, lost data, and delay.

In its calculations, Vivinet Assessor modifies the E-model slightly and adds three call quality categories, Good, Acceptable, and Poor, to help you determine how well VoIP performs on your network. You can change the way the categories are applied to conform to your own quality standards.

Readiness Assessment reports, however, also show how many calls could not be completed (“Unavailable” calls) and give you the objective measurements of lost data, jitter, and delay so that you can independently judge for yourself. See Section 11.2, “VoIP Quality Assessment Errors,” on page 122.

Vivinet Assessor uses a modified version of the ITU G.107 standard E-Model equation to calculate a Mean Opinion Score (MOS) estimate for each call group.

The E-Model, developed by the European Telecommunications Standards Institute (ETSI), has become ITU standard G.107. This algorithm is used to evaluate the quality of a transmission by factoring in the “mouth-to-ear” characteristics of a speech path. The output of an E-model calculation is a single scalar, the “R-value,” which is derived from voice quality impairment factors. The R-value output is then mapped to an estimated MOS.

In calculating the MOS, Vivinet Assessor modifies the E-model slightly, using the following factors:

Factor	Description
End-to-End Delay	Delayed datagrams are perhaps the single greatest hindrance to VoIP call quality. This value includes all network (or one-way) delay, packetization delay, and jitter buffer delay between the endpoints For more information, see Section 8.5.2, “Delay,” on page 100.
Jitter Buffer Loss	Jitter occurs when there are variations in datagram arrival times within a single transmission. When jitter exceeds jitter buffer capacity, datagram loss occurs, reducing call clarity. For more information see Section 8.5.3, “Jitter,” on page 101.
Lost Data	Datagrams that never arrived at the receiver. When a datagram is lost, you can lose an entire syllable, and the more datagrams that are lost consecutively, the more the clarity suffers. For more information, see Section 8.5.5, “Lost Data,” on page 102.

A MOS of 5 is excellent; a MOS of 1 is unacceptably poor. The following table (taken from ITU G.107) summarizes the relationship between the MOS and user satisfaction:

MOS (lower limit)	User Satisfaction
4.34	Very satisfied
4.03	Satisfied
3.60	Some users dissatisfied
3.10	Many users dissatisfied
2.58	Nearly all users dissatisfied

By default, Vivinet Assessor maps MOS estimates to the three readiness ratings categories as follows:

MOS Range	Score	Meaning
5.0 - 4.03	Good (green)	Most or nearly all users satisfied
4.02 - 3.60	Acceptable (yellow)	Some users satisfied
Below 3.60	Poor (red)	Most or nearly all users dissatisfied

If the MOS value calculated for a call group during an assessment is less than the maximum possible for the codec being used, the “Factors Affecting Call Quality” charts in the report will show which impairment factors contributed to the degradation in the MOS, and how much they contributed. Therefore, these tables provide rudimentary guidelines for improving call quality on your network.

8.5.2 Delay

The end-to-end delay, or latency, as measured between the endpoints is a key factor in determining VoIP call quality. Vivinet Assessor calculates the end-to-end delay for calls between the endpoints in a single direction by adding the following factors:

Delay Type	How Calculated
Network (or one-way) delay	Datagram's RTP timestamp subtracted from the time it was received by receiving endpoint. Includes: ◆ **propagation delay**: time spent on the actual network ◆ **transport delay**: time spent getting through intermediate network devices, such as routers and switches
Packetization delay	Fixed value; dependent on codec selected. For more information, see Section 7.11.2, “Reviewing Codec Types,” on page 78.
Jitter buffer delay	Fixed value; dependent on type and size of jitter buffer configured by user. For more information, see Section 7.11.6, “Understanding Jitter Buffers,” on page 80.
Additional fixed delay	Fixed value; user-configured. For more information, see Section 7.10.1, “Adding a Call Script,” on page 75.

There is a distinction between the delay *impairment factor* and the delay *statistic*. In charts reporting delay statistics, the calculations include all the factors shown in the table above. However, in charts showing call-quality impairment factors, the packetization delay is included in the Codec impairment value, not in the Delay impairment value.

Most callers notice round-trip delays in excess of 250 ms. ITU-T standard G.114 specifies 150 ms as the maximum one-way delay that is tolerable for high-quality VoIP, so you should consider these factors when determining your delay budget.

How Endpoints Calculate Delay

To provide a useful measurement of delay for VoIP, the endpoints in each call group must continuously synchronize their high-precision clocks. The endpoints maintain virtual (software) clocks for each partner involved in a VoIP test. These virtual clocks consist of the offset between the microsecond clocks maintained by the two endpoints

A high-resolution microsecond clock is maintained independently of the operating system’s system clock. The endpoints paired with each other in a call group compare their respective versions of the clocks prior to the start of each set of simulated calls and periodically during the calls. They also measure clock synchronization and drift between sets of calls to establish a track record for the expected delay. If an error occurs in this process, you will see error message **CHR0359**:

```
An error was detected in the high precision timer.
```

The Windows 98 and Windows Me operating systems do not support high-precision timing very well. You will see **CHR0384** if you try to use endpoints on these operating systems in your VoIP Quality assessment.

8.5.3 Jitter

As simulated calls run during a VoIP Quality assessment, the endpoints calculate jitter, a factor known to adversely affect call quality. Jitter is also called delay variation, and it indicates the differences in arrival times among all datagrams sent during a simulated voice over IP call.

When a datagram is sent, the sender (one of the) gives it a timestamp. When it is received, the receiver adds another timestamp. These two timestamps are used to calculate the datagram's transit time. If the transit times for datagrams within the same call are different, the call contains jitter. In a telephone call, the effects of jitter may be similar to the effects of packet loss: some words may be missing or garbled.

The amount of jitter in a call depends on the degree of difference between the datagrams' transit times. If the transit time for all datagrams is the same—no matter how long it took for the datagrams to arrive—the call contains no jitter. If the transit times differ slightly, the call contains some jitter. And if there is any jitter detected for a call, Vivinet Assessor measures jitter buffer loss as well.

Vivinet Assessor reports show jitter as an average. But to calculate call quality scores, it uses the statistic for datagrams lost due to the size of the jitter buffer ("jitter buffer loss") in the call script.

8.5.4 Jitter Buffers and Datagram Loss

VoIP equipment typically has a jitter buffer, either frame-based or absolute. A frame-based jitter buffer holds a given number of voice datagrams, whereas an absolute jitter buffer is based on time. They both smooth out VoIP network jitter. All call scripts used in VoIP Quality assessments by default emulate a frame-based jitter buffer of two datagrams. For more information, see Section 7.11.6, "Understanding Jitter Buffers," on page 80.

Although jitter buffers smooth out jitter by feeding datagrams to the application in a steady stream, they also exacerbate data loss: datagrams that are not contained by the jitter buffer are discarded. Thus, Vivinet Assessor's jitter buffer lost datagrams statistic includes:

- **jitter buffer overruns**—datagrams that had a delay variation greater than the jitter buffer size or were delayed too long. For example, a datagram with a delay of 50 ms would not be contained in a jitter buffer set to 40 ms. Or if five datagrams were delayed sequentially, an absolute jitter buffer set to two datagrams would discard three datagrams.
- **jitter buffer underruns**—datagrams that arrived too quickly while the jitter buffer was still full.

Jitter buffers may be static or dynamic. Each type of buffer has its strengths, but it is in the nature of IP networks to exact a trade-off. One assumption used in calculating call quality is that buffering not only causes loss, but also adds delay, which can offset the positive effects of smoothing out jitter.

In charts reporting jitter statistics, the calculations are based on jitter buffer loss, but the jitter average is also shown in the accompanying table. Similarly, in charts showing call-quality impairment factors, the jitter impairment factor reflects jitter buffer loss for the call scripts used.

When jitter is detected, jitter buffer loss totals are factored into the Mean Opinion Score estimate and also reported separately. You can determine what levels of jitter buffer loss are acceptable on your network by configuring result ranges. For more information, see Section 5.2, "Determining Assessment Result Ranges," on page 44.

Jitter buffer loss in excess of .5% of all datagrams sent in a call can adversely affect call quality.

8.5.5 Lost Data

In VoIP Readiness Assessment reports, Vivinet Assessor includes statistics on lost packets, expressed as a percentage of all data sent in the relevant calls. For example, in charts indicating lost data by call group, lost data is expressed as a percentage of all data sent between the endpoints in the call group over the course of the entire assessment. Other charts might show data loss as a percentage of data sent at a certain time of day, averaged over the course of all days in the assessment.

When a packet is lost during a VoIP transmission, you can lose an entire syllable or word in a conversation. Obviously, packet loss can severely impair call quality. Vivinet Assessor therefore includes data loss as a call quality impairment factor in calculating the MOS of each simulated VoIP call. Industry-wide, greater than 5% packet loss is considered a problem for VoIP.

To measure data loss, one computer in each call group keeps track of how many bytes of data it sent. The sending endpoint reports to the receiving endpoint how many bytes it sent, and the receiver compares that value to the amount received to determine lost data.

In Analysis Console, you can see values for Maximum Consecutive Datagram Loss, which is not included in the reports. Consecutive loss has a greater negative impact on call quality than simple datagram loss. Analysis Console also shows how many datagrams were received out of order over the course of the assessment. For more information, see Chapter 9, “Working with Analysis Console,” on page 105.

If you have packet loss concealment (PLC) enabled for the G.711 codecs, call quality will improve if any data is lost during the assessment. PLC may make the codec itself more expensive to manufacture, but it does not add delay or have other bad side-effects. The VoIP equipment you plan to purchase probably uses PLC, which has become an industry standard. For more information, see Section 7.11.2, “Reviewing Codec Types,” on page 78.

8.5.6 Time Zone Considerations

If you run a VoIP Quality assessment across various time zones, be aware that you will need to “translate” some of your results to understand the actual times they were recorded. Vivinet Assessor creates graphs and reports for all results in the Executive Summary or Complete Report as if they have occurred in the local time zone—the time zone where the Console is located.

Unless you take time zones into account, you may misinterpret some results. Here is an example:

VoIP quality may improve from noon to 1 PM for call groups located on the East Coast as data traffic on the network is reduced during the lunch hour. However, this same time slot on the West Coast (that is, 9 AM to 10 AM) is a likely to be a time of heavy traffic, and VoIP quality may be much lower for these call groups. Yet Vivinet Assessor reports will graph the 9 AM to 10 AM West Coast call groups in the same time slot as the 12 to 1 PM call groups on the East Coast. In graphs that show average quality broken out by time of day, be aware of the role that time zones are playing.

In addition, keep in mind that Vivinet Assessor is using the localization (date and time) settings of the operating system when it generates charts and graphs in Analysis Console, as well as reports. The Scheduler service also uses these settings. If you change the Windows default setting to **Automatically adjust clock for daylight saving changes** on the Console computer, you need to reboot the computer or restart the Scheduler service so that it will use the same settings. Otherwise, you may see a negative value for the “% complete” reading during Verification.

8.6 Reviewing Utilization Assessment Factors

To evaluate a network device or link's readiness to carry VoIP traffic, Vivinet Assessor places the measurements taken during Utilization monitoring into VoIP readiness ratings categories. You can determine how a measurement is rated by changing the result ranges for the Utilization assessment. For more information, see Section 5.2, "Determining Assessment Result Ranges," on page 44 and Section 8.4.2, "Readiness Ratings," on page 95.

The topics in this section define each measurement used to determine device and link readiness and discuss how these measurements are taken.

8.6.1 Router Measurements

To determine each router's VoIP readiness, Vivinet Assessor uses SNMP queries to take the following measurements. Each measurement is then rated according to the readiness ratings configured for the Utilization assessment. For more information, see Section 8.4.2, "Readiness Ratings," on page 95 and Section 5.2, "Determining Assessment Result Ranges," on page 44.

The Router Measurements section of the VoIP Readiness Assessment report provides the following information:

Measurement	Description
Average memory utilization	The total memory used, expressed as a percentage of memory capacity, averaged from all polling intervals.
Average CPU utilization	The average CPU utilization, expressed as a percentage of processor time, averaged from all polling intervals.
Buffer errors	The number of buffer errors (memory allocation failures) that occurred on the router, averaged from all polling intervals.
CRC errors	The number of cyclical redundancy check (CRC) errors that occurred on the router, averaged from all polling intervals. **NOTE:** Some vendors, including Nortel, do not break out interface errors to show CRC errors specifically. In these cases, the overall interface error count is substituted for this metric.
Input queue drops	The rate at which packets were dropped from a router input queue, expressed as a percentage of all packets that entered the router, averaged from all polling intervals.
Output queue drops	The rate at which packets were dropped from a router output queue, expressed as a percentage of all packets that exited the router, averaged from all polling intervals.

When Vivinet Assessor monitors routers, it gathers device statistics from each of a router's individual interfaces. For many metrics, the values it reports are derived from an average of all measurements, from all interfaces. For example, for input and output queue drops per hour and CRC errors, the measurements are taken from active interfaces and averaged for the entire router.

Equipment by different vendors gathers and reports on these statistics slightly differently in a few cases. For example, the CRC errors metric taken from routers actually reflects the overall interface error count for Nortel routers because these routers do not break out interface errors to show CRC errors specifically.

8.6.2 Switch Measurements

To determine each switch's VoIP readiness, Vivinet Assessor uses SNMP queries to take the following measurements. Each measurement is then rated according to the readiness ratings configured for the Utilization assessment. For more information, see Section 8.4.2, "Readiness Ratings," on page 95 and Section 5.2, "Determining Assessment Result Ranges," on page 44.

Some Nortel and Extreme switches do not provide the necessary MIB data for Utilization monitoring. Therefore, values from these switches show no data in the results.

The Switch Measurements section of the VoIP Readiness Assessment report provides the following information:

Measurement	Description
Average backplane utilization	The switch backplane utilization (expressed as a percentage of backplane bandwidth), averaged from all polling intervals.
Average CPU utilization	The CPU utilization (expressed as a percentage of processor time), averaged from all polling intervals.

8.6.3 Link Measurements

To determine each WAN or LAN link's VoIP readiness, Vivinet Assessor uses SNMP queries to take and average the following measurement. The average measurement is then rated according to the readiness ratings configured for the Utilization assessment. For more information, see Section 8.4.2, "Readiness Ratings," on page 95 and Section 5.2, "Determining Assessment Result Ranges," on page 44.

The Link Measurements section of the VoIP Readiness Assessment report provides one measurement:

Average bandwidth utilization

Bandwidth utilization on this link, expressed as a percentage of available bandwidth, or link capacity, averaged from all polling intervals.

9 Working with Analysis Console

Analysis Console lets you get a closer look at data from individual call groups or even individual calls. With Analysis Console, you can generate custom charts on demand for use in detailed reports.

Invoke Analysis Console by clicking the **Analyze and Chart Results** button in the Run view of the VoIP Quality assessment. It is available anytime you design and save an assessment of VoIP Quality.

The charts you create with Analysis Console can be saved or exported to the Windows Clipboard and pasted into other Microsoft applications, such as Word documents or PowerPoint presentations. You can use them to enhance the VoIP Readiness Assessment reports.

Running as a standalone application, Analysis Console helps you do more with the results you see in the Run view of the VoIP Quality assessment and in VoIP Readiness Assessment reports. With Analysis Console, you can:

- View results sorted by call group or by call time, if you collected timing records during the assessment.
- Orient your view of the data using real-time rotation, zooming, and panning.
- Re-order the data streams and apply colors within a chart to improve readability.
- Mix and match data and chart styles within a single chart.
- Detect when results breach a high or low threshold by creating static threshold indicators.
- Re-use chart data in other applications.

Analysis Console is divided into several panes, as shown in the illustration above. See the following topics for more information.

9.1 Results Pane

In the Results pane, the Results Table lets you analyze, sort, and group results from a VoIP Quality assessment, as well as select results for charting. You have two options for selecting the broad set of results that are shown in the table:

- View results from all call groups or from a particular call group by selecting that group from the **Call Groups** list.
- View results from all the calls that were simulated during the entire assessment, or the results from a single call that occurred at a particular time by selecting the time from the **Call Times** list.

Selecting a call time gives you access to a more granular level of data. You can only select a call time if you collected timing records during the VoIP Quality assessment. To collect timing records, select to run a **Single Set of Calls** in the Schedule view, or select **Collect timing records when running a series of calls**. For more information, see Section 7.8.4, “Setting Assessment Run Options,” on page 72.

You can further sort the results by clicking the various column headers. If you click the “Call Script” column header, for example, results in the table are rearranged to sort them by the associated call script. Group the results by clicking a column header and dragging it to the gray area above the table.

To add a metric to a chart:

1. Right-click the desired row of data and select **Add Measurement to Chart**.
2. Select the desired measurement from the list.
3. *To remove all the data streams* from the current chart and start over, right-click and select **Create New Chart with Measurement**. You are prompted to save or discard the current chart.
4. *To show actual values in the Results table measured to two decimal places*, select **Show results as average values**. For more information, see Section 7.8.1, “Setting Result Ranges,” on page 68.
5. *To show values in the Results table as VoIP Quality indicators* and the colors associated with the three readiness ratings categories—Good, Acceptable, or Poor—instead of the actual measurements, select **Show results as VoIP Quality indicators**. For more information, see Section 8.5.1, “Mean Opinion Score,” on page 98.
6. *To review how VoIP Quality was evaluated for this assessment*, click **View VoIP Quality Indicators Legend**. “Result ranges” determine how call performance measurements are mapped to VoIP quality ratings. For more information, see Section 7.8.1, “Setting Result Ranges,” on page 68.
7. *To restore the Results table to its default settings*, click **Clear Groupings and Filters**. By default, no results are excluded (filtered) from the table, and call groups are sorted by connector, in the order in which connectors were created.

9.2 Understanding the Results Table

The Results table not only provides a way to view, sort, and group the data you received from a VoIP Quality assessment. It also shows data that *is not* included in VoIP Readiness Assessment reports. Each tabbed view in the table contains a summary of the major statistics—those that figure directly in the MOS calculation—as well as a listing of the measurements used to derive the major statistics.

For example, when you click the **Lost Data Results** tab, you can find out whether data loss was in a random or a bursty pattern by looking at the “Maximum Consecutive Datagrams Lost” column. Or you can check whether a significant number of datagrams were received out of order.

The Results table lets you easily see which factors contributed to a particular call-quality problem and also helps you test possible remedies. Adding quality of service to network traffic is one example of such a remedy. If you add QoS settings to some of the call groups in the VoIP Quality assessment, you can later access Analysis Console to sort the results by QoS. Just click on the “QoS” column heading and drag it to the gray area just above the Results table to sort the results by QoS setting. Similarly, you can sort the results by codec (call script) by clicking and dragging the “Script” column heading.

When you view the values in the Results table as **Average Values**, you might notice some apparent discrepancies in the totals. For example, assume you ran a VoIP Quality assessment containing four call groups. Each call group was created by a VoIP connector that defined four simultaneous calls. Analysis Console lets you view averages per call if you drill down into details for a call group. Select the call group in the **Call Group Details** list above the Results table.

The Results table presents data for each of the simultaneous “calls” whose results were collected over the course of the entire assessment. Averages are shown per call and per call direction.

Click to view the results as **VoIP Quality indicators**. Position the mouse over an indicator to see whether any calls were “Unavailable.” If you see any Unavailable results, the per-call values will not be exact averages of the per-direction values. That is because to be included in the per-call averages, a call must be *complete*: it must have generated results *in both directions*. Results from

either direction may be unavailable. The per-direction averages include all results received for each direction. But unavailable results in one direction mean that the (available) results for the other direction are excluded from the per-call averages.

9.2.1 VoIP Results Tab

The VoIP Results tab summarizes the results from the VoIP Quality assessment. By default, results are sorted by lowest MOS to highest. More information about each of the VoIP performance metrics shown in the tab (delay, jitter, and lost data) is available in the following topics.

The following information is shown on the **VoIP Results** tab:

Column Name	Description
Endpoint 1/Endpoint 2	The endpoints in a call group. Endpoints are computers that initiated and received bi-directional, simulated VoIP calls during the assessment.
Script	The call script used to generate the simulated VoIP traffic between the endpoints. Corresponds to a popular VoIP codec type.
QoS	Quality of service setting used by the simulated VoIP traffic, if any. For more information, see Section 7.11.7, “Reviewing Quality of Service,” on page 81.
# Calls	The number of simulated calls that ran simultaneously between the endpoints in each call group. The **Call Multiplier** in the VoIP connector definition determines the number of calls.
Call Quality	The average Mean Opinion Score (MOS) estimate that a call group received over the course of the assessment. A score of 5.0 is the highest possible and is only theoretically achievable. By default, Vivinet Assessor assigns a VoIP readiness rating of "Good" to call groups with a MOS in the range of 5.0 to 4.03. For more information, see Section 8.5.1, “Mean Opinion Score,” on page 98.
End-to-End Delay (ms)	The average delay, or latency, measured between the endpoints in a call group from one end of the network to the other. Calculated by adding the network delay, packetization delay, jitter buffer delay, and additional fixed delay (if any was configured).
Jitter Buffer Loss (%)	Average data loss due to the jitter buffer configured in the call script, shown as a percentage of all data sent between the endpoints in a call group.
Lost Data (%)	Lost datagrams, expressed as a percentage of all data sent between the endpoints in a particular call group over the course of the entire assessment.
R-value	The output of an E-model calculation. The E-Model, ITU standard G.107, is an algorithm used to evaluate the quality of a voice transmission. The R-value is derived from voice quality impairment factors and mapped to an estimated Mean Opinion Score.
Throughput (kbps)	The average data rate achieved by the call traffic sent between the endpoints in a particular call group over the course of the VoIP Quality assessment.
Comment	Identifies the VoIP connector. By default, consists of the following information: `Call script name: Endpoint 1 name - Endpoint 2 name Call multiplier`.

9.2.2 Delay Results Tab

The Delay Results tab summarizes the delay results from the VoIP Quality assessment. By default, results are sorted by lowest MOS to highest. For more information, see Section 8.5.2, “Delay,” on page 100.

See Section 9.2.1, “VoIP Results Tab,” on page 107 for definitions of the “Endpoint,” “Script,” “QoS,” “Call Quality,” and “Comment” columns on the Delay Results tab. The following measurements are also shown:

Column Name	Description
End-to-End Delay (ms)	The average delay, or latency, measured between the endpoints in a call group from one end of the network to the other. Calculated by adding the network delay, packetization delay, jitter buffer delay, and additional fixed delay (if any was configured).
Network Delay (ms)	Also referred to as "one-way delay." A datagram's RTP timestamp (signifying the time it was sent by the sending endpoint), subtracted from the time it was received by the receiving endpoint. Includes both of the following: ◆ **propagation delay**—time spent on the actual network ◆ **transport delay**—time spent getting through intermediate network devices. must synchronize their high-precision clocks to calculate network delay. For more information, see “How Endpoints Calculate Delay” on page 100.
Estimated Clock Error (ms)	An estimate of the maximum discrepancy between the synchronized high-precision clocks on the endpoint computers used to measure network (one-way) delay. Add the estimated clock error to and subtract it from the network delay measurement to yield an upper and lower bound for the actual network delay. **NOTE:** The estimated clock error can be unexpectedly large for any of the following reasons: ◆ The endpoints just synchronized their clocks for the first time (as in a quick quality check with a single set of simulated calls). Therefore, insufficient information has been gathered to calculate an accurate estimated clock error. A conservatively large estimated clock error is shown instead. ◆ During clock synchronization, network conditions changed such that data flowed between the endpoints significantly more rapidly in one direction than in the other. Accurate clock synchronization requires a symmetric connection between , where data is sent with equal speed in both directions. ◆ One or both of the endpoints was busy with other processing during clock synchronization.

9.2.3 Jitter Results Tab

The Jitter Results tab summarizes the delay results from the VoIP Quality assessment. By default, results are sorted by lowest MOS to highest. For more information, see Section 8.5.3, “Jitter,” on page 101 and Section 8.5.4, “Jitter Buffers and Datagram Loss,” on page 101.

See Section 9.2.1, “VoIP Results Tab,” on page 107 for definitions of the “Endpoint,” “Script,” “QoS,” “Call Quality,” and “Comment” columns on the Jitter Results tab. The following measurements are also shown:

Column Name	Description
Jitter Buffer Loss (%)	Average data loss due to the jitter buffer configured in the call script, shown as a percentage of all data sent between the endpoints in a call group. Includes the following totals: ◆ jitter buffer overruns—datagrams with a delay variation (jitter) greater than the jitter buffer size or were delayed too long. ◆ jitter buffer underruns—datagrams that arrived too quickly while the jitter buffer was still full.
Jitter (ms)	The average jitter, or delay variation, measured between the endpoints over the course of the VoIP Quality assessment. Shows the differences in arrival times among all datagrams sent between these endpoints
Max. Jitter (ms)	The maximum jitter, or delay variation, measured between the endpoints during the VoIP Quality assessment.

9.2.4 Lost Data Results Tab

The Lost Data Results tab summarizes the delay results from the VoIP Quality assessment. By default, results are sorted by lowest MOS to highest. For more information, see Section 8.5.5, “Lost Data,” on page 102.

See Section 9.2.1, “VoIP Results Tab,” on page 107 for definitions of the “Endpoint,” “Script,” “QoS,” “Call Quality,” and “Comment” columns on the Lost Data Results tab. The following measurements are also shown:

Column Name	Description
Lost Data (%)	The average amount of data lost between the endpoints during a set of simulated calls. Expressed as a percentage of all datagrams sent.
Max. Cons. Datagrams Lost	The maximum number of datagrams lost consecutively. The RTP header includes sequencing information to help the receiver reconstruct the transmission. The endpoints can use this information to measure consecutive datagram loss.
Datagrams Lost	The number of datagrams lost between the endpoints during a set of simulated calls.
Datagrams Out of Order	The number of datagrams received out of order during each set of simulated calls.

9.2.5 Endpoint Configuration Tab

The Endpoint Configuration tab identifies each endpoint used in the VoIP Quality assessment and provides the following information:

Column Name	Description
Name	The domain name assigned to the endpoint computer.
Version	The version of the Performance Endpoint software.
Build Level	The build number of the Performance Endpoint software.
Operating System	The operating system of the endpoint computer.
OS Version Major	Operating system version.
OS Version Minor	The revision of the operating system.
CSD Level	Service-pack information for the operating system installed on the endpoint computer.
Memory	Total amount of random-access memory (RAM), in kilobytes, on the endpoint computer (not the available RAM).

For more information, see Section 1.4, “NetIQ Performance Endpoints,” on page 12.

9.2.6 Background Traffic Tab

The Background Traffic tab summarizes the results from any background traffic that ran during the VoIP Quality assessment. For more information, see Section 7.11.1, “Understanding Background Traffic,” on page 78.

See Section 9.2.1, “VoIP Results Tab,” on page 107 for definitions of the “Endpoint” and “Comment” columns on the Background Traffic tab. The following measurements are also shown:

Column Name	Description
Configured Data Rate	The data rate selected when the Background Traffic connector was created. Default is 28.8 kbps (modem).
Actual Data Rate (kbps)	The throughput for TCP traffic that was measured during the assessment.

9.3 Chart Tree

The lower-left pane of Analysis Console contains the Chart Tree, which lists all charts that have been saved for an assessment. Any Analysis Console instance is always associated with a single saved VoIP Readiness assessment.

The first charts listed in the Chart Tree are *chart starters*: pre-defined charts of particular performance metrics, such as Jitter Buffer Loss. You can add other data streams to these charts, including other types of measurements (such as Lost Data) and measurements from other call groups. It is a good idea to make your charts based on chart starters, which perform a lot of the work involved in creating a chart.

Chart starters define parameters and build a chart from them. For example, the “Call Quality for Worst 5 Call Groups” chart starter builds a chart that shows key performance metrics from the five call groups with the lowest call quality scores. Double-click any chart starter in the Chart Tree to generate a chart.

Just below the list of pre-defined charts, charts you already generated and saved appear under the heading “Your Charts.” Double-click any saved chart to view it.

When you save a chart, you are saving the chart parameters, such as which call groups to include and which data streams to chart. You are not, however, saving the data, which is dynamically taken from the assessment database. If you run an assessment again after saving a chart, the next time you look at that chart, it reflects data from the current assessment run, not from the initial run.

9.4 Working with Charts

When you create a chart, either by double-clicking a chart starter or selecting a measurement in the Results table, by default you see only a chart of the entire series of calls that ran during the VoIP Quality assessment. That chart is displayed on the **Series Summary** tab, as shown below:

To see a chart of a selected set of calls, select a time from the **Call Time** list at the top of the Analysis Console window. Or double-click a data point on the chart to open the Graph Data Details dialog box. Then click the **View Call Details** button. A red, vertical Call Time indicator appears on the original chart of the call series.

In addition, the **Call Details** tab is displayed. Click the **Call Details** tab to see detailed information about the calls that ran on the network at the time you selected.

NOTE

- Call details are available only if you collected timing records during the assessment. With new assessments, timing records are collected by default. For more information, see Section 7.8.4, “Setting Assessment Run Options,” on page 72.
- Assessments with large numbers of simulated calls will take longer to process, and Analysis Console may slow down. Charting of metrics may take two or more minutes, depending on the amount of data being processed.

Right-click the chart and select **Show aggregation** to display the following fields beneath the chart (and above the legend):

- **Aggregate**—Allows you to combine data points into larger time segments. For example, if you select **12 hours**, the chart shows one data point for each 12-hour period of the assessment. The value shown is the averaged—aggregated—values that went into that 12-hour bucket.
- **Fit data to window**—When checked, all the data is made to fit in one chart window. When cleared, some data points are shown within the first window, while others require scrolling to be seen. When cleared, the number of data points shown at once is controlled by the Point Density chart property. Change the point density by right-clicking the chart and choosing **Properties**. Move the **Point Density** slider to the left to show fewer points per window, to the right to show more.

9.4.1 Reviewing the Chart Legend

By default, a legend is displayed beneath a chart in Analysis Console.

The following table describes the legend components and indicates how, or whether, they can be customized:

Component	Description
Last Value	The last value recorded in the assessment database for this metric.
Scale	A scaling factor. When applied to a data stream, this factor multiplies all the values (for example, by 10, 100, .1, etc.) to bring them into the same range as a selected measurement (Lost Data %, for example). Change the scaling factor by right-clicking the chart and selecting **Data Streams** on the Properties menu. Then enter a value in the **Scale** field.
Interval	The approximate number of seconds or minutes between data points in the data stream. Due to variations in the length of timing records, this is an approximation of the interval between most of the data points.
Points	The number of data points charted for this metric.

If you do not want to see the chart legend, right-click the chart and select **Show legend**. This option is a toggle. Repeat the step to reveal the legend.

9.4.2 Understanding Data Streams

The building blocks of an assessment database are called data points. Data points represent single units of numeric data—the individual measurement—collected during a VoIP Quality assessment.

A series of these data points, collected while a VoIP Quality assessment runs and summarized in the Analysis Console Results pane, is called a data stream. Data streams represent averaged results, usually from multiple simulated VoIP calls. Once they are selected for charting, they are plotted over time.

NOTE: For a couple of measurements—maximum jitter and maximum consecutive datagrams lost—the results are not averaged. Instead, the maximum value is used.

To place a data stream in a chart, select a table cell that contains data. Right-click and select **Add Selected Measurement to Chart**. Although there is no true limit to the number of data streams that can be added to a single chart, the practical limit is about 20 because above that number, the colors representing individual data streams become more or less indistinguishable.

The actual measurement that a single data point represents was collected by the endpoints and sent over the network to the Vivinet Assessor Console, which stored it in the assessment database. Endpoints collect and send data using timing records. A single timing record does not necessarily become a single data point in Analysis Console, however. Assessment results may be collected either from a single set of simulated calls (a quick quality check) or from a series of simulated calls sent over the course of a scheduled assessment. And the endpoints send data in two directions, so their timing records are averaged.

Data points may represent a set of timing records whose results have been averaged. Or you can also choose to collect more granular data. On the Run Options tab, select **Collect call details (timing records) when running a series of calls**. By default, this selection is enabled for all new assessments.

The Run Options tab also gives you the option to control the size of timing records. Changing the default setting is recommended only for advanced users. By default, a new timing record is generated every five seconds. For more information, see Section 7.8.4, “Setting Assessment Run Options,” on page 72.

If you double-click a selected data stream in a chart, the Graph Data Details dialog box is displayed. When accessed from the Series Summary tab, the Graph Data Details dialog box includes a button labeled **View Call Details**. Click the button to switch to the Call Details tab and see detailed data about a selected call instead of viewing averaged results for the series.

For more information, see Section 9.2, “Understanding the Results Table,” on page 106.

9.4.3 Changing Chart Properties

Change the appearance of a chart or add information such as screentips to a chart by changing the Chart Properties. The options on the General, Colors, and Data Streams tabs of the Chart Properties dialog box let you change chart attributes such as frame rate, graphical style and color scheme, threshold values and colors, and dates and times for which data is displayed.

To change the properties of a chart:

1. Right-click a chart and select **Properties**.
2. To determine properties for your chart that include the type of perspective from which to display it, the maximum value for the y axis, CPU usage, and data stream settings, click the **General** tab. Complete the fields as described in the following table:

Field	Description
View	**Perspective**: Select to render the chart in perspective. The foremost data stream appears larger than the last one in the chart. **Parallel**: Select to render the chart in parallel mode. All data streams in the chart have the same size relative to value.
Performance > Frame Rate: (CPU Usage)	Determines the amount of CPU time devoted to interactive chart rendering (rotating, zooming, panning, scrolling). A low frame rate is less fluid, but uses less CPU time. A high frame rate offers the best visual performance, but uses 100% of the CPU.

Field	Description
Vertical Maximum	**Auto**: Select to automatically set the maximum value of the y axis of the grid to a value greater than the highest data point rendered. **Manual**: Select to manually set a maximum value for the y axis of the grid.
Wireframe when rotating, zooming and panning	Select to render the chart in wireframe when rotating, zooming or panning. This option conserves CPU resources.
ScreenTips for data points	Select to display a ScreenTip when you rest the cursor over a data point.
Data stream settings	**Depth**: Move the slider to adjust the depth of each data stream along the z axis. **Point Density**: Move the slider to adjust the density of data points along the x axis.

3 To determine the color scheme for your chart, click the **Colors** tab. Complete the fields as described in the following table:

Field	Description
Scheme	Choose a defined color scheme from the list.
Save As	Click to save the currently-defined color scheme under a unique name.
Delete	Click to delete the current color scheme.
Colors	**Title**: Select a color for the chart title as it appears in the Chart pane. **Grid Lines**: Select a color for the grid lines in the 3-D grid. **Grid Panels**: Select a color for the sides and bottom of the 3-D grid. **Time Scale**: Select a color for the numbers in the time line along the x axis. **Left Scale**: Select a color for the numbers along the left y axis of the 3-D grid.y **Right Scale**: Select a color for the numbers along the right y axis of the 3-D grid. **Background**: Select a background color for the Chart pane. **Gradient**: Select this option to create a gradient for the background of the Chart pane. Select a color for the bottom of the gradient. The color you selected for Background serves as the top color in the gradient. **Data Gap**: This option fills in missing points in a data stream rendered with the Area option (a chart style; see the **Data Streams** tab). If data is unavailable for some period during the assessment, the gap in points is filled in. Select a color for the area of missing points. **Data Stream Colors**: Click to open the Data Stream Colors dialog box. Use this dialog box to determine which color is applied to each data stream in a chart.
Solid Grid	Select this option to render the 3-D grid as a solid object.
Show Left Values	Select this option to display the values along the y axis on the left side of the 3-D grid.

Field	Description
Show Right Values	Select this option to display the values along the y axis on the right side of the 3D grid.

4 To set style, scale, and threshold settings for the data streams in your chart, click the **Data Streams** tab. Complete the fields as described in the following table:

Field	Description
Stream	Select a data stream from the chart to which you will make changes. Streams correspond to call groups that have data.
Style	Select the visual style of the data stream: ◆ Area ◆ Bar ◆ Cylinder ◆ Line ◆ Ribbon
Scale	Select a scale for the data stream. The data stream scales in the y axis relative to its original scale of 1.0. The grid is not affected.
Thresholds > Add	◆ Click to open the Threshold dialog box. Threshold applies to: ◆ **This data stream only**: The threshold indicator appears only along the selected data stream. ◆ **Entire chart**: The threshold indicator appears along all data streams. ◆ **Value**: Threshold limit.**Warning color**: Color of the threshold indicator. ◆ **Threshold is active**: Select this option to activate the threshold.
High Thresholds > Modify	Select a defined threshold. Click **Modify** to open the Threshold dialog box. Edit any parameters.
High Thresholds > Delete	Select a defined threshold. Click **Delete** to delete the threshold.
Other information	The SQL query used to retrieve the data stream.

9.4.4 Exporting Charts

The charts you create, edit, and save can be exported to the Windows Clipboard, to an XML file, or as HTML files in a report format.

Exporting a chart to the Clipboard is the easiest way to insert a chart into one of the Vivinet Assessor VoIP Readiness Assessment reports, which are in Microsoft Word format.

To export a chart to the Clipboard:

1 Right-click a chart and select **Export > Image to Clipboard**.

2 In Microsoft Word, click **Paste** on the Edit menu to paste the image into a Word document.

To export a chart as an image file in .png format:

1. Right-click a chart and select **Export > Image to File**.
2. Supply a filename and folder location.

To export a chart as an HTML file:

1. Right-click a chart and select **Export > Report to HTML**. The HTML Report wizard starts.
2. In the Report Type dialog box, choose to export both the chart and the data reflected in it, the chart alone as a .png (image) file, or the chart data only, formatted as a table in HTML.

   Use the **Include the following data streams list** to exclude any previously charted data streams from the exported report.
3. Click **Next**.
4. In the Report Title dialog box, check or change the **Report title** to be used for the exported report. You can also choose a **Chart color scheme**. The default setting has a white background. The color-scheme choices are the same as those you can select in the Chart Properties dialog box. For more information, see Section 9.4.3, “Changing Chart Properties,” on page 113.
5. Click **Finish**. Provide a **Save in** location and a **File name**, and then click **Save**. To maintain its formatting and keep the text and image files together, the exported report is placed in a folder of the same name as the selected file name.

10 Working with the SQL Database

Vivinet Assessor saves assessment definitions (all your configuration choices from the Design view, the schedule you selected, and any Assessment Options), any results associated with assessments you have run, plus any error information, in a SQL database system. The SQL service is installed with the instance name VASSESSOR.

The name you assigned to an assessment when you saved it identifies each assessment within the SQL database system, but assessments are not also saved in separate files that you can readily access, e-mail to coworkers, or move to other locations. Each assessment is instead stored as a separate database within the system.

However, Vivinet Assessor offers several features that help you manipulate your data, use existing assessments as templates for future assessments, export scripts and assessments—with or without results—into files that can be e-mailed or otherwise transported, and delete individual assessments.

10.1 Using SQL Server Management Studio Express

The Vivinet Assessor database is fully compatible with Microsoft SQL Server Management Studio Express (SSMSE), which means you can view and manipulate the data from an assessment.

SSMSE is a graphical management tool for managing SQL Server 2014. It is available free from the following location:

https://www.microsoft.com/en-in/download/details.aspx?id=30438

For more information about using SSMSE, see https://technet.microsoft.com/en-us/library/ms365247(v=sql.105).aspx.

10.2 Changing the Location of Your Assessment

If you want to save assessments to a different location (if, for example, you do not have enough disk space on the drive you were using), you can choose where the SQL database system writes (saves) assessment information.

To change assessment locations:

1. In the Vivinet Assessor Console, click **Assessment Location** on the Options menu.
2. Clear **Use default location** and then click **Browse** to select a new location. The new location you select must be a local, fixed drive and not a network drive, a CD drive, or a floppy disk drive. To distribute assessments to locations other than fixed, local drives, see Section 10.3, “Exporting and Importing Assessments, Scripts, and Definitions,” on page 118.
3. Click **OK**.

From now on, any new assessments you create or import will be saved to the new location. However, existing assessments will not be moved to this location. To save an existing assessment to a new location, first follow the steps above to change locations. Then open the assessment and click **File > Save As**.

NOTE: Clicking **Save As** will not let you copy an existing assessment to a new location unless you also give the assessment a new name. You should then delete the old assessment by clicking **Delete** on the File menu.

10.3 Exporting and Importing Assessments, Scripts, and Definitions

You can distribute assessments, assessment configurations, and call scripts by exporting and then importing them into different Vivinet Assessor Consoles or into different assessments. You can export and import the following:

Export Option	Description
Complete Assessment	An entire assessment, including any results or errors logged.
Assessment Definition	An assessment, excluding results or errors.
Script	A script, including any optional parameters selected.

NOTE

- If an assessment or script you import is marked as read-only, the SQL database system will cause the import operation to fail. Therefore, if you plan to distribute assessments or call scripts on a CD, you must first copy them to a local drive and change their properties to make them writable before you try to import them.
- Ensure the directory to which you are exporting the assessment or script allows the System account to have write access. Otherwise, you will receive an error message. The SQL server service, which runs under the System account, must be able to write the exported file to the target directory.

10.3.1 Working with Assessments

Suppose you want to use an existing assessment as a template for future assessments. You export an assessment definition, transfer the file to another computer if desired, and then import it, into another copy of Vivinet Assessor, for example. You can also use the following procedure to export an entire assessment.

To export an assessment or an assessment definition:

1. Open the assessment you want to export and make sure it is not running or verifying. The assessment cannot be active during the export.
2. On the File menu, click **Export** and then click **Complete Assessment** or **Assessment Definition**.
3. In the Save As dialog box, supply the name you want to assign to the exported file.
4. Browse to the location where Vivinet Assessor will save the exported file.
5. Click **OK**.

After the export is complete, you can move, or import, the exported file anywhere you like, including to another computer. The exported file has the extension `.AEF`.

Vivinet Assessor does not allow you to overwrite an existing assessment if that assessment is active. When you import an assessment definition, the status of the assessment will be changed back to “Ready to verify” if the status was “Completed,” “Running,” “Stopped,” or “Stopped with Errors.” Any results are lost.

Before you can import an .aef file, the Group or user names field on the Security tab for the file must contain permission for Network Service. You need to give this permission for each .AEF file individually, even if the file is located in a directory that already has permission given to Network Service.

To set up Network Service permissions and import an .aef file:

1. Right-click the assessment and select Properties.
2. On the Security tab, click Add.
3. In the Object Name field, type Network Service.
4. Click OK.
5. Click OK and continue with your import.
6. On the File menu, click **Import**.
7. In the **Look in** field, enter the location where you saved the exported assessment definition, or click **Browse** to find the exported file.
8. In the **Import as assessment name** field, supply a name for the imported file. Or choose the name of an existing assessment from the list.
9. Click **OK**.
10. If you import a file with the name of an existing assessment, you are asked whether you want to overwrite the existing assessment. Click **Yes**.

10.3.2 Working with Call Scripts and Definitions

Vivinet Assessor exports all the call scripts and QoS definitions in the source assessment. You cannot overwrite only a selected script or definition in the destination assessment when you import the scripts or definitions you exported.

To export call scripts or QoS definitions:

1. Open the assessment that uses the call scripts or QoS definitions you want to export.
2. On the Options menu, click **Call Scripts** or **Options**, and then select **Export**.
3. In the Save As dialog box, supply the name you want to assign to the script or definition file once it is exported.
4. Browse to the location where Vivinet Assessor will save the exported file.
5. Click **OK**.

When the export operation is complete, you can move the exported file anywhere you want. However, bear in mind that it can only be imported from a local, fixed drive.

To import call scripts or QoS definitions:

1. From the assessment into which you want to import the scripts or definitions, click **Call Scripts** or **QoS Definitions** on the Options menu, and then select **Import**.
2. In the Import dialog box, enter the location where you saved the exported script file, or click **Browse** to find the exported file.
3. Click **OK**.

11 Troubleshooting

The topics in this chapter provide guidance if you experience difficulties working with Vivinet Assessor.

For problems generating and printing reports using Microsoft Excel and Word, see Section 8.4.1, “Working with Microsoft Word and Excel,” on page 94.

11.1 Verification Errors

If errors occur during verification, a red Error symbol, plus a number indicating the number of verification calls that experienced an error, appear in the **Errors** column of the table in the Assess VoIP Quality - Run view.

A yellow Warning indicator appears when an endpoint reports a warning, such as **CHR0384**, which informs you that one of the endpoint operating systems may not yield the most accurate results. This warning probably means that one of the endpoints in the call group is running on Windows Me. Select another endpoint—one that is running a different supported operating system.

NOTE: The Warning indicator is shown only once because it applies to an unchanging condition. You see the Warning indicator in the Errors column only if no errors have been reported for the call group.

Always click **View Error Log** if you see an Error or Warning indicator during verification. The Log Viewer not only tells you why you received the message, but it also advises you how to correct the problem and avoid the message at the next verification. Click **Details** in the Log Viewer to see a detailed explanation of the highlighted message. Then click **Help for Message** to see what action you should take to correct the problem. To view only the errors reported by a single call group, highlight that call group in the table, right-click, and select **View Error Log for this Call Group**.

There is no need to start over with a new assessment if you receive verification errors. On the View menu, click **Assess VoIP Quality** and **Design** to return to the Design view and edit your assessment. Double-click on any endpoint or connector to edit it. Or, in the Run view, highlight the call group that has the error symbol. Right-click, and select **Show Connector in Design** to go straight to that call group in the Design view.

The most common errors you are likely to encounter occur when you have not correctly configured your SNMP community string information. The Network Inventory and Utilization assessments cannot proceed without this information. For more information, see Section 3.1.1, “Editing SNMP Configuration Information,” on page 26.

Other common errors associated with the VoIP Quality assessment occur because the endpoint software is not installed, or is installed improperly. If this is the case, during verification you will see the error **CHR0200**: “`The TCP connection attempt timed out.`,” or **CHR0204**: “`No partner program is waiting to accept this TCP sockets connection.`” The pie graph in the Verify view should show a black portion to indicate that these endpoints were “Unavailable.”

If you see either of these errors, check the endpoint computers included in the assessment and make sure the endpoint software is installed and running. The endpoint documentation includes advice for checking to make sure the endpoint is running and for restarting it, if necessary.

11.2 VoIP Quality Assessment Errors

Certain types of errors that occur during a VoIP Quality assessment are no real cause for concern. For example, Vivinet Assessor may detect an error in one of the endpoint computers' high-precision timers and generate error **CHR0359**. If you see this error while the assessment is running, there is no need to stop the assessment because the error will not invalidate your results. If you see the error during verification, simply run the verification again.

A lack of *endpoint availability* is a common source of errors and can occur if network links go down, if the endpoint software is improperly installed, or if the software or the computer where it is installed is no longer running.

Other types of errors that commonly occur will invalidate or impede the VoIP Quality assessment. When one of the endpoints is powered off during the assessment period, your results will show **CHR0200**. A few examples of this problem over the course of a seven-day assessment will not invalidate the assessment, but obviously, as long as the target computer is inactive, you are not logging any results for that call group. If you see error **CHR0125** while an assessment is running, you should stop the assessment. An endpoint you included in the Design is an older endpoint version and does not support VoIP Quality assessments. Take one of the following steps:

- From the table in the Run view, right-click over the call group that shows the error and select **Show Connector in Design** to jump to that endpoint. Change the Design to exclude it.
- Install the latest version of the endpoint software on the affected computer.

When you receive an error, you should always check the Log Viewer and read the error details, which provide detailed Help for each error message. Click **View Error Log** to find out more about the error. For more information, see Section 11.5, "The Log Viewer," on page 123.

11.3 Scheduler Errors

The Vivinet Assessor Scheduler service is described in detail in Section 2.2.4, "Vivinet Assessor Scheduler Service," on page 22. It is the component responsible for initializing and running assessments. If you receive an error from the Console that says the Scheduler needs to be started, first check to make sure it is started. Try to verify an assessment; if it verifies, the Scheduler is running.

Most Scheduler errors simply require you to stop and restart the Scheduler service. First, make sure no assessments are running. Then do the following:

From a command prompt in the Vivinet Assessor root directory, enter

`net stop netiqvivinetassessor` (to stop the service)
`net start netiqvivinetassessor` (to start it)

Or take the following steps:

1. Navigate to the Control Panel and double-click **Administrative Tools**.
2. Double-click **Administrative Services** and select **NetIQ Vivinet Assessor**.
3. Click **Restart** on the Actions menu.

The Scheduler logs any errors that occur to the `ASSESSOR.log` file in the `Micro Focus\Vivinet Assessor` directory. To read this log file, use the command-line program `FMTLOG.exe`. For more information, see Section 11.4, "Formatting Error Logs," on page 123.

NOTE: The Scheduler also writes information about Scheduler errors to the Application Log of the System Event Viewer. In the Scheduler error message window, click **View Event Logs** and then click **Application Log**.

11.4 Formatting Error Logs

Whenever the Vivinet Assessor application encounters a problem, the Scheduler logs the problem information to an error log file, `assessor.log`, at the Console. Similarly, whenever one of the endpoint programs encounters a problem it cannot report to the Console, it logs that problem to an error log file at the endpoint, `endpoint.log`, in the endpoint's directory.

To view the Console error log, you can use the Log Viewer. To view any error log, you can use the command-line program named `FMTLOG`, which is installed in the root directory where you installed Vivinet Assessor. For more information, see Section 11.5, "The Log Viewer," on page 123.

The program `FMTLOG` reads from a binary log file, and writes its formatted output to stdout. Here is the syntax of the `FMTLOG` command:

```
FMTLOG log_filename >output_file
```

The `FMTLOG` program is installed by default in the `\Program Files\Micro Focus\Vivinet Assessor` folder and is also installed at the endpoints For more information, see the *Performance Endpoints* guide included in the Vivinet Assessor documentation set.

11.5 The Log Viewer

Whenever the Console or one of the endpoint programs encounters a problem, error informationis logged into the Vivinet Assessor database. When errors have occurred, the **View Error Log** button is enabled and an error symbol appears in the Results table.

Use the Log Viewer to read and organize the error information. To open the Log Viewer, click the **View Error Log** button.

The Log Viewer shows the record number of the entry, the date and time, the source of the error and a brief description of the error.

An error log for an assessment or verification is not saved to disk as a separate file. Instead, it is immediately committed to the database. Errors in the log are usually detected or caused by the endpoints. Errors caused by problems with the Scheduler service are handled slightly differently. For more information, see Section 11.3, "Scheduler Errors," on page 122.

The Log Viewer is available only if errors occurred during the present verification or run. Any errors that occurred during a previous verification or run are erased when an assessment is verified or run for a second time.

You can select the criteria for the entries that you want to view. For more information, see Section 11.5.3, "Filtering Log Entries," on page 125. You can also choose to see the entire error log for a VoIP Quality assessment, or the errors that occurred for a particular call group. To see the entire error log, click the **View Error Log** button. To see the error log for a single call group, highlight the group name in the Call Groups table. Right-click, and select **View Error Log for this Call Group**.

11.5.1 Reviewing an Error Log

Click **Error Log** on the View menu or click **View Error Log** to review the entries shown in the Log Viewer to determine why errors occurred during assessment verification or while an assessment was running. Click any column heading to sort the entries by that column. By default, entries are sorted by record number.

Error Log Component	Description
Record	Shows the order in which errors were detected. Record numbers do not change when sorting or filtering is applied.
Date/Time	The date and time the error was detected.
Detected by	The component that detected the error: either the Console or the endpoints
Call group	The endpoints in the call group. Endpoint 1 is listed first.
Description	Briefly describes the error.
Details button	Accesses detailed information about each error. The Log Details dialog box lets you scroll between error messages in the Log Viewer and also gives you access to Help for each message to help you avoid it in the future.
Filter button	Lets you determine which error messages are shown in the Log Viewer. For more information, see Section 11.5.3, “Filtering Log Entries,” on page 125.
Find button	Helps you find a specific string in the Log Details dialog box. Highlights the record containing the string. You can double-click the highlighted record to view the details.
Refresh button	Refreshes the Log Viewer dialog box with any errors that have been detected since you opened the dialog box.

11.5.2 Viewing Error Details

To get more information about an entry in the Log Viewer, highlight the entry and click **Details**. The Log Details dialog box shows detailed information about the selected entry.

Log Details Component	Description
Help for Message	Provides more information about the error, including the steps you can take to avoid it.
Close	Closes the Log Details dialog box and returns to the Log Viewer.
Next	Shows details about the next entry in the log.
Previous	Shows details about the previous entry in the log.

11.5.3 Filtering Log Entries

Click **Filter** in the Log Viewer dialog box to determine which entries in the log are shown in the Log Viewer. Select **Filter Log** to enable filtering, and then choose from the following filtering options:

Option	Description
Filter by Date/Time	Filter out records based on certain date/time combinations. To build your filter, select either **First Record** or **Records on** in the **From** and **To** lists. If you want the Log Viewer to show the first entry generated during the assessment, select **First Record**. Clicking **Records on** lets you enter a date and/or time in the fields provided. Filter selection is based on a 12-hour clock with **AM** and **PM** designations.
Only Show Records With	If you want the Log Viewer to show only entries containing a specific error message, check the **Message=CHR** checkbox. Then enter or select the message number from the list. You can also filter the error log entries by call group. Check the **Group** checkbox and select the call group from the list. Record numbers remain unchanged after filters are applied to the Log Viewer. Their order indicates how the filter is being applied and which records have been filtered out.

11.6 Getting Technical Support

If you are unable to resolve your problem using the topics in the Troubleshooting chapter, contact NetIQ Technical Support.

Telephone:	713-418-5555 In North, Central, and South America, and in the Caribbean
Support:	www.netiq.com/support/va/phone.asp Provides a complete list of support phone numbers, as well as access to the NetIQ Knowledge Base and Technical Support

In many cases, Technical Support personnel will ask you to gather certain files from your computer that are needed to determine the sort of problem you are experiencing. Vivinet Assessor includes a tool that automates that procedure for you.

Gany Problem Sleuth (GanyPS) collects pertinent data for problem determination and uses FTP to send it directly to NetIQ Technical Support.

GanyPS builds a list of files and zips them within a directory created during product installation. Next, GanyPS attempts to FTP the `.zip` file to the Support Team. You are notified when the FTP operation has succeeded.

To run GanyPS, enter the following at a command prompt in the directory where you installed Vivinet Assessor:

```
ganyps filename [-t ftp_site]
```

The usage is as follows:

`filename`: When you contact Technical Support, you should receive an incident number, expressed as the filename to enter here.

`-t ftp_site`: Specifies an alternative FTP site. The default is `ftp://web.ganymede.com/`.

12 Working with the Sample Assessment

This chapter discusses the assessments you can review and the reports you can generate from the Sample assessment that ships with Vivinet Assessor. A review of the Sample assessment will acquaint you with the kind of data you can get from your own VoIP Readiness Assessment.

To view the Sample assessment, click **Open** on the File menu, select **Sample** from the list, and then click **OK**.

12.1 Sample Network Inventory

The Network Inventory view tells Vivinet Assessor how to discover switches, router, and links on your network. Vivinet Assessor enters discovered devices and links into the Vivinet Assessor SQL database, along with their names, locations, and IP addresses.

To see how the Sample Network Inventory was set up, expand the **Inventory Network** view tab and click the **Set Up** view tab. For more information, see Section 3.1, “Setting Up a Network Inventory,” on page 25.

The Sample Network Inventory was scheduled to start immediately after activation using a default gateway of 10.0.60.165. Click **Edit SNMP Configuration** to see that the Network Inventory used the “public” community string. For more information, see Section 3.1.1, “Editing SNMP Configuration Information,” on page 26.

Click the Discover view tab to see which devices the Network Inventory found. For more information, see Section 3.2, “Discovering Network Devices and Links,” on page 31.

The Discovered Devices and Links table shows all switches, routers, and links that Vivinet Assessor discovered in the subnet you specified in the Set Up view. Each tab in the table indicates how many of each item were discovered.

Vivinet Assessor reports provide more information about discovered devices. For more information, see Chapter 8, “Generating Reports,” on page 91.

12.2 Sample Configuration Assessment

During a Configuration assessment, Vivinet Assessor examines the information in the database for devices discovered during the Network Inventory. It compares the available information to the rules file and clearly reports any devices that passed or failed rule criteria. For more information, see Chapter 4, “Task 2: Assessing Configuration,” on page 35.

Vivinet Assessor applies the Sample rules file to the information in the Sample database to perform a Configuration assessment. A valid rules file is essential to completing a successful Configuration assessment.

To apply the Sample rules file:

1. Expand the **Assess Configuration** view tab and click the Set Up view tab.
2. Click **Browse**, navigate to `\Program Files\Micro Focus\Vivinet Assessor\Samples` and select **SampleRules.xml**.
3. Click **Import**.
4. On the **Routers** and **Switches** tabs of the table, select each router and switch so that each device is included in the Configuration assessment.

To run the Sample Configuration assessment:

1. Click the **Run** view tab. Notice that the **Rules description** field displays the name of the Sample rules file.
2. Click **Activate Assessment**.
3. When prompted, click **Yes** to save the assessment. When complete, the assessment results are displayed on the **Routers** and **Switches** tabs of the Results table.

NOTE: Although the routers and switches being assessed are not actually installed on your network, the Configuration assessment completes successfully because the devices being assessed are included in the Sample database.

When the assessment is complete, you can analyze the results.

Click the plus sign (+) to expand the first set of results in the Results table. By default, results for routers are displayed first, sorted by result. Failure results are first, as indicated by the red error symbol, then by rule name (taken from the Sample rules file), and then by device name. To see results for switches, select the Switches tab.

Mouse over the first failure result row in the table to view the mouse over text that makes it easy to see why the device failed the rule:

The routers named `belattix01.bellevue.netiq` and `sjcdgibsonst01.sanjose.netiq` did not pass the rule named `CiscoMemoryRule`. As directed by the Sample rules file, the rule checked all Cisco Model 3640 routers with an operating system level of either 12.3(14)T or 12.3 to ensure they all had at least 64 MB of RAM. The following is an excerpt of the rule from the Sample rules file.

```
<Rule Name="CiscoMemoryRule
 Description=”Cisco /memoryRAM/MemoryFlash/model/version rule”>
 <TopRule LogicalOperator="AND">
  <!--Check all 3640 routers are running IOS 12.3 or 12.3(14)T1 and have greater
than 64 MB or RAM-->
 <IntermediateRule LogicalOperator=”OR”>
  <BasicRule ComparisonOperator="EqualTo">
   <BasicPropertyItem>
    <Property>OSRevision</Property>
    <Type>String</Type>
    <Unit>None</Unit>
    <Value>12.3(14)T1</Value>
    <DeviceType>router</DeviceType>
   </BasicPropertyItem>
  </BasicRule>
  <BasicRule ComparisonOperator=”EqualTo”>
   <BasicPropertyItem>
    <Property>OSRevision</Property>
    <Type>String</Type>
    <Unit>None</Unit>
    <Value>12.3</Value>
    <DeviceType>router</DeviceType>
   </BasicPropertyItem>
  </BasicRule>
 </IntermediateRule>
  <BasicRule ComparisonOperator=”EqualTo”>
   <BasicPropertyItem>
    <Property>Model></Property>
    <Type>String</Type>
    <Unit>None</Unit>
    <Value>cisco3640</Value>
    <DeviceType>router</Devicetype>
   </BasicPropertyItem>
  </BasicRule>
  <BasicRule ComparisonOperator="EqualTo">
   <BasicPropertyItem FilterOn=”true”>
    <Property>Vendor</Property>
    <Type>String</Type>
    <Unit>None</Unit>
    <Value>Cisco</Value>
```

```
    <Devicetype>router</DeviceType>
   </BasicPropertyItem>
  </BasicRule>
  <BasicRule ComparisonOperator=”GreaterThanEqualTo”>
   <BasicPropertyItem>
    <Property>MemoryRAM</Property>
    <Type>Integer</Type>
    <Unit>Megabytes</Unit>
    <Value>64</Value>
    <DeviceType>router</DeviceType>
   </BasicPropertyItem>
  </BasicRule>
 </TopRule>
</Rule>
```

Take a few minutes to scan the Sample rules file, which is saved by default in the `\Program Files\Micro Focus\Vivinet Assessor\Samples` directory. It is carefully commented to help you understand how rules can be constructed to avoid false failures, to enforce vendor-recommended operating system and memory levels, and to check for installed modules. For more information, see Section 4.1.1, “Creating a Rules File,” on page 36.

If you further expand the failure results for routers, you see that another Cisco router failed a rule because it did not have the required number of voice ports. And, with only 8 MB of RAM, a Nortel router failed the `NortelMemoryRule` requiring Rapid City routers of type rcA8610 to have at least 64 MB of RAM.

12.3 Sample Utilization Assessment

The Utilization assessment gathers and assesses utilization statistics for the devices and links on your network to let Vivinet Assessor determine whether your network is VoIP-ready. Vivinet Assessor contacts every device and link discovered during the Network Inventory.

The first steps in assessing utilization are to set up and verify the assessment. However, for the purposes of reviewing this Sample assessment, we will look only at the results. For more information, see Section 5.1, “Setting Up the Utilization Assessment,” on page 44 and Section 5.3, “Verifying the Utilization Assessment,” on page 46.

You run the Utilization assessment from the Monitor view, which is also where results are displayed. To access the Monitor view, expand the **Assess Utilization** view tab and click the **Monitor** view tab. It is easy to see from the pie charts that our Sample network may be close to 100% VoIP-ready. Only 1% of switches and links were rated “Poor.”

In the table below the pie charts, notice that no router, switch, or link was found to be “Unavailable.” However, several were rated “Poor” or only “Acceptable,” indicating places where upgrades may be needed to ensure the network supports high-quality VoIP calls.

For more information about assessment ratings, see Section 5.2, “Determining Assessment Result Ranges,” on page 44.

12.4 Sample Bandwidth Modeling

After you complete the Utilization assessment, you can try the Bandwidth Modeling feature. Bandwidth Modeling lets you project the effects of different codecs and call volumes, and helps you determine whether more bandwidth is required to support high-quality VoIP traffic after deployment. In other words, you can test multiple “what if” VoIP usage scenarios.

Bandwidth Modeling is pretty straightforward. Click the **Model Bandwidth** view tab, select a link in the Monitored Links table, and click **Create Modeled Link**.

In the Create a Modeled Link dialog box, select the parameters you want to test, and then click **OK**. A bandwidth model is displayed in the Modeled Links table.

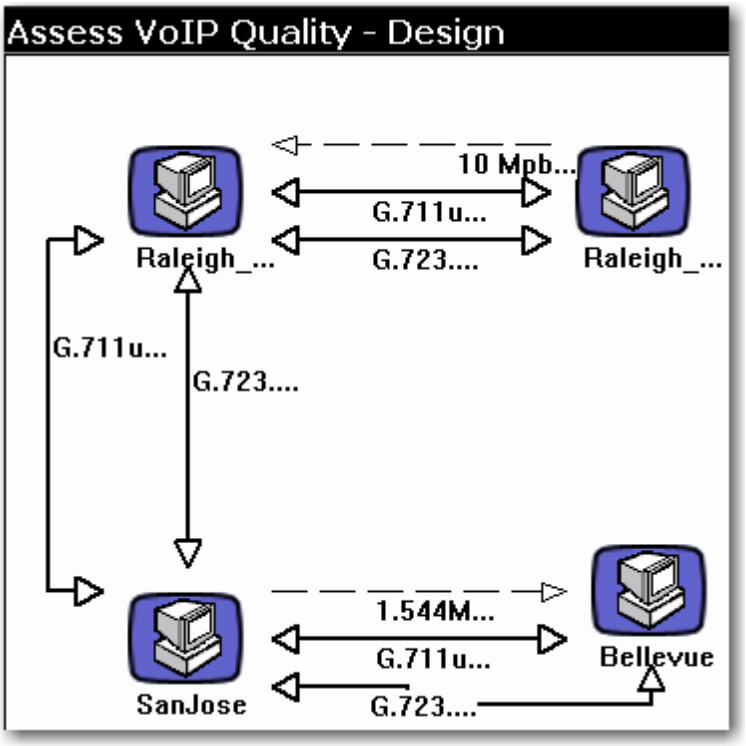
Feel free to experiment with different variations of models using the links discovered during the Sample Network Inventory. For more information, see Chapter 6, “Task 4: Modeling Bandwidth,” on page 49.

12.5 Sample VoIP Quality Assessment

The Sample assessment was designed to illustrate good VoIP Quality assessment design principles. In addition, the assessment has already been scheduled, verified, and activated. For the purposes of the Sample assessment, we will review only the design. However, for an actual VoIP Quality assessment, you must perform all relevant steps. For more information, see Chapter 7, “Task 5: Assessing VoIP Quality,” on page 55.

In the Sample assessment, expand the **Assess VoIP Quality** tab and click the **Design** view tab.

The Sample assessment deploys endpoints in a variety of locations and creates call groups to assess local and long-distance calling on a corporate network, using two different codecs.



As you can see from the Design view, two call groups contain endpoints located in Raleigh. Two VoIP connectors run simulated calls between these endpoints using different codecs, G.711u and G.723.1, so that the performance of each codec can be compared.

Two other call groups using the same two codecs send VoIP traffic across a WAN link between Raleigh and San Jose. A WAN link in your network is likely to cause VoIP performance issues and should be a part of any assessment.

The final two call groups run calls between San Jose and Bellevue over a long-distance link that is not a geographically dispersed as the Raleigh-San Jose link. The same two codecs are compared.

Take a look at Section 12.6, “Sample Reports,” on page 132 to see how this design helps identify which codecs perform the best. You can also compare MOS impairments that were caused by external factors, such as a slow WAN link, with impairments that were caused solely by the codec. In “VoIP Quality Assessment Results” on page 134, notice how we isolated a slow network segment by comparing the performance of the worst-performing call group using the G.711u codec with that of the worst-performing group using the G.723.1-ACELP codec.

12.6 Sample Reports

With the Sample assessment, you can generate an Executive Summary report and a Complete report. For more information, see Chapter 8, “Generating Reports,” on page 91.

Expand the **Report** tab, click the **Generate** view tab, and then review the following topics.

- Section 12.6.1, “Sample Executive Summary Report,” on page 132
- Section 12.6.2, “Sample Complete Report,” on page 134

12.6.1 Sample Executive Summary Report

The Executive Summary report provides a high-level overview of the results of each component of the VoIP Readiness Assessment.

To generate the Executive Summary report:

1. In the Generate view, select **Executive Summary**.
2. Click **Generate Report**. The report is generated in Microsoft Word and opens in its own window.

The Executive Summary begins by summarizing the VoIP Readiness Assessment, including which assessments were run and whether they ran to completion:

The Network Inventory section of the summary indicates the number of routers, switches, and links that were discovered.

Executive Summary reports do not include information about Configuration assessments and Bandwidth modeling.

Utilization Assessment Results

Scroll down through the Executive Summary into the section of results from the Utilization Assessment. After the summary of relevant information about when utilization monitoring was performed and what result ranges were configured, you see the following chart:

The Utilization Readiness Summary is the highest-level summary of the results from utilization monitoring. At a glance, you can see that which of the monitored links had enough “Good” utilization measurements to receive a “Good”, “Acceptable, or “Poor” rating.

The Executive Summary also includes charts that illustrate router, switch, and link utilization measurements broken out by day and by hour. Again, a quick look makes it apparent that the quality of the utilization statistics might vary slightly by the day of the week.

In fact, the **Link Measurements by Hour** chart, farther into the report, might reveal that utilization measurements were significantly worse between the hours of 8:00 AM and 6:00 PM, the hours when, more than likely, most users were accessing the network.

VoIP Quality Assessment Results

The “VoIP Quality Assessment” section of the Executive Summary includes information about the Potential Lost Revenue calculation. Vivinet Assessor found that **17.47%** of the simulated VoIP calls made during the assessment were either “Poor” or “Unavailable.”

Based on a projected loss of $42.67 per hour, per employee, in the Financial industry, Vivinet Assessor has calculated that the Poor and Unavailable calls in this assessment could lead to a revenue loss of as much as $745.44 per hour.

Farther down, the **Call Quality Summary** chart shows the percentage of all calls that fell into each call quality category.

This chart provides a first indication that further investigation of the results is required: although **45%** of the simulated calls were Good quality and **37%** were Acceptable quality, **13%** were Poor quality and **5%** were Unavailable.

Just below the Call Quality Summary chart, the **Factors Affecting Call Quality** chart indicates that the greatest impairment factors in the Sample assessment were codec at **82%**, delay at **14%**, and lost data at **4%**. You can analyze these results with the information provided by the Complete report. For more information, see Section 12.6.2, “Sample Complete Report,” on page 134.

Scroll down to the **Call Quality Summary by Call Group** chart. At a glance, you can tell which call groups had the lowest call quality. With a MOS of 3.50, the worst-performing call group was **Raleigh_Bldg 1-SanJose:G.723.1-ACELP**. The endpoints in this call group are located in the Raleigh and San Jose offices. Two call groups include these: **Raleigh_Bldg 1-SanJose: G.723.1-ACELP** and **Raleigh_Bldg 1-SanJose: G.711u**.

Although the Raleigh_Bldg 1-San Jose link experienced much better performance using the G.711u codec, it was still the worst-performing call group using that codec. According to the result ranges defined for this assessment (shown on the previous page of the report), the G.711u codec produced Good results (MOS of **4.18**) between these, while the G.723.1-ACELP codec produced Poor results (MOS of **3.50**).

12.6.2 Sample Complete Report

The Complete report expands on the information provided by the Executive Summary, allowing you to drill down into results for a more detailed analysis.

To generate the Complete report:

1. Click the **Generate** view tab and select **Complete Report**.
2. In the Filter Content tree, expand **VoIP Quality Assessment** and then click to check **Call Group Details**. Selecting this option provides a breakout of results per call group.
3. Click **Generate Report** and then click **Yes** to save your changes. The report is generated in Microsoft Word and opens in its own window. This process may take several minutes. The Complete report is much longer than the Executive Summary report.

Network Inventory Results

In the report, find **Network Inventory** in the Table of Contents. Click the corresponding page number to go straight to that section. Discovered routers, switches, and links are identified in tables. The names of devices and links are hyperlinks that take you to an appendix with some very detailed information. Click a hyperlink to see the information that is available for each device and link type.

TIP: It is easier to navigate within the Complete report if you use the **Back** and **Forward** arrow buttons in Word. Click **Toolbars** on the View menu, and then select the **Web** toolbar.

Click **Back** to return to the Table of Contents. To see how the routers fared during the Utilization Assessment, find the **Router Utilization Details** subsection and click on the corresponding page number to see a table.

The router names correspond to their locations. One router in the table might be the best-performing one, while another router might perform the worst, with CPU and output queue drops as the worst measurements. Both measurements suggest that this router is congested.

Return to the Table of Contents and navigate to the **Router Average CPU Utilization by Day** and **Router Average CPU Utilization by Hour** sections.

VoIP Quality Assessment Results

This section of the Complete report provides information about the poorly performing call group. This codec appears to be the major source of the poor-quality calls made by this call group. However, it is best to make sure no other factors were involved before purchasing the phones that will use this codec.

Navigate to **Factors Affecting Call Quality by Call Group**, located in the Calls by Group section of the VoIP quality assessment to view results. For more information, see Section 7.11.2, “Reviewing Codec Types,” on page 78.

To determine if was delay a major problem, navigate to the **Delay Evaluation by Call Group** chart, which. Notice that **89.66%** of delay values recorded for this call group fell into the Acceptable range.

The delay for this call group is not alarming. However, the average delay for this call group hovered around **176 ms**, as seen in the Delay Summary by Call Group chart, and most vendors believe that delay of more than 150 ms impairs call quality. Even though delay stayed within the Acceptable range, the delay impairment combined with the G.723.1 codec impairment was sufficient to drive call quality to a Poor level. Because the G.723.1 codecs have a theoretical maximum MOS of only 3.69, even a minor impairment can make their call quality Poor.

The G.723.1 call group may not be the only low performer. In the **Factors Affecting Call Quality by Call Group** chart, notice that the Raleigh_Bldg 1-San Jose: G.711u call group shows data loss of **.18** MOS point.

First, find out whether a network performance problem occurred during the assessment to cause the excessive data loss. Perhaps a problem existed on the link between Raleigh and San Jose. Navigate to the **Call Quality Evaluation by Day** chart.

Notice that call quality held pretty steady on each day of the assessment except for Monday, May 21, when **19.11%** of all MOS scores fell into the Poor range.

The **Factors Affecting Call Quality by Call Group** chart indicates that lost data was the largest MOS impairment factor for the G.711u call group, so look more closely at the Lost Data charts for this call group. Navigate to the **Lost Data Evaluation by Day** chart.

The chart indicates that Monday, May 21, experienced the highest amount of data loss: **0.07%**. On that day, **4.53%** of all lost data values fell into the Acceptable range. For an even more granular view of the data, navigate to the **Lost Data Evaluation by Hour** chart.

Notice that at its worst, data loss at 2 PM was low enough to be considered Good at **89%**. Most VoIP vendors recommend data loss of no more than 0.50% to maintain good call quality, so our loss of .07% (and less for the rest of the week) is not considered significant. Data loss for the G.711u call group is not a major contributor to the overall low MOS.

Pre-Deployment Discussion

The network delay results for the Raleigh_Bldg 1-San Jose: G.723.1-ACELP call group raise the question: Are the cross-country links adequate to carry high-quality VoIP in their present state?

The delay on these links was enough, when combined with the low-performing G.723.1-ACELP codec, to push call quality to an Acceptable or Poor level. And, according to the Link Utilization Details section of the Complete report, even the VoIP readiness of all the links was rated only Acceptable after the Utilization assessment.

Even using the high-performing G.711u codec, some calls between Raleigh and San Jose still have either Poor or Acceptable quality. Upgrading the fractional T3 line may work, but is expensive.

However, perhaps adding or changing **QoS**, which is recommended by most VoIP vendors, will improve call quality. You may want to deploy some call groups that use QoS and others that do not. You can compare the results to see which method provides better call quality. For more information, see Section 7.11.7, “Reviewing Quality of Service,” on page 81.