NetIQ® Vivinet® Diagnostics Version 2.3

User Guide

October 2012

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

Contents

About This Book and the Library

The *User Guide* provides conceptual information about NetIQ Vivinet Diagnostics and defines terminology and various related concepts. It also provides information for individuals responsible for understanding Vivinet Diagnostics concepts and for individuals who troubleshoot VoIP or evaluate VoIP performance on a network.

Other Information in the Library

The Vivinet Diagnostics library provides the following additional resources:

Performance Endpoints Guide

Explains how to install, configure, and troubleshoot Performance Endpoints for the platforms Vivinet Diagnostics supports.

Messages Guide

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

Help

Includes context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each dialog box.

The documentation library is available online at the NetIQ Vivinet Diagnostics Documentation page.

Conventions

This guide uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	◆ Window and menu items ◆ Technical terms, when introduced
Italics	◆ Book and installation kit titles ◆ Variable names and values ◆ Emphasized words
`Fixed Font`	◆ File and folder names ◆ Commands and code examples ◆ Text you must type ◆ Text (output) displayed in the command-line interface
Brackets, such as *[value]*	Optional parameters of a command

Convention	Use
Braces, such as *{value}*	Required parameters of a command
Logical OR, such as *value1*|*value2*	Exclude parameters. Choose one parameter.
(Conditional)	◆ “Conditional” means that you must perform an action if certain conditions exist. For example: (Conditional) If you use Control Center 7.x, run the module installer for each QDB attached to Control Center.
(Optional)	◆ “Optional” means that you can choose to perform an action. For example: (Optional) Click **Test** in browser to open a browser and go to the URL you just specified.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

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.

1 Introducing NetIQ Vivinet Diagnostics

AppManager diagnoses problems with the routing, connections, and performance of Voice over IP (VoIP) telephone calls on your network. With the data you receive from a Diagnosis, you can quickly resolve problems with VoIP hardware, software, and performance.

Vivinet Diagnostics is designed to perform two primary functions:

- Diagnose and locate the source of problems you detect on your network, such as poor-quality voice transmissions, dropped calls, and cutouts.
- Analyze the path a particular call actually takes through your network, including routers, switches, or voice gateways that intervene between the calling and called parties.

In addition, Vivinet Diagnostics can work along with NetIQ AppManager, which can alert you when a problem arises with your VoIP implementation but cannot pinpoint the source of the problem nor offer advice for resolving it. When end-user complaints or AppManager events indicate a performance problem, use Vivinet Diagnostics to diagnose the issue. For more information, see Chapter 8, "Working with NetIQ AppManager," on page 129.

1.1 How Vivinet Diagnostics Works

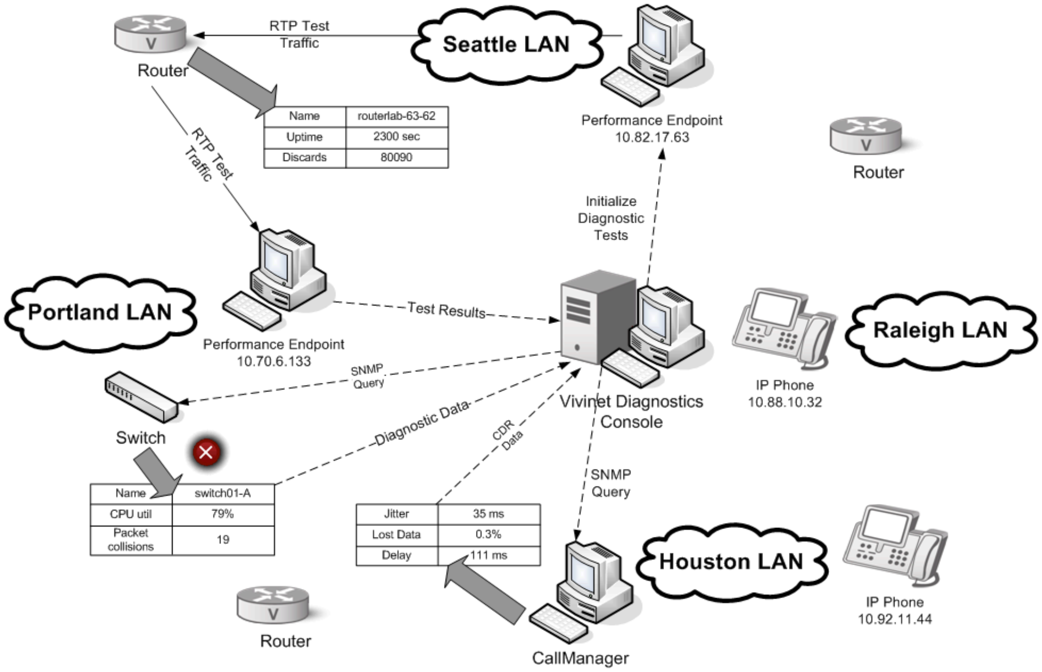
Vivinet Diagnostics helps you diagnose and remedy problems on your VoIP network by gathering data from network devices and measuring simulated VoIP traffic. To pinpoint the source of a problem, it also runs a *Path Trace* between two selected devices on the network.

Vivinet Diagnostics contains a *Knowledge Engine* that stores data collected on your network from each Diagnosis you run. The Knowledge Engine compares the data it collects to its own information (or rules) about VoIP, network hardware and software, and typical VoIP trouble spots to analyze and diagnose a problem you report.

Before you run a Diagnosis, install NetIQ Performance Endpoints near soft phones, voice gateways, and servers in your network. Endpoints help gather diagnostic information and can send test VoIP traffic between Target Devices to uncover problems. For more information, see Section 1.7, "NetIQ Performance Endpoints," on page 13.

To run a Diagnosis, select two *Target Devices* you believe are located at or near the source of the problem. Target Devices can be endpoints, telephones, routers, or gateways. As the Diagnosis runs, Vivinet Diagnostics sends simulated VoIP traffic between the selected devices and shows you a path trace indicating exactly how the traffic is traveling from Point A to Point B. Vivinet Diagnostics takes measurements, checks call data records from VoIP network software, and uses its Knowledge Engine to arrive at a Diagnosis. A diagnostic report helps you analyze the problem and respond appropriately.

The following diagram illustrates how Vivinet Diagnostics works in a network in which Performance Endpoints are deployed:



Name	routerlab-63-62
Uptime	2300 sec
Discards	80090

Name	switch01-A
CPU util	79%
Packet collisions	19

Jitter	35 ms
Lost Data	0.3%
Delay	111 ms

Suppose a user has reported difficulty making a VoIP call over the corporate WAN between Seattle and Portland. The Vivinet Diagnostics Console is located at Corporate Headquarters in Raleigh. A switch in Portland is congested and has been identified as the source of the problem (as the error symbol indicates).

During a Diagnosis, Vivinet Diagnostics contacts the endpoint computers you identified as Target Devices. Test RTP traffic (Real-Time Transport Protocol, indicated by solid arrows in the diagram) that emulates real VoIP traffic is then sent between the endpoints. The endpoints take measurements of the simulated VoIP traffic, while the Vivinet Diagnostics Console uses the Simple Network Management Protocol (SNMP) to query hardware and software MIBs like that of the switch shown in the diagram.

Results are collected and sent back to the Console (dashed arrows), where they are analyzed to derive a Diagnosis. In this particular Diagnosis, the Console queries the router, the Portland switch, and both endpoints to gather data on dropped or deferred packets, delay, CPU and memory utilization, and other metrics.

If you do not install endpoints in the subnet where the problem occurred, the Console gathers call performance data using the following:

- Cisco tools, including the Service Assurance Agent and CDP
- Avaya (Heritage-Nortel) tools, including SONMP and the `RTPStatShow` command
- The vendor-neutral LLDP

1.2 Cisco IOS IP Service Level Agreement

The Cisco IOS IP Service Level Agreement (IOS IP SLA, previously known as Cisco Service Assurance Agent) is part of the Cisco IOS router operating system, version 12.0 (5)T and later, and allows users to gather network performance metrics for troubleshooting purposes. As long as two

Cisco routers are present in the path between the Target Devices, IOS IP SLA can measure one-way delay, packet loss, jitter, and other performance data between the routers. You may have to do some extra configuration to allow IOS IP SLA measurements. For more information, see Section 3.4, "Tips for a Successful Diagnosis," on page 30.

Network performance measurements are a vital part of any Diagnosis of a VoIP problem. Like Vivinet Diagnostics, IOS IP SLA sends out packets with sequencing information and timestamps to measure packet loss and one-way delay between routers. Vivinet Diagnostics normally uses Performance Endpoints to generate test VoIP traffic and measure call quality statistics. However, if no endpoints are installed near where a VoIP problem is occurring, Vivinet Diagnostics can gather performance measurements from IOS IP SLA by using SNMP.

1.3 Cisco Discovery Protocol

Vivinet Diagnostics uses Cisco Discovery Protocol (CDP) queries to discover Cisco Layer 2 devices that might be relevant to the Diagnosis. Until devices are discovered, Vivinet Diagnostics cannot send them SNMP queries to find out where network issues are occurring.

CDP is enabled by default on Cisco routers, switches, and CallManager Media Convergence Servers. If you disabled it on any piece of Cisco equipment, re-enable it.

NOTE: You may have disabled CDP as a workaround for Cisco vulnerabilities CSCdu09909 and CSCdv57576. If so, and you enabled LLDP (Link Layer Discovery Protocol) instead, you do not need to enable CDP. For more information, see www.cisco.com/application/pdf/paws/13621/cdp_issue.pdf.

To enable CDP:

1 Issue the following command to find a router's global configuration settings, including whether CDP is enabled:

```
hostname# show cdp neighbors
```

where "`hostname#`" is the DNS hostname of the router.

2 Then issue the following commands:

```
hostname# configure terminal
hostname(config)# cdp run
hostname(config)# end
hostname# show cdp
```

1.4 Nortel RTPStatShow

A Nortel IP phone monitors VoIP traffic from phone conversations and keeps track of various statistics. Phase 1 phones track only RTCP (Real Time Transport Control Protocol). Phase 2 phones track both RTCP and RTCP-XR (Real Time Transport Control Protocol-Extended Reports). The IP phone periodically communicates the statistics to the Nortel Signaling Server.

RTCP, the control protocol extension of RTP for IP networks, monitors the quality of service of RTP data and tracks call information, including packet loss and delay. RTCP-XR, a superset of RTCP, provides better versions of packet loss and delay values, and also provides a value for average discard rate, which is similar to jitter buffer loss.

Vivinet Diagnostics telnets into the Signaling Server and invokes the `RTPStatShow` command to retrieve the statistics it has collected. How Vivinet Diagnostics presents the statistics in the **Performance** and **Quality Stats** tabs in the Report view, as part of a Diagnosis between Nortel Target Devices, depends on how the Diagnosis was implemented.

Diagnosis triggered by AppManager Knowledge Script

The AppManager NortelCS_Alarms Knowledge Script can run Action_DiagnoseNortelIPT when a QOS SNMP trap is raised after a voice quality metric exceeds a designated threshold. For more information, see Chapter 8, "Working with NetIQ AppManager," on page 129.

Phase 2 phones notify the Signaling Server when a threshold exceeds the Warning or Unacceptable level. The Signaling Server then raises the R-value trap.

NOTE: Because Phase 1 phones do not calculate R-value, they cannot raise the R-value QOS trap. Vivinet Diagnostics does not support R-value diagnoses for Phase 1 phones.

Vivinet Diagnostics uses the voice quality metrics from the trap to create the Diagnosis that appears in the **Performance** and **Quality Stats** tabs in the Report view. However, it uses the metrics from `RTPStatShow` to populate the **Quality Stats** tab that appears in the Phone details pop-up dialog box in the Path Trace of the Diagnose view.

Diagnosis triggered by Define view configuration

Vivinet Diagnostics collects voice quality metrics from `RTPStatShow` for both devices you configure in the Define view. It then determines which phone has the worst voice quality. These "worst" values are used to create the Diagnosis that appears in the **Performance** and **Quality Stats** tabs in the Report view. The metrics from `RTPStatShow` also populate the **Quality Stats** tab that appears in the Phone details pop-up dialog box in the Path Trace of the Diagnose view.

1.5 Nortel SONMP or NDP

Vivinet Diagnostics uses SNMP requests to Nortel devices to discover Nortel Layer 2 switches that might be relevant to a Diagnosis. These SNMP requests query for information that the devices receive through the SynOptics Network Management Protocol (SONMP, otherwise known as Nortel Discovery Protocol or NDP). Until the switches are discovered, Vivinet Diagnostics cannot send them SNMP queries to find out where network issues are occurring.

SONMP is a subclass of SNMP, which is the primary method by which Vivinet Diagnostics retrieves data from the Layer 2 environment. SONMP is a Layer 2 protocol that supplies topology information of devices that speak SONMP, mostly switches and hubs. SONMP is implemented in Nortel switches. The Layer 2 trace uses SONMP to find the interconnections between Nortel switches.

Layer 2 Nortel switches for which SONMP is not enabled are invisible to a diagnostic test and can bring the test to a halt. When SONMP is enabled, Vivinet Diagnostics can automatically determine the management IP addresses of physically neighboring Layer 2 switches. SONMP is enabled by default on Nortel switches. If you disabled it on any switch, re-enable it.

To enable SONMP:

1. Using Telnet, access the switch configuration and select **SNMP Configuration**.
2. In the **AutoTopology** field, select **Enabled**.

1.6 Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 discovery protocol, also known as IEEE standard 802.1ab. Vivinet Diagnostics uses LLDP in addition to CDP and SONMP to gather diagnostic information from a device's management information base (MIB). Many networks run a combination, or hybrid, of CDP and LLDP, or SONMP and LLDP. In such situations, Vivinet Diagnostics queries the LLDP portion of the MIB *and* the CDP or SONMP portion for information regarding all neighboring Layer 2 devices for a particular device.

NetIQ has tested Vivinet Diagnostics with the following Nortel LLDP implementations: ERS83xx (versions 3.0 and later), ES425 (version 3.6), and ES325 (version 3.6).

Management TLVs must be enabled on the LLDP devices you want to monitor. In a device's MIB, the LLDP data consists of sequences of short, variable-length information elements known as TLVs (type, length, value). The Management category of TLVs consists of the following TLVs, which are not stored in the MIB unless they are enabled:

- Port Description
- System Name
- System Description
- System Capabilities
- Management Address

Use your device's command line interface to enable Management TLVs. In general, the syntax for the command is as follows. Consult the documentation for your device for specific instructions.

```
lldp tx-tlv [port <portlist>] [port-desc] [sys-name] [sys-desc] [sys-cap] [local-
mgmt-addr]
```

1.7 NetIQ Performance Endpoints

NetIQ Performance Endpoints allow you to send synthetic VoIP traffic between two nodes or devices on your network and take performance measurements.

1.7.1 Downloading and Installing Endpoints

You can download free Performance Endpoints from the Current Performance Endpoints Product Upgrades page. PDFs are available on the same page that explain how to install and deploy endpoints for all of the supported 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 diagnoses, and should not interfere with other application traffic.

1.7.2 Deploying Endpoints

Install NetIQ Performance Endpoints on the same subnets as the phones on your network, particularly in locations where users have reported poor call quality or network performance issues. The endpoints allows Vivinet Diagnostics to send test VoIP traffic between two nodes on your network and take performance measurements. For more information, see Section 1.1, "How Vivinet Diagnostics Works," on page 9.

Install one Performance Endpoint on each subnet in your network. Consider also installing Performance Endpoints near all phones, VoIP gateways, and critical VoIP servers in your network. Endpoints help Vivinet Diagnostics obtain more information about your VoIP hardware and software to use in each Diagnosis. Plan to install the endpoints on a variety of computers, and consider the following for present and future needs:

- Install an endpoint in every subnet on the network where you anticipate VoIP traffic originating or terminating.
- Install endpoints near phones that have reported problems in the past.
- Install endpoints both close to and far from critical VoIP equipment such as gateways and servers. These endpoints will help you diagnose network-related issues in which location and access to equipment are factors.
- Install a few endpoints on either side of a WAN link, which is likely to be the site of problems with your VoIP implementation.
- Install endpoints on either side of a firewall. Some firewalls, particularly NAT-enabled firewalls, do not handle VoIP traffic very well.
- Install enough endpoints so that you can troubleshoot problems all over your network, at all user sites.

Although using Performance Endpoints as Target Devices is optional, deploying them allows the Console to run diagnostic network tests that collect additional data for problem analysis. Without endpoints, Vivinet Diagnostics must use other tools (such as Cisco IOS IP SLA and CDP, or Nortel SONMP, RTPStatShow, the R-value trap, or RTCP-XR) to gather information. Vivinet Diagnostics can run with some older versions of the endpoints, but to get the most accurate Diagnosis, install the latest endpoint version.

Even with endpoints installed, Vivinet Diagnostics uses the Nortel tools when diagnosing Nortel environments. The endpoints drive RTP traffic during device polling, which makes the polling results more meaningful.

1.7.3 Searching Subnets for Performance Endpoints

Vivinet Diagnostics is designed to discover the IP addresses of Performance Endpoint computers in a /24 subnet network, which has a subnet mask of 255.255.255.0 and a maximum of 254 hosts to scan for endpoints.

If you have something other than a /24 subnet network, Vivinet Diagnostics treats it as a /24 network and scans only 254 hosts for endpoints. To maximize the effectiveness of the data that Vivinet Diagnostics can gather from endpoints, consider the following options when deploying endpoints in your subnet network.

If phone IP addresses are not sparsely distributed throughout your network, deploy endpoints near groups of phones in your network so that the endpoints will be discovered.

- Disadvantage: Even clustered phone IP addresses can require many endpoints.
- Advantage: You can deploy endpoints to closely resemble the design of your physical network.

When defining a Diagnosis, use the Endpoint-to-Endpoint option and provide the IP address for both endpoints.

- Disadvantage: You can lose phone-specific information from the Diagnosis.

When defining a Diagnosis, use the IP phone-to-Other option and provide the endpoint IP address as the “other” address.

- Disadvantage: You can lose endpoint performance test information from the Diagnosis.

2 Installing and Registering Vivinet Diagnostics

The topics in this section help you install, register, and uninstall Vivinet Diagnostics.

2.1 Security Considerations

Review the following security topics to ensure the security of your VoIP network. In addition, ensure your computers are properly secured against intrusions using available Windows security mechanisms.

Consideration	Description
SNMP security	Never give an unauthorized user access to the computer on which Vivinet Diagnostics is installed. One essential step in setting up a Diagnosis is providing your network's SNMP permission information to grant Vivinet Diagnostics the ability to contact and query devices on your network. Intruders could use this information for malicious attacks. Vivinet Diagnostics encrypts this information to save it in an Options file and also encrypts it in any diagnoses you save. For SNMP v1 and v2, Vivinet Diagnostics sends the SNMP community string for SNMP queries in clear text. Vivinet Diagnostics encrypts the community strings and stores them locally. For SNMP v3, Vivinet Diagnostics reads the permissions information configured for NetIQ Vivinet Assessor or NetIQ AppManager. If you use SQL Server authentication, the permission information is stored locally and encrypted in an Options file. To grant Vivinet Diagnostics access to your voice quality data, configure SNMP permissions into Vivinet Diagnostics. This information is not encrypted until Vivinet Diagnostics stores it on your hard drive. For more information, see Section 3.5.1, "Configuring SNMP Permissions," on page 32.
Cisco CallManager security	Vivinet Diagnostics accesses and displays information from Cisco Call Detail Records (CDRs). Some of this information may be sensitive, such as information about the numbers called from a particular phone, as well as how long the calls lasted. To grant Vivinet Diagnostics access to CDRs, configure CallManager user IDs and passwords into Vivinet Diagnostics. This information is not encrypted until Vivinet Diagnostics stores it on your hard drive. For more information, see Section 3.5.4, "Configuring CallManager User IDs and Passwords," on page 36.

Consideration	Description
Avaya (Heritage-Nortel) CS1000 security	Vivinet Diagnostics accesses and displays information from the Avaya (Heritage-Nortel) CS1000 Signaling Server and Call Server. Some of this information may be sensitive, such as information about the numbers called from a particular phone, as well as how long the calls lasted. To grant Vivinet Diagnostics access to your Signaling and Call Server, configure SL1 level 1 login user IDs and passwords into Vivinet Diagnostics. This information is not encrypted until Vivinet Diagnostics stores it on your hard drive. For more information, see Section 3.5.6, "Configuring Nortel CS1000 Call and Signaling Servers," on page 40.

2.2 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, this module supports all updates, hotfixes, and service packs for the releases listed below.

Vivinet Diagnostics has the following system requirements:

Hardware and Software	Notes
Requirements for the computer on which you install Vivinet Diagnostics	
Microsoft Windows operating system	You need Administrator privileges to install and run Vivinet Diagnostics. ◆ **Windows Server 2012** ◆ **Windows 8 (32-bit or 64-bit)** ◆ **Windows Server 2008 R2** ◆ **Windows Server 2008 (32-bit or 64-bit)** Requires configuration of the firewall. For more information, see Section 2.7, "Working with the Windows Server 2008 Firewall," on page 25. Support for Quality of Service settings on Windows 7, Windows 2008, and Windows 2008 R2 endpoints requires the latest version of the NetIQ Performance Endpoints. Download the updated Performance Endpoints at the Current Performance Endpoints Product Upgrades page. ◆ **Windows 7 (32-bit or 64-bit)** ◆ **Windows Vista (32-bit or 64-bit)** Windows Vista does not support Quality of Service settings based on the Differentiated Services Code Point (DSCP) field in the IP header. ◆ **Windows Server 2003 (32-bit or 64-bit)** Vivinet Diagnostics requires WinHTTP 5.1, a component of Windows Server 2003, in order to retrieve Cisco CallManager data through the Secure Sockets Layer (SSL). ◆ **Windows XP (32-bit or 64-bit)** NetIQ Corporation recommends Service Pack 1 if you enabled SSL on your Cisco CallManager computer. Vivinet Diagnostics requires WinHTTP 5.1, a component of Service Pack 1, in order to retrieve CallManager data through the SSL.

Hardware and Software	**Notes**
One or both of these NetIQ applications, to enable diagnoses of SNMP v3-enabled devices	◆ Vivinet Assessor version 3.3 ◆ AppManager version 7.x or later
Requirements for the environment you are diagnosing	
NetIQ Performance Endpoints	Install NetIQ Performance Endpoints on every computer you want to diagnose. For more information, see Section 1.7, “NetIQ Performance Endpoints,” on page 13.
Avaya Communication Manager	Vivinet Diagnostics supports Avaya Communication Manager 6.0, 5.x, or 4.x.
Avaya (Heritage-Nortel) Communication Server 1000 (CS1000)	Vivinet Diagnostics supports Avaya (Heritage-Nortel) CS1000 versions 7.5, 7.0, 6.0, 5.5, 5.0, 4.50, or 4.0 Versions 6.0 and earlier of Nortel CS1000 require the following patches and firmware: **Patches**: Obtain these patches from your Nortel support and maintenance provider. For Signaling Server versions 4.00.31 and 4.00.55, install four patches: ◆ **MPLR19592**, which updates the `eStatShow` and `isetInfoShow` commands. Without the patch, the server does not send back output for these commands and Vivinet Diagnostics cannot retrieve phone details. ◆ **MPLR19581**, which updates RTCP-XR for the R-value metric. ◆ **MPLR20987**, which fixes BERR705 and BERR504. ◆ **MPLR21070**, which fixes a memory leak from `telnet/rlogin` command-line interface commands. For Signaling Server version 4.50.25, install two patches: ◆ **MPLR20987**, which fixes BERR705 and BERR504. ◆ **MPLR21297**, which enables simultaneous traceroutes between the same two phones. **Phone firmware**: Firmware versions D98 and later meet the firmware prerequisite. Versions D98 and later contain an update to `rTraceRoute`. Nortel CS1000 versions 7.0 and 7.5 do not require these firmware versions. If you use version D97 or earlier, upgrade your firmware. Versions D97 and earlier do not contain the update to `rTraceRoute`, causing your diagnoses to stop running and producing incomplete results.
Avaya (Heritage-Nortel) Communication Server 2100 (CS2100)	Vivinet Diagnostics supports Avaya (Heritage-Nortel) CS2100 version SN11 or SE11 using Phase 2 phones.

Hardware and Software	Notes
Cisco Unified Communications Manager	Vivinet Diagnostics supports: - Cisco Unified Communications Manager, version 8.0, 7.1(2), 7.0, 6.1, or 5.0 - Cisco Unified CallManager, version 4.x or 3.x **Important** Do not install Vivinet Diagnostics on a computer on which you have installed a Cisco TFTP server. Vivinet Diagnostics runs its own TFTP server to perform certain diagnostic checks. If a Cisco TFTP server is already running on the same computer, Vivinet Diagnostics will be unable to access the information it needs, and will generate an error indicating a TFTP request timed out

2.3 Installing Vivinet Diagnostics

The installation program, `diagnostics.exe`, automatically identifies and updates all relevant Vivinet Diagnostic components on a computer. Therefore, run the installation program only once on any computer. When installation is complete, you may be asked to restart your computer.

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

Install Vivinet Diagnostic on a local hard disk of the computer from which you want to run diagnoses. You should not install Vivinet Diagnostics on a LAN drive. The additional network traffic will influence your diagnostic results. The default directory is `Program Files\NetIQ\Vivinet Diagnostics` on your boot drive.

Select whether you want to diagnose **Nortel** or **Cisco** phones, or phones from **Other** vendors. You can run diagnoses for more than one vendor by changing the vendor later using the Options menu in the Vivinet Diagnostics console. To run diagnoses between Performance Endpoints only, you can select any vendor.

2.4 Reviewing Directories and File Types

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

Directory	Files Contained in the Directory
Program Files\NetIQ\Vivinet Diagnostics	- Vivinet Diagnostics executable file for the Console: `diagnostics.exe` - Vivinet Diagnostics `.dll` files - Vivinet Diagnostics Readme file: `Readme.htm` - Vivinet Diagnostics license file created when you register the product: `vdiag.lic` - `fmtlog.exe`, used to format log files - If you deregister the product, the Vivinet Diagnostics deregistration file: `.dat`
NetIQ\Vivinet Diagnostics\Help	Help files with file extension `.chm`

Directory	Files Contained in the Directory
NetIQ\Vivinet Diagnostics\MIBS	Management Information Base (MIB) files to help Vivinet Diagnostics interface with certain types of MIBs
NetIQ\Vivinet Diagnostics\Report Template	`.htm` and image files needed to format a Vivinet Diagnostics report
NetIQ\Vivinet Diagnostics\Samples	Sample diagnoses you can open and analyze
Documents and Settings\All Users\Application Data\NetIQ\Vivinet Diagnostics	◆ Files that save endpoint and telephone definitions you have entered: `DiagEndpoint.dat and DiagPhone.dat` ◆ Error logs for application errors: `DiagnosticsTrace1.txt`, `DiagnosticsServerTrace1.txt`, `assert.err`, and `errorlog.txt` ◆ Files that save configuration values when you make changes from the **Options** menu. As a rule, you can edit only `CancelDiagnosesConfig.txt`, although for troubleshooting purposes you may be asked to edit the `TraceConfig.txt` file. For more information, see Section 6.4, "Disabling Selected Diagnoses," on page 110.

2.5 Registering Vivinet Diagnostics

Vivinet Diagnostics runs in Demo mode until you register an evaluation or retail license. Demo mode provides only limited functionality and does not allow you to diagnose a problem. For more information, see Section 2.5.3, "Reviewing Demo Mode," on page 23.

The Vivinet Diagnostics Registration component allows you to perform any registration task online, including registering a temporary evaluation license, reregister to upgrade your license, or deregister your license so you can transfer the software to another computer.

If the **Evaluate** and **Register** buttons in the initial Registration dialog box are grayed out, you may not have the necessary privileges to register Vivinet Diagnostics on this computer. These buttons also may be grayed out if a Diagnosis is currently running or if multiple Diagnosis windows are open.

Click **Help** in any Registration dialog box to read context-sensitive help for that dialog box.

For more information, see the following topics:

- To register a license, see Section 2.5.1, "Registering," on page 22.
- To register a temporary evaluation license, see Section 2.5.4, "Reviewing Evaluation Mode," on page 23.
- To upgrade a time-limited license, see Section 2.5.5, "Upgrading a Vivinet Diagnostics License," on page 23.
- To deregister a license to use it on another computer, see Section 2.5.6, "Deregistering Vivinet Diagnostics," on page 24.

2.5.1 Registering

You register Vivinet Diagnostics with the NetIQ Registration Center to receive an authorization key for a retail or evaluation license. By default, no license is present, and Vivinet Diagnostics runs in Demo mode. You can run Vivinet Diagnostics in Demo mode free of charge for as long as you like, but significant restrictions on functionality apply. For more information, see Section 2.5.3, “Reviewing Demo Mode,” on page 23.

If your computer is connected to the Internet, you can register immediately on our Web site. Or you can contact the NetIQ Registration Center by phone or e-mail. A series of Registration dialog boxes guides you through the necessary steps.

To register Vivinet Diagnostics:

1. From the Options menu, click **Registration** and then click **Register**.
2. Supply the **Registration Number** and **Password** from the registration card included in your product package. Do not type any spaces or tabs.
3. Click **Next**.
4. Select **Get an authorization key** and then click **Next**.

   NOTE: If you are not connected to the Internet, deselect **Get an authorization key**, click **Next**, and then continue with Section 2.5.2, “Completing Registration by Telephone or E-mail,” on page 22.
5. If your browser is not configured to make secure connections, disable **Use a secure connection**.
6. Click **Next**. The NetIQ Registration Center Web page opens in your default Web browser.

   In the online form, ensure your contact information is correct. Make changes or additions if necessary. Click **New User** if the information applies to another person, and type your own information in the blank form that appears.
7. Click **Generate License**. Your unique authorization key appears in the browser window. Highlight the key and copy it. Do not copy any extra spaces after the key. If you paste the key plus extra spaces into the **Authorization Key** field, registration will fail.
8. In the Enter Authorization Key dialog box, paste or type the key into the **Authorization Key** field.
9. Click **Next**.
10. To print a copy of your registration, click **Print Registration Info**.

2.5.2 Completing Registration by Telephone or E-mail

If you indicated your computer is not connected to the Internet, the Registration Summary dialog box shows the registration number and password you provided in the first Registration dialog box, plus a license code. Click **Print** to print this information, or write it down, because you must supply this information when you call or e-mail the Registration Center.

E-mail requests, as well as after-hours calls, are processed within one business day. These requests *must include* the product and version number, registration number, password, and the license code provided in the Registration Summary dialog box. Provide this information to the Registration Center representative, who will in turn give you an authorization key to enable the retail version of Vivinet Diagnostics. Type the key in the appropriate field in the Enter Authorization Key dialog box and click **Finish** to complete your registration.

2.5.3 Reviewing Demo Mode

By default, Vivinet Diagnostics runs in Demo mode until you register an evaluation or retail license. "Demo" is indicated on the Console interface, and functions such as running a Diagnosis or entering SNMP information are unavailable.

Demo mode lets you run the product free of charge for as long as you like. Functionality is severely restricted, however. Although you can open and view a Diagnosis of your network, you cannot run a Diagnosis. You can also generate reports from diagnoses you created while the product was running with a valid license.

If you purchased a time-limited license for Vivinet Diagnostics, the application reverts to Demo mode after the time limit is reached.

To register Vivinet Diagnostics, see Section 2.5, "Registering Vivinet Diagnostics," on page 21.

2.5.4 Reviewing Evaluation Mode

After installation, Vivinet Diagnostics runs in Demo mode until it detects a valid evaluation or retail license file. To create a license file, enable an evaluation with a temporary authorization key, or provide a valid registration number and password, which are supplied when you purchase a retail license.

To create an evaluation license, click **Registration** on the Options menu, and then click **Evaluate**. A series of dialog boxes lets you enter your temporary authorization key, which you received from a NetIQ sales representative.

After you authorize an evaluation, Vivinet Diagnostics runs in Evaluation mode. Evaluation mode provides the application's normal functioning, but is time-limited. After the three-day evaluation period expires, the application again runs in Demo mode. For more information, see Section 2.5.3, "Reviewing Demo Mode," on page 23.

At any point during your evaluation, you can register the software if you have a registration code and password. For more information, see Section 2.5, "Registering Vivinet Diagnostics," on page 21.

2.5.5 Upgrading a Vivinet Diagnostics License

You can upgrade an existing evaluation Vivinet Diagnostics license to extend the time period. Use the Registration dialog boxes to *reregister* an upgraded license for Vivinet Diagnostics. The dialog boxes direct you to perform the same steps for registering and obtaining an authorization key.

You must first contact a NetIQ sales representative and purchase an upgraded license. For more information, see Section 6.5, "Getting Technical Support," on page 113.

After you purchase an upgraded license, you can reregister it. For more information, see Section 2.5.1, "Registering," on page 22. The procedure for updating a license is the same as that of registering.

2.5.6 Deregistering Vivinet Diagnostics

To relinquish your Vivinet Diagnostics license or transfer your license to another user or computer, deregister your current Vivinet Diagnostics license. You must deregister before you uninstall or your product license will not allow you to use Vivinet Diagnostics on another computer or at a later time.

It is not necessary, or possible, to deregister an evaluation license.

To deregister Vivinet Diagnostics:

1. From the Options menu, click **Registration**, and then click **Deregister**.
2. As appropriate, select or deselect **This computer is connected to the Internet** and **Use a secure connection**.

   NOTE: To deregister without an Internet connection, contact the NetIQ Registration Center by telephone or e-mail and provide your registration number and deregistration code.

3. Click **Next**.
4. In the Confirmation dialog box, click **Yes**. A deregistration code is provided in the Deregistration Summary dialog box if deregistration succeeds. This unique code is tied to your authorization key and password. During deregistration, this information is saved in an ASCII text file, `deregister.dat`, in your `Program Files\NetIQ\Vivinet Diagnostics` directory.
5. Click **Print Deregistration Information** to print a copy of your information in case you need to contact the NetIQ Registration Center.

After you deregister, you cannot use Vivinet Diagnostics again until you reregister. If you restart Vivinet Diagnostics after deregistering, the application runs in Demo mode.

After you deregister, you can register again. For more information, see Section 2.5, "Registering Vivinet Diagnostics," on page 21.

If deregistration fails, follow the steps outlined in Section 2.5.7, "Deregistration Failures," on page 24.

2.5.7 Deregistration Failures

If deregistration fails for any reason, your Vivinet Diagnostics license becomes invalid and you must manually complete the deregistration process.

To manually deregister:

1. Navigate to the `deregister.dat` file in your `Program Files\NetIQ\Vivinet Diagnostics` directory.
2. Open the file using a Windows utility, such as Notepad, and locate the deregistration code. Copy the code to the Windows clipboard.
3. Use a Web browser to navigate to www.netiq.com/register/nw.
4. Click the **Deregister** link.
5. Paste the deregistration code into the **Dereg code** field, and then click **Deregister**. Your browser should display the message "Deregistration Successful."

If you have problems with deregistration, contact NetIQ Technical Support. For more information, see Section 6.5, "Getting Technical Support," on page 113.

2.6 Uninstalling Vivinet Diagnostics

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

When you uninstall Vivinet Diagnostics, files you created, such as saved Diagnosis files, are not removed. The folders containing these files are also preserved. Registry entries, however, are not removed automatically. You must remove registry entries manually.

NOTE: Before you uninstall the application, deregister the Vivinet Diagnostics license. Otherwise, you cannot register the program on another computer. For more information, see Section 2.5.6, "Deregistering Vivinet Diagnostics," on page 24.

To uninstall Vivinet Diagnostics:

1. From the Control Panel, double-click **Add/Remove Programs**.
2. Highlight **NetIQ Vivinet Diagnostics** and click **Add/Remove** (or **Change/Remove** or **Remove**, depending on your version of Windows).
3. In the Confirm File Deletion dialog box, click **Yes**.
4. When uninstallation is complete, click **OK** twice.
5. *To remove registry entries*, run the `REGEDIT` command from a command prompt.
6. Delete the following keys:
   - `HKEY_LOCAL_MACHINE\Software\NetIQ Network Performance\Vivinet Diagnostics`
   - `HKEY_CURRENT_USER\Software\NetIQ\Vivinet Diagnostics`

2.7 Working with the Windows Server 2008 Firewall

If you are running Vivinet Diagnostics on Microsoft Windows Server 2008, you are running with a firewall and may find that diagnoses do not run properly. Perform one of the following tasks:

- Disable the firewall option in Windows Server 2008.
- Create an inbound rule for the `diagnostics.exe` executable file.

To create an inbound rule for the diagnostics.exe executable:

1. From the Start menu, select **Administrative Tools** and then double-click **Windows Firewall with Advanced Security**.
2. In the left pane, select Inbound Rules.
3. In the right pane, select New Rule, and then click Next.
4. Click Browse and navigate to `diagnostics.exe` in the file system.
5. Click Next in this and the next two dialog boxes.
6. Provide a Name for the rule, such as Allow diagnostics.exe.

3 Working with Vivinet Diagnostics

The topics in this section provide guidance as you perform basic tasks with Vivinet Diagnostics.

3.1 Reviewing the Vivinet Diagnostics Console Interface

When you open Vivinet Diagnostics, you are welcomed to the product by the **Vivinet Diagnostics** tab, which identifies the three primary steps involved in creating a Diagnosis: Define, Diagnose, and Report.

Click the tabs in the upper left corner to navigate Vivinet Diagnostics and review the status bar at the bottom of the Console for more information.

Console Component	Description
Define tab	Use the fields in the Define view to identify the type of devices you want to use in your Diagnosis. If you select **Phones**, choose two phones and the time a problem occurred. If you select **Endpoints**, choose two endpoints and a call script. If you select **IP Phone-to-Other**, choose one phone and one non-phone device. For more information, see Section 3.6, "Defining the Problem (Step 1)," on page 43.
Diagnose tab	The contents of the Diagnose view vary slightly depending on the selections you made in the Define view. Use the Diagnose view to begin your Diagnosis, view the traceroute of the hops your VoIP call made during its journey from calling party to called party, and view the Error Log and status information. For more information, see Section 3.7, "Diagnosing the Problem (Step 2)," on page 45.
Report tab	Use the Report view to review the results of your Diagnosis, and to generate a copy of your Diagnosis in HTML or CSV format. For more information, see Section 3.8, "Reporting the Results (Step 3)," on page 47.
Status bar	**Start Time**—the time you started the Diagnosis. **Duration**—the length of time the Diagnosis has been running (if still running), or ran, if completed. **Issues**—a tally of the potential problems Vivinet Diagnostics has found between the Target Devices. In the Diagnose view, the Issue count does not necessarily correspond to the number of icons shown because devices having more than one Diagnosis display only one icon. Shown in all views at the bottom of the Console. **Created By**—who or what set up the Diagnosis. *User* indicates the Diagnosis was set up by a user at the Vivinet Diagnostics Console. *AM* indicates the Diagnosis was launched by an AppManager Action script. For more information, see Chapter 8, "Working with NetIQ AppManager," on page 129. **License Expiration**—expiration date of the current registered license.

3.2 Getting Started

Perform the steps in this checklist to prepare your environment for diagnosing VoIP problems. When you have completed these steps, you are ready to set up a Diagnosis.

Step	Description
Register the software.	When installation completes, Vivinet Diagnostics runs in Demo mode, which has only limited functionality. You must register the product to start diagnosing problems. For more information, see Section 2.5, "Registering Vivinet Diagnostics," on page 21.
Review the needs of your VoIP environment.	Before you design your first Diagnosis, research the needs and idiosyncrasies of your network and your VoIP implementation. For more information, see Section 3.3, "Understanding Your VoIP Network," on page 29.
Configure SNMP, SONMP, and CDP settings.	Vivinet Diagnostics must be able to query the key devices on your network in order to diagnose VoIP problems. For more information, see Section 3.4, "Tips for a Successful Diagnosis," on page 30.
Deploy Performance Endpoints.	Endpoints are not a prerequisite for running Vivinet Diagnostics, but they gather essential performance metrics that aid in making accurate diagnoses. For more information, see Section 1.7, "NetIQ Performance Endpoints," on page 13.
Configure Layer 2 devices.	Visible (configured) Layer 2 devices prevent Vivinet Diagnostics from overburdening your network when it performs sweeps of subnets during diagnoses. For more information, see Section 4.4.2, "Device Configuration," on page 68.
Configure Cisco CallManager addresses.	Before you run a Diagnosis between Cisco phones, configure the address of CallManager devices that are not discovered by other means such as CDP or LLDP. For more information, see Section 3.5.3, "Adding or Deleting a CallManager," on page 36.
Identify Nortel Call Servers and Signaling Servers.	Vivinet Diagnostics must be able to recognize the destination phones identified in R-value traps that come in to the Signaling Server. Trap information is not usable until you configure all Signaling Server and Call Server user IDs and passwords. For more information, see Section 3.5.6, "Configuring Nortel CS1000 Call and Signaling Servers," on page 40.
Configure VRRP routers.	If you use VRRP routers, and especially if you are using them as gateway routers for phones, Vivinet Diagnostics needs to know the IP addresses of your Master and backup routers. For more information, see Section 3.5.8, "Configuring VRRP IP Addresses," on page 42.
Review configuration tips.	Review the list of configuration tips and perform any that are applicable to your environment. For more information, see Section 3.4, "Tips for a Successful Diagnosis," on page 30.

Step	Description
Set up and run a Diagnosis.	◆ **Define** the problem you detected on your VoIP network. Select the phones, endpoint computers, or other non-phone devices where the Diagnosis should be carried out. For more information, see Section 3.6, “Defining the Problem (Step 1),” on page 43. ◆ **Diagnose** the problem by running the Diagnosis you defined. For more information, see Section 3.7, “Diagnosing the Problem (Step 2),” on page 45. ◆ **Report** the results. View results or generate a report summarizing the findings. For more information, see Section 3.8, “Reporting the Results (Step 3),” on page 47.

3.3 Understanding Your VoIP Network

Before you design your first Diagnosis, research your network and your VoIP implementation.

- Look at existing network documentation to find peak and average usage statistics. Network congestion is likely to be the chief cause of poor VoIP performance. Knowledge of typical usage is helpful for setting performance thresholds.
- Call Detail Records (CDRs), stored in a SQL database by Cisco CallManager help Vivinet Diagnostics to discover whether jitter, lost data, and delay are creating call performance issues. If any of these metrics presents a problem, CDRs help you determine where to begin running diagnoses. CallManager does not collect CDRs. For more information, see Section 3.4, “Tips for a Successful Diagnosis,” on page 30.
- Nortel data comes from two sources: the *Call Server* and the *Signaling Server*. The Call Server identifies the Directory Number and Signaling Server for a phone’s IP address. The Signaling Server runs `rTraceRoute`, `RTPStatShow`, `eStatShow`, `isetInfoShow`, and `isetGet`. The latter three commands collect various phone properties such as telephone number and firmware version. Ensure access to the Call Server and Signaling Server is not blocked by a firewall. For more information, see Section 4.1, “Running a Diagnosis Through a Firewall,” on page 57.
- Familiarize yourself with the codecs in use on your network. Understanding the codecs and how they are configured will help you when you set up problems for Vivinet Diagnostics to diagnose. For more information, see Section 4.2.2, “Reviewing Codecs,” on page 60.
- If you use NetIQ AppManager, review call performance data and run through the last few weeks’ events to identify problems that are reported frequently. For instance, if you see a lot of events about CPU utilization on a router, you may want to use Vivinet Diagnostics to diagnose call performance problems experienced by VoIP phones using that router. For more information, see Chapter 8, “Working with NetIQ AppManager,” on page 129.

3.4 Tips for a Successful Diagnosis

Before you set up and run a Diagnosis, review the following configuration tips and perform any that are applicable to your VoIP environment. Performing some or all of these tips can improve the quality of data that you receive from a Diagnosis.

Tip	Description
Supply your SNMP permissions information	Vivinet Diagnostics supports SNMP versions 1, 2, and 3. SNMP permissions allow Vivinet Diagnostics to gather information from SNMP-enabled network devices. Read/write authorization for SNMP versions 1 and 2 is required for running Cisco IOS IP SLA tests on routers and to retrieve QoS configuration information. For other types of queries, such as queries of CallManagers, read-only access is adequate. For more information, see Section 3.5.1, "Configuring SNMP Permissions," on page 32.
Ensure Diagnoses can run through firewalls	For each Diagnosis, Vivinet Diagnostics attempts to perform a traceroute test to find the exact path VoIP packets are taking. A firewall could prevent the packets from making some hops, however. To ensure Vivinet Diagnostics works properly with a firewall on your network, select the port Vivinet Diagnostics should use for the call (or RTP) traffic it sends. Remember, RTP traffic uses even-numbered ports. For more information, see Section 4.1, "Running a Diagnosis Through a Firewall," on page 57.

Ensure IOS IP SLA is properly configured	The Cisco IOS IP SLA allows network performance monitoring between a Cisco router and a remote device, such as another Cisco router or an IP host. IOS IP SLA or the Monitor Responder support running jitter and delay tests on many Cisco routers. In cases where the Target Devices for the Diagnosis are phones (instead of Performance Endpoints), Vivinet Diagnostics gathers data from IOS IP SLA tests to diagnose the problem. Two routers, each running IOS IP SLA, are required (one is a sender, the other a responder). To test jitter, the responder must be enabled.
	To determine whether IOS IP SLA is enabled on a router, issue the following command:
	`show ip sla monitor responder`
	To enable IOS IP SLA, issue the following commands:
	`configure terminal`
	`ip sla monitor responder`
	If you are running a Diagnosis between Nortel phones in a network that uses Cisco routers, ensure you have enabled IOS IP SLA. Vivinet Diagnostics looks first to the Nortel phones and then to the endpoints for data. Should either source not provide information, Vivinet Diagnostics gathers data from IOS IP SLA.

Enable your Console's IP address on SNMP devices	During a Diagnosis, Vivinet Diagnostics communicates with the SNMP-enabled devices on your network. The Vivinet Diagnostics Console address must be included in any access list that controls access to these devices.
	To determine whether the Console's IP address is included in a device's access list, issue the following command:
	`show access-list`
	To add an IP address to a device's access list, issue the following command:
	`configure access-list`

Tip	Description
Configure CallManager to collect CDRs and CMRs	1. CallManager Call Detail Records (CDRs) and Call Management Records (CMRs) give Vivinet Diagnostics access to valuable information about call metrics and call quality. CallManager does not gather these records by default. You must manually configure the collection of these useful data records: In Cisco CallManager Administration, click **Service > Service Parameters**. Select the desired CallManager computer. Select the **Cisco CallManager** service. To enable the generation of CDRs, set **CDREnabled** to **True**. To enable the generation of CMRs, set **CallDiagnosticsEnabled** to **True**.
Configure SNMP on CallManagers	On each CallManager computer, ensure the SNMP service is running and configured properly. From Administrative Tools, double-click **Services**. Ensure the SNMP service is set to “Automatic” and is running. Right-click the service and select **Properties**. In the Service Properties dialog box, select **Applications** on the Agent tab. Add a read-only community string on the Security tab. Then add this community string to Vivinet Diagnostics. For more information, see Section 3.5.1, “Configuring SNMP Permissions,” on page 32.
Ensure CDP is enabled	CDP enables the discovery of Cisco devices, particularly Layer 2 devices (switches). Because switches constitute potential bottlenecks for VoIP traffic, information about their location and utilization is important for a Diagnosis. Do not disable CDP on your devices before you run a Diagnosis. For more information, see Section 1.3, “Cisco Discovery Protocol,” on page 11.
Ensure ports 443 and 80 are available on CallManager server	Vivinet Diagnostics always attempts to use the Secure Sockets Layer (SSL) protocol through port 443, the standard SSL Internet port, when requesting CallManager data. If the attempt fails, Vivinet Diagnostics uses the HTTP protocol through port 80, the standard Internet port.
Ensure SONMP is enabled	SONMP is a Layer 2 protocol that supplies topology information about devices that also speak SONMP, mostly switches and hubs. SONMP is implemented in Nortel devices. Layer 2 devices for which SONMP is not enabled are invisible to a diagnostic test or can bring the test to a halt. SONMP is enabled by default on Nortel devices. If you disabled it on any piece of Nortel equipment, re-enable it. For more information, see Section 1.5, “Nortel SONMP or NDP,” on page 12.
Ensure LLDP TLVs are enabled	LLDP data is not saved to a device’s MIB unless the Management TLVs are enabled. For more information, see Section 1.6, “Link Layer Discovery Protocol,” on page 13.
Configure the actual speed on serial interfaces	To diagnose a problem involving serial interfaces, including frame relay and serial links, Vivinet Diagnostics needs to determine the bandwidth utilization on these links. However, device MIBs for these interfaces often provide the wrong speed attribute, showing the links’ theoretical maximum speed instead of the actual speed at which they are running. Diagnoses on serial links will be more accurate if you ensure the correct (that is, operating) speed is configured for the bandwidth parameter on serial interfaces. That way, the SNMP MIB variable `ifSpeed` will reflect the correct value.

Tip	Description
Synchronize router clocks	In order for Vivinet Diagnostics to retrieve delay statistics on VoIP calls using Cisco IOS IP SLA, the clocks on all the routers must be synchronized with each other. To synchronize router clocks, issue the following command (from router configuration): `ntp server <server>` where <*server*> is the IP address or DNS hostname of the Network Time Protocol (NTP) server on the network.
Ensure ICMP is enabled	Vivinet Diagnostics runs some diagnoses by sending out Internet Control Message Protocol (ICMP) packets to gather information at each router hop. If a router's ICMP is disabled, it cannot provide pertinent information for a Diagnosis. Refer to your device documentation for information about enabling ICMP.
Configure thresholds.	As an optional step, configure thresholds that help Vivinet Diagnostics determine whether a network condition should be reported as an issue. For more information, see Section 3.5.5, "Setting Thresholds," on page 37.

3.5 Configuring Additional Information

Vivinet Diagnostics can diagnose many VoIP call quality problems on your network right out of the box. However, some additional configuration can ensure your diagnoses are based on as much information about your particular network and its quality requirements as is possible to collect.

3.5.1 Configuring SNMP Permissions

Vivinet Diagnostics 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.

Configure SNMP information in the Vivinet Diagnostics Console or in NetIQ AppManager or Vivinet Assessor. This configuration provides Vivinet Diagnostics the permissions it needs to access the MIBs (management information bases) on SNMP-enabled network devices.

The type of information you configure varies according to the version of SNMP implemented on your network devices. Vivinet Diagnostics supports SNMP versions 1, 2, and 3

Configuration for Versions 1 and 2

For SNMPv1 and SNMPv2, the community string acts as a password to let Vivinet Diagnostics collect information from the MIB on SNMP-enabled devices.

Before you run a Diagnosis, configure SNMP properties to let Vivinet Diagnostics communicate with devices on your network. If you do not supply your community string information, the Vivinet Diagnostics attempts to use the default SNMP community string, which is not secure and therefore is probably not in use on your network.

NOTE: Each string's authorization indicates the type of variables it can access from a device MIB: either read/write or read-only. Read/write strings are required for certain Cisco IOS IP SLA actions and traceroute testing.

To configure a community string:

1. On the Options menu, click **SNMP**.
2. On the SNMPv1v2 tab, click **Add**. Complete the fields according to the information below:

Field	Description
Community String	Provide the SNMP community string currently in use on your network. Community strings for read-only variables may be different from those for read/write variables. Add each valid community string on your network to the list, one by one. Strings are limited to 64 characters. Because the SNMP community string allows access to the MIB of each network device, secure the console computer to protect this and any other sensitive information. SNMP community strings are case-sensitive.
Community string has read/ write authorization	Identifies the type of variable Vivinet Diagnostics can access from a VoIP device's MIB with this community string. Read/write community strings can access both read/write and read-only variables. Read/write authorization is required for Cisco IOS IP SLA tests.
Community string has read-only authorization	Identifies the type of variable Vivinet Diagnostics can access from a VoIP device's MIB with this community string. Read-only community strings can access only read-only variables.

Configuration for Version 3

Vivinet Diagnostics diagnoses devices using SNMP v3 by borrowing the SNMP v3 permissions you configured for NetIQ Vivinet Assessor or NetIQ AppManager. To use SNMP v3 permissions from either application, Vivinet Diagnostics looks for matching permission configurations in the following order:

- AppManager Security Manager entry for a single IP address with a `VDiag` label
- AppManager Security Manager entry for a single IP address with a `NetworkDevice` label
- Vivinet Assessor device range, single IP address, or fully qualified domain name
- AppManager Security Manager "default" entry with a `VDiag` label
- AppManager Security Manager "default" entry with a `NetworkDevice` label

NOTE: In environments with a mixture of SNMP v2 and v3 devices, you must configure Vivinet Assessor or AppManager Security Manager permissions for every SNMP v3-enabled device.

If all other attempts fail, Vivinet Diagnostics tries the SNMP v1 and SNMP v2 community strings until it finds one that works, or until they all fail.

Using SNMP v3 Permissions from Vivinet Assessor

In order for Vivinet Diagnostics to use the permissions configured for Vivinet Assessor, Vivinet Assessor must be installed on the computer on which Vivinet Diagnostics is installed.

To use the SNMPv3 permissions from Vivinet Assessor:

1. On the Options menu, click **SNMP**.

2 On the SNMPv1/v2 tab, ensure the Community String is **public** and the Authorization is **read-only**, even if you have no SNMPv1 or v2 devices configured on your network.

3 On the SNMPv3 Vivinet Assessor tab, select **Use SNMPv3 profiles defined in NetIQ Vivinet Assessor**.

4 In the list, select the assessment that contains the SNMPv3 profiles you want to you in Vivinet Diagnostics. If you have recently created an assessment that does not appear in the list, click **Refresh Assessment List**.

   The list contains only those assessments for which at least one SNMPv3 profile exists.

Using SNMP v3 Permissions from AppManager

To use SNMP v3 permissions from AppManager, Vivinet Diagnostics searches AppManager Security Manager for entries created with either *VDiag* or *NetworkDevice* labels. If you have no NetworkDevice-labeled permissions that provide access to the devices you want to diagnose, you can configure permissions with a VDiag label. In addition, you can override a NetworkDevice label with information configured with a VDiag label. For more information, see "Configuring Vivinet Diagnostics SNMP v3 Permissions in AppManager" on page 34.

AppManager and Vivinet Diagnostics do not need to be installed on the same computer.

To use the SNMPv3 permissions from AppManager:

1 On the Options menu, click **SNMP**.

2 On the SNMPv1/v2 tab, ensure the Community String is **public** and the Authorization is **read-only**, even if you have no SNMPv1 or v2 devices configured on your network.

3 On the SNMPv3 AppManager tab, select **Use SNMPv3 profiles defined in NetIQ AppManager**.

4 In the **Server** field, type the fully qualified domain name of your AppManager server.

5 In the **Repository** field, type the name of your AppManager repository.

6 *If access to your AppManager server requires Windows authentication*, select **Use Windows authentication**.

   If access requires SQL Server authentication, select **Use SQL Server authentication**, and then provide the **Login name** and **Password**.

7 To ensure Vivinet Diagnostics can connect to your AppManager repository, click **Test Connection**. A message indicates whether the connection attempt was successful.

   If the attempt was not successful, ensure you are attempting to access a repository for which you have connectivity permissions. Also, if you selected **Use SQL Server authentication**, ensure your login name and password are correct.

Configuring Vivinet Diagnostics SNMP v3 Permissions in AppManager

Vivinet Diagnostics supports the following authentication modes for SNMP v3:

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

In addition, the application supports the following protocols for SNMPv3:

- MD5 (Message-Digest algorithm 5, an authentication protocol)

- SHA (Secure Hash Algorithm, an authentication protocol)
- DES (Data Encryption Standard, encryption protocol)

Your SNMP v3 implementation may support one or more combinations of mode and protocol. That combination dictates the type of information you configure in AppManager Security Manager: User Name (or entity), Context name, protocol name, and protocol passwords.

You must configure AppManager Security Manager with the SNMP v3 permissions that provide Vivinet Diagnostics with access to the devices you want to diagnose. In environments with a mixture of SNMP v2 and v3 devices, you must explicitly identify every SNMP v3-enabled device.

On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	`VDiag` To share this configuration with the AppManager for Network Device module, type `NetworkDevice`.
Sub-label	- For a User Name and Context for a single device, type the <*IP address*> of the device. - To use the same User Name and Context for all devices, type `default`.
Value 1	SNMP user name or entity configured for the device. All SNMP v3 modes require an entry in the **Value 1** field.
Value 2	Name of a context associated with the user name or entity you entered in the **Value 1** field. A context is a collection of SNMP information that is accessible by an entity. If possible, enter a context that provides access to all MIBS for a device. If the device *does not* support context, type an asterisk (`*`). All SNP v3 modes require an entry in the **Value 2** field.
Value 3	Combination of protocol and password appropriate for the SNMPv3 mode you have implemented. - *For no authentication/no privacy mode*, leave the **Value 3** field blank. - *For authentication/no privacy mode*, type `md5` or `sha` and the password for the protocol, separating each entry with a comma. For example, type `md5,abcdef` - *For authentication/privacy mode*, type `md5` or `sha` and the associated password, and then type `des` and the associated password, separating each entry with a comma. For example, type `sha,hijklm,des,nopqrs`

3.5.2 Changing the “Public” String for a CallManager

The Cisco CallManager application uses a predefined SNMP community string named “public.” Its rights are set to “none.” To diagnose VoIP problems for CallManager, change those rights to be “read-only.” After changing the rights, you can add the community string to Vivinet Diagnostics.

To change the community string rights on a CallManager server:

1. In Control Panel, double-click **Administrative Tools**, and then double-click **Services**.
2. Right-click **SNMP Service** and select **Properties**.
3. On the Security tab, in the Accepted community names panel, select **public** and then click **Edit**.

4 In the Community rights list, select **READ ONLY**, and then click **OK** twice to exit the Properties dialog box.

5 Configure the SNMP community string in Vivinet Diagnostics. For more information, see "Configuration for Versions 1 and 2" on page 32.

3.5.3 Adding or Deleting a CallManager

Cisco CallManager handles VoIP call processing and maintains records about call activity. Vivinet Diagnostics can gather important information to use in diagnosing your network problems by querying CallManager applications that are active on the VoIP network.

You must configure information about at least one CallManager. Vivinet Diagnostics should be able to locate all others based on that information. You can configure more CallManagers if necessary.

NOTE: Ensure SNMP is running on the CallManagers to be queried.

To add or delete a CallManager:

1 On the Options menu, click **CallManager**.

2 *To add a CallManager to the list*, click **Add** in the CallManagers section.

Specify the IP network address of the CallManager server in dotted notation, such as `122.34.56.78`, or a DNS hostname, such as `callmgrsvr01`. The address or hostname must be no more than 64 characters in length.

Click **OK** to add the new CallManager to the list.

3 *To remove a CallManager from the list*, highlight its name or address in the list and click **Delete**.

3.5.4 Configuring CallManager User IDs and Passwords

If the CallManagers on your network have been secured with user ID and password protection, configure the CallManager security information into Vivinet Diagnostics.

For CallManager versions earlier than version 4.0, the default user ID and password for any CallManager are actually the default SQL Server user ID and password, which are not secure. Vivinet Diagnostics can gather a lot of useful diagnostic information from CallManagers using this CallManager security information.

NOTE: The `CiscoCCMCDR` user ID is already configured into Vivinet Diagnostics. If you changed this ID, configure the new ID in Vivinet Diagnostics. In addition, configure any additional SQL users you may have created.

To add user IDs/passwords for CallManager versions earlier than 4.0:

1 On the Options menu, click **CallManager**, and then click **Add** in the User IDs and Passwords section.

2 In the **User ID** and **Password** fields, type the SQL Server user ID and password.

In CallManager versions 4.0 and later, the method used for obtaining information is different from earlier versions. For security reasons, SQL Server user IDs and passwords are no longer used to access information. Instead, CallManager uses a new API called AXL (AVVID XML Layer). Configure Vivinet Diagnostics with the user ID and password that have authority to use this API. In most cases, the CallManager administrator user ID and password have the authority.

NOTE: You may have used the Cisco Multilevel Administration (MLA) application to set up other accounts to have the same authorization.

To add user IDs/passwords for CallManager version 4.0 and later:

1. On the Options menu, click **CallManager**, and then click **Add in** the User IDs and Passwords section.
2. In the **User ID** and **Password** fields, type the AXL user ID and password.

3.5.5 Setting Thresholds

You set thresholds to control how Vivinet Diagnostics evaluates network conditions and reports them as "issues" in the Diagnose view. To set thresholds, click **Thresholds** from the Options menu.

A collected statistic crosses a threshold, and thereby flags an issue, when it either *exceeds* or *fails to meet* the threshold level you set. For each metric, you can set one or two different thresholds. Values discovered during a Diagnosis that exceed a Marginal threshold indicate poor VoIP performance. Values that exceed the Good threshold indicate marginal, or barely acceptable, performance.

Thresholds determine the *performance rating* assigned to each performance metric in the Results portion of the Diagnosis. They also determine the *severity* assigned to any issue discovered during a Diagnosis. For more information, see Section 5.1.9, "Severity," on page 86.

Threshold settings apply *only* to the present Diagnosis unless you select **Set As Defaults**. This option ensures the settings you select apply to any new diagnoses you configure. The settings can be changed at any point. However, if you change a threshold for a Diagnosis that has already run and has results, those results will be cleared.

Click **Restore Defaults** to change threshold settings back to the values you previously set as defaults. If you never changed the defaults, **Restore Defaults** changes the thresholds back to the recommended values — the settings Vivinet Diagnostics uses by default. However, after you select

Set As Defaults to set new default values, you must *manually* restore the recommended values. See the following threshold definitions for a discussion of the default values for each tab in the Thresholds dialog box.

Call Quality Thresholds

Use the Call Quality tab to set thresholds for MOS, R-value, delay, jitter buffer loss, and lost data.

Threshold Type	Description
MOS	Refers to the Mean Opinion Score, which represents the quality of a VoIP transmission by factoring in the “mouth-to-ear” characteristics of a speech path. Vivinet Diagnostics calculates the MOS by evaluating simulated VoIP traffic based on a standardized model. A MOS of 5 is considered excellent. A MOS of 1 is unacceptably bad. The default is 4.03 for Good performance. For more information, see Section 5.3.7, “Mean Opinion Score,” on page 103. You can select either MOS or R-value, not both. MOS is the default selection. The call quality metric you choose is displayed in the Diagnosis table of the Report view. However, both metrics are displayed on the Performance tab of the Results table in the Report view. After you set a MOS threshold, the R-values for Good and Marginal change accordingly. Note, a single MOS score can map to a range of R-values. Therefore, the equation Vivinet Diagnostics uses to convert MOS to R-value (and vice versa) produces an approximate R-value. For example, with a MOS score of 4.1, the conversion equation produces an R-value of 82.64. However, when converting an R-value of 82.64, the equation produces a MOS of 4.12, a small, but noteworthy, difference.
R-value	Call quality value derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor). The default is 80.45 for Good performance. For more information, see Section 5.3.9, “R-value,” on page 104. You can select either MOS or R-value, not both. The call quality metric you choose is displayed in the Diagnosis table of the Report view. However, both metrics are displayed on the Performance tab of the Results table in the Report view. After you set an R-value threshold, the MOS values for Good and Marginal change accordingly. Note, a range of R-values can map to a single MOS. Therefore, the equation Vivinet Diagnostics uses to convert R-value to MOS (and vice versa) produces an approximate MOS. For example, with an R-value of 82.64, the conversion equation produces a MOS of 4.12. However, when converting a MOS of 4.12, the equation produces an R-value of 83.28, a small, but noteworthy, difference.
Delay	Determines how much delay (latency) in milliseconds can be detected for a simulated VoIP call before Vivinet Diagnostics reports an issue. Vivinet Diagnostics uses the delay statistic when calculating a MOS for simulated VoIP traffic sent between the Target Devices. The default is 150 ms for Good performance. For more information, see Section 5.3.3, “Delay,” on page 100.
Jitter Buffer Loss	Determines how much datagram loss due to jitter (or delay variation) can be detected for a VoIP call before Vivinet Diagnostics reports an issue. Any jitter detected in the call is compared to the size of the jitter buffer in the call script. Jitter buffer lost datagrams are then expressed as a percentage of all datagrams sent. Vivinet Diagnostics uses the jitter buffer loss statistic when calculating a MOS for simulated VoIP traffic sent between the Target Devices. The default is 0.500% for Good performance. For more information, see Section 4.2.5, “Defining Jitter Buffer,” on page 61 and Section 5.3.5, “Jitter Buffer Loss,” on page 102.

Threshold Type	Description
Lost Data	Determines how much packet loss can be detected for a simulated VoIP call before Vivinet Diagnostics reports a problem. Equals the number of datagrams lost between the Target Devices, expressed as a percentage of all data sent. Vivinet Diagnostics includes data loss when calculating a MOS for simulated VoIP traffic. The default is .500% for Good performance. For more information, see Section 5.3.6, “Lost Data,” on page 102.

Device/Link Thresholds

Use the Device/Link tab to set thresholds for WAN and LAN interface bandwidth utilization, device CPU utilization, and insufficient bandwidth.

Threshold Type	Description
WAN interface bandwidth utilization	Determines how much traffic a particular WAN link can carry, expressed as a percentage of the total capacity of that link, before Vivinet Diagnostics reports a problem. Vivinet Diagnostics defines a WAN link as any interface slower than 10 Mbps. The default is 30% for Good performance. For more information, see Section 5.3.8, “Network Congestion,” on page 103.
LAN interface bandwidth utilization	Determines how much traffic a particular LAN link can carry, expressed as a percentage of the total capacity of that link, before Vivinet Diagnostics reports a problem. Vivinet Diagnostics defines a LAN link as any interface 10 Mbps or faster. The default is 50% for Good performance. For more information, see Section 5.3.8, “Network Congestion,” on page 103.
Device CPU utilization	Refers to the percentage of processor (CPU) time being taken up by network processes. Vivinet Diagnostics checks CPU utilization on any network device that carries the VoIP RTP traffic between the Target Devices during a Diagnosis. It does not check CPU utilization on the end devices themselves. The default is 30% for Good performance.
Insufficient bandwidth	Determines how little bandwidth can be available on a particular VoIP network link before Vivinet Diagnostics reports an issue. The default is 35 kbps for Marginal performance (only determines “insufficient” bandwidth, not “sufficient,” and therefore, does not have a Good threshold). For more information, see Section 5.3.4, “Insufficient Bandwidth,” on page 101.

POTS Interface Thresholds

Use the POTS Interface tab to set thresholds for voice signal strength, ACOM, ERL, and T1/E1 bearer channel utilization.

Threshold Type	Description
Signal	Voice signal strength is a measurement of decibel relative to one milliwatt. Use this field to specify the thresholds for **Good** and **Marginal** voice signal strength.
ACOM	Short for *ACombined*, ACOM is equal to ERL + ERLE (Echo Return Loss Enhancement). ERLE is the amount of echo provided by an echo canceller. Use this field to specify thresholds for **Good** and **Marginal** ACOM decibel levels.
ERL	*Echo Return Loss* is the ratio of the power level of the transmitted voice signal to the power level of the echo signal generated by the VoIP gateway. ERL varies greatly depending on the switched telephone network connected to the VoIP gateway. There will always be echo whenever you have an analog trunk line connected to a digital network. Use this field to specify thresholds for **Good** and **Marginal** ERL decibel levels.
T1/E1 Bearer Channel utilization	Bearer channels are the channels in a T1 or E1 circuit that carry phone calls. Use this field to specify **Good** and **Marginal** thresholds for the percentage of bearer channels that can be in use at any time.

Traffic Class Thresholds

Use the Traffic Class tab to set thresholds for traffic class utilization, priority queue depth, and dropped packet rate.

Threshold Type	Description
Traffic class utilization	A traffic class is a particular category of traffic on an interface. For example, voice and data can be classified as individual traffic classes. Use this field to set the threshold for what is considered “marginal” traffic class utilization in your network. Vivinet Diagnostics can provide diagnoses only for those traffic classes for which priority queuing is enabled. For details about enabling priority queuing, see the QoS configuration documentation for your device.
Priority queue depth	Use this field to set the threshold for the highest number of packets that can be in the priority queue before being considered an issue.
Dropped packet rate	Use this field to set the highest acceptable rate at which packets are dropped due to factors such as queuing, policing, early detection, or traffic shaping.

3.5.6 Configuring Nortel CS1000 Call and Signaling Servers

In a Nortel CS1000 environment, the *Call Server* provides call and connection management services for the IP network, and helps Vivinet Diagnostics determine whether the destination IP address is a phone in a Diagnosis triggered by AppManager.

The *Signaling Server* provides signaling interfaces to the IP network, and performs call control services such as the registration of terminals and gateways, admission control, IP address translation, and bandwidth control. The R-value SNMP trap on the Signaling Server provides the call quality information Vivinet Diagnostics uses in diagnoses triggered by AppManager. If you define a Diagnosis from the Define view, the Signaling Server provides the call quality information collected by `RTPStatShow`.

NOTE: Vivinet Diagnostics obtains the SNMP trap information from the NortelCS_Alarms and Action_DiagnoseNortelIPT AppManager Knowledge Scripts. For more information, see Chapter 8, "Working with NetIQ AppManager," on page 129.

When a trap comes in, Vivinet Diagnostics must determine whether the destination IP address is a phone. To this end, it queries the Signaling and Call Servers, which are not available for querying unless you configured all possible address/user ID/password combinations into Vivinet Diagnostics. Without complete or correct configuration information, Vivinet Diagnostics may not be able to determine whether the destination address is a phone, and instead will consider it to be "other," for instance a VGMC or a voice application such as Call Pilot.

Vivinet Diagnostics also uses this configuration information to collect phone properties, `RTPStatShow` call quality information, and `rTraceRoute` path information.

Ensure you selected Nortel as your phone vendor, and then complete the following procedures for each Call Server and Signaling Server. For more information, see Section 3.5.7, "Changing the Phone Vendor," on page 42.

To configure Call Server user IDs and passwords:

1. On the Options menu, click **Call Server**, and then click **Add**.
2. Complete the following fields:

Field	Description
Call Server	IP address of the Call Server
User ID	SL1 level 1 user ID associated with the Call Server
Password	SL1 level 1 password associated with the Call Server

To configure Signaling Server user IDs and passwords:

1. On the Options menu, click **Signaling Server**, and then click **Add**.
2. Complete the following fields:

Field	Description
Signaling Server	IP address of the Signaling Server
User ID	SL1 level 1 user ID associated with the Signaling Server If you never configured your Signaling Server with the `LNAME` option in overlay 17, the user ID is the default, which is `admin`.
Password	SL1 level 1 password associated with the Signaling Server

3.5.7 Changing the Phone Vendor

When you installed Vivinet Diagnostics, you were asked to select the vendor (Nortel, Cisco, or Other) whose Target Devices you will use to run diagnostic tests. By selecting a vendor, you customize the Define view, and the Options menu. Cisco-specific options and fields will not appear when you select Nortel or Other as a vendor. The reverse is also true.

You can change vendors without having to reinstall Vivinet Diagnostics.

To change the phone vendor:

1. On the Options menu, click **Phone Vendor** and select **Nortel**, **Cisco**, or **Other**.
2. To make the selection permanent for future diagnoses, click **Set As Default**

NOTE

- If you run diagnoses between Performance Endpoints only, you can select any vendor.
- To run diagnostic tests for Avaya devices, select **Other**.

3.5.8 Configuring VRRP IP Addresses

The Virtual Router Redundancy Protocol (VRRP), implemented by Cisco and Nortel, provides for router failover. VRRP allows multiple routers to be configured together as one *virtual router*. This virtual router advertises a virtual IP address as the default gateway. At any one time, there is a *Master* router, which is the actual router acting as the default gateway, and one or more *backup* routers. If the Master router fails, one of the backup routers becomes the Master and begins routing traffic.

Vivinet Diagnostics’ SNMP queries to VRRP-enabled devices are successful if you configured VRRP so that the Master router’s real IP address *is the same* as the VRRP virtual IP address.

If router failover has occurred, or if the VRRP virtual IP address is *not the same* as the Master router’s real IP address, Vivinet Diagnostics’ SNMP queries *cannot* determine the real IP address of the Master router.

To enable Vivinet Diagnostics to query a Master router regardless of failover or VRRP IP address configuration, you must provide a list of VRRPs in use in your network. Perform the following steps for each router acting as a VRRP Master or backup.

To add VRRP IP addresses:

1. On the Options menu, click **VRRP**, and then click **Add**.
2. Complete the following fields:

Field	Description
VRRP Router	Management IP address of the router
Virtual IP	Virtual IP address of the virtual router
VRID	Virtual router identifier for the group of routers that back up the IP address you specified in the **Virtual IP** field. A virtual router is defined by its virtual router identifier and its associated IP addresses.

3.6 Defining the Problem (Step 1)

To begin diagnosing a problem on your network, click the **Define** tab to enter the Define view. Diagnoses take place between Target Devices: two sites on the network (phones, endpoints, or non-phone devices) where Vivinet Diagnostics will try to pinpoint the problem.

3.6.1 Defining a Phone-to-Phone Diagnosis

To diagnose a VoIP problem between two phones, select **Phones** as your Device Type. Vivinet Diagnostics will trace the path taken by VoIP traffic between the two phones you select. These phones can be either IP telephones currently active on your VoIP network or regular POTS (Plain Old Telephone Service) telephones that might make calls to the IP phones on your network.

NOTE

- If you choose Cisco phones as the device type, configure information about their CallManagers to help Vivinet Diagnostics diagnose the problem. For more information, see Section 3.5.3, “Adding or Deleting a CallManager,” on page 36.
- If you choose Nortel phones as the device type, configure information about their Call Servers and Signaling Servers to help Vivinet Diagnostics diagnose the problem. For more information, see Section 3.5.6, “Configuring Nortel CS1000 Call and Signaling Servers,” on page 40.
- When you choose phones as Target Devices, you cannot select a call script. As part of the Diagnosis, Vivinet Diagnostics attempts to run VoIP performance tests between Performance Endpoints installed in the same subnet. These tests emulate the G.711 codec, with “Best Effort” QoS. If no endpoints are installed in the subnet, Vivinet Diagnostics uses other methods to help diagnose the problem. For more information, see Section 1.1, “How Vivinet Diagnostics Works,” on page 9.

Complete the remaining fields as shown below. Then, run the Diagnosis by clicking the **Diagnose** tab. For more information, see Section 3.7, “Diagnosing the Problem (Step 2),” on page 45.

Field	Description
Phone 1	An IP telephone or a POTS phone on the PSTN that is considered the source of the call traffic that experienced a problem. In a Cisco environment, either Phone 1 or Phone 2 must be an IP telephone. In a Nortel or Avaya environment, both phones must be IP phones. *In a Cisco or Nortel environment*, type one of the following: ◆ The phone’s full phone number, such as `222-555-1212` ◆ The phone’s extension, such as `6003` ◆ The IP address of the IP phone in dotted notation, such as `135.25.25.5` ◆ The DNS hostname, such as `devel_lab_netiq` *In an Avaya environment*, type the IP address of the phone. **NOTE**: To diagnose a Nortel phone when the Directory Number is not unique across the Call Servers, ensure you type the Terminal Number (TN) instead of the phone number. Type the TN using the following format: `xxx-yy`. If you omit the dash, Vivinet Diagnostics will be unable to find the TN on the Call or Signaling Server.

Field	Description
Phone 2	An IP telephone or a POTS phone on the PSTN that is considered the target or destination of the call traffic that experienced a problem. In a Cisco environment, either Phone 1 or Phone 2 must be an IP telephone. In a Nortel environment, both phones must be IP phones. **NOTE**: To run a Diagnosis between an IP phone and a PSTN phone in a Nortel environment, use the **IP Phone-to-Other** option and provide the IP address of the voice gateway in the **Other** field.
Time problem occurred	The approximate time of the call that experienced the problem. If you do not know the time, select **Unknown** from the list. This information helps Vivinet Diagnostics find the relevant call details.
Validate button	Click to save all parameters of your problem definition and ensure the Diagnosis is ready to run.

3.6.2 Defining an Endpoint-to-Endpoint Diagnosis

To diagnose a VoIP problem between two endpoints, select **Endpoints** as your Device Type. Vivinet Diagnostics will trace the path taken by VoIP traffic between the two endpoints you select. Endpoints are computers on which you installed Performance Endpoints. For more information, see Section 1.7, “NetIQ Performance Endpoints,” on page 13.

If you select endpoints connected only by switches, in other words, if there are no routers in the path, your Diagnosis produces a Path Trace showing the source and destination endpoints with no devices between them. Vivinet Diagnostics still collects data, but does not generate a warning or error about an empty path.

Complete the remaining fields as shown below. Then, run the Diagnosis by clicking the **Diagnose** tab. For more information, see Section 3.7, “Diagnosing the Problem (Step 2),” on page 45.

Field	Description
Endpoint 1	Acts as the source Target Device. The simulated (bidirectional) VoIP traffic will originate with this endpoint, as if it had placed the VoIP call. Type the endpoint computer’s IP network address (in dotted notation such as `135.25.25.5`) or a DNS hostname, such as `devel_lab_netiq`.
Endpoint 2	An endpoint computer’s IP network address. Type a DNS hostname or the IP address of the endpoint computer in dotted notation.
Call Script	The type of simulated VoIP test traffic to send between the endpoints. Call scripts are given names that identify the codec they emulate. Select the codec in use on your network. If you are using another NetIQ product, use the same call script you used when you first discovered the problem.
View button	Click to see the parameters configured in the call script. To change any parameter, you must add a new call script. For more information, see Section 4.2, “Working with Call Scripts,” on page 58.
Validate button	Click to save all parameters of your problem definition and ensure the Diagnosis is ready to run.

3.6.3 Defining an IP Phone-to-Other Diagnosis

To diagnose a VoIP problem between an IP phone and a *non-phone* Target Device such as a router or a Cisco IP telephony H.323 voice gateway, select **IP Phone-to-Other** as your Device Type. Vivinet Diagnostics will trace the path taken by VoIP traffic between the two devices you select.

Use this Device Type when performing a Diagnosis between an IP phone and a Cisco CallManager Express device. For more information, see Section 5.1.3, "Other Properties," on page 75.

Complete the remaining fields as shown below. Then, run the Diagnosis by clicking the **Diagnose** tab. For more information, see Section 3.7, "Diagnosing the Problem (Step 2)," on page 45.

Field	Description
Phone 1	An IP telephone. Considered the source of the call traffic that experienced a problem. Type the IP phone's full phone number, such as `222-555-1212`, or the phone's extension, such as `6003`. **NOTE**: If you want to diagnose a Nortel phone and the Directory Number is not unique across the Call Servers, ensure you type the Terminal Number (TN) instead of the phone number. Type the TN using the following format: `xxx-yy`. If you omit the embedded dash, Vivinet Diagnostics will be unable to find the TN on the Call or Signaling Server.
Other	The IP address of the non-phone Target Device, such as a router or a gateway. Type the DNS hostname or the IP address of the Target Device in dotted notation, such as `10.46.4.15`.
Validate button	Click to save all parameters of your problem definition and ensure the Diagnosis is ready to run.

3.7 Diagnosing the Problem (Step 2)

In the Diagnose view, run a Diagnosis by clicking **Start Diagnosis**. The first time you start a Diagnosis, you may see the Verify SNMP Settings dialog box, which reminds you to provide the SNMP permissions currently in use on your network. The permissions allow Vivinet Diagnostics to gather information from your network devices. For more information, see Section 3.5.1, "Configuring SNMP Permissions," on page 32.

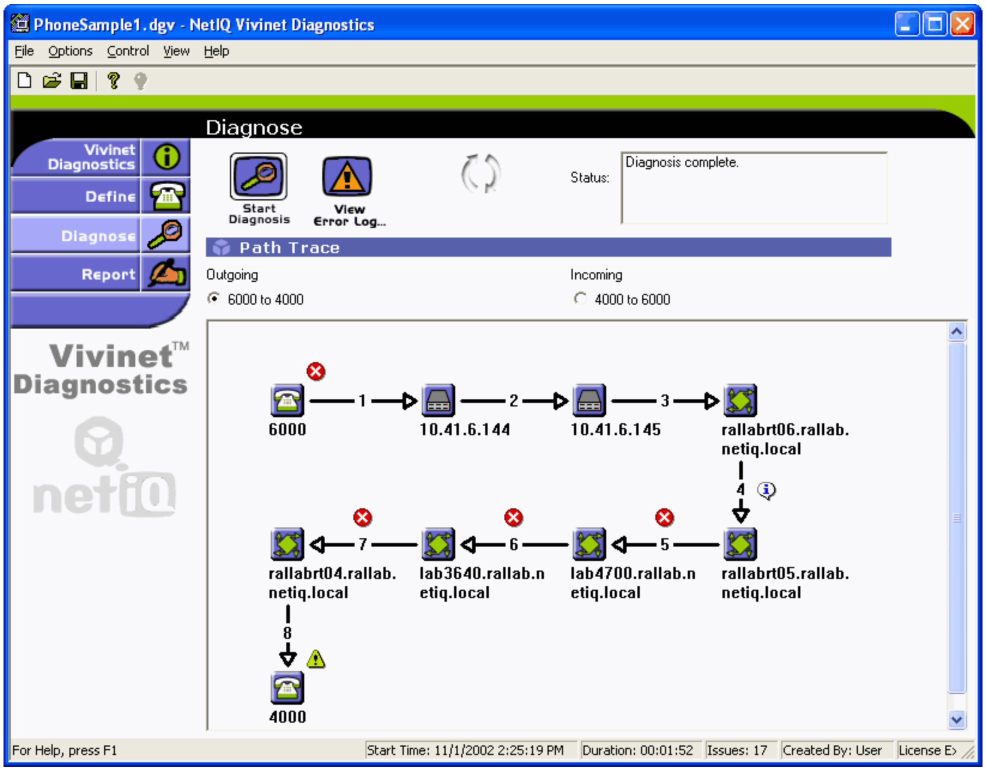
NOTE: Unless your network is still using default SNMP permissions, which creates a risky network security hole, you need to provide your network's SNMP permissions information in the SNMP Properties dialog box so Vivinet Diagnostics can query your network devices. Click Verify in the dialog box to type this information.

The Diagnose view shows you how a Diagnosis is proceeding. The **Status** field is continually updated, and the green arrows remain in motion until the status reads "Diagnosis completed."

After the Path Trace appears in the Diagnose view, icons represent the network devices in the path, and arrows indicate links between devices. Click a link or device icon to view identifying details about that device or link. A severity icon is displayed next to devices or links that have issues. Click the severity icons for information about the issue that has been detected. From any device, link, or severity properties dialog box, press **[F1]** to view definitions of the data shown and get help with diagnostic information.

If an error occurs, the **View Error Log** button is enabled. However, depending on the severity of the error, the Diagnosis may still complete. Click **View Error Log** to find out what happened. You then can stop the Diagnosis and change configuration parameters before starting it again. For more information, see Chapter 6, "Troubleshooting," on page 105.

Vivinet Diagnostics keeps track of the status of the Diagnosis and displays it in the window, along with the number of potential issues it has uncovered in your network. Devices having more than one Diagnosis display only one icon, so the number of issues may not correspond with the number of icons.


PhoneSample1.dgv - NetIQ Vivinet Diagnostics
File
Options
Control
View
Help
Diagnose
Vivinet Diagnostics
Define
Diagnose
Report
Vivinet™ Diagnostics
netiQ
Start Diagnosis
View Error Log...
Path Trace
6000
1
10.41.6.144
2
10.41.6.145
3
rallabrt06.rallab.netiq.local
4
rallabrt05.rallab.netiq.local
5
lab4700.rallab.netiq.local
6
lab3640.rallab.netiq.local
7
rallabrt04.rallab.netiq.local
8
4000

Status: Diagnosis complete.

Outgoing

● 6000 to 4000

Incoming

○ 4000 to 6000

For Help, press F1 | Start Time: 11/1/2002 2:25:19 PM | Duration: 00:01:52 | Issues: 17 | Created By: User | License E>

Although the Diagnose view lets you stop a Diagnosis that is in progress, Vivinet Diagnostics also stops the Diagnosis when all actions necessary to gather the appropriate information have been completed.

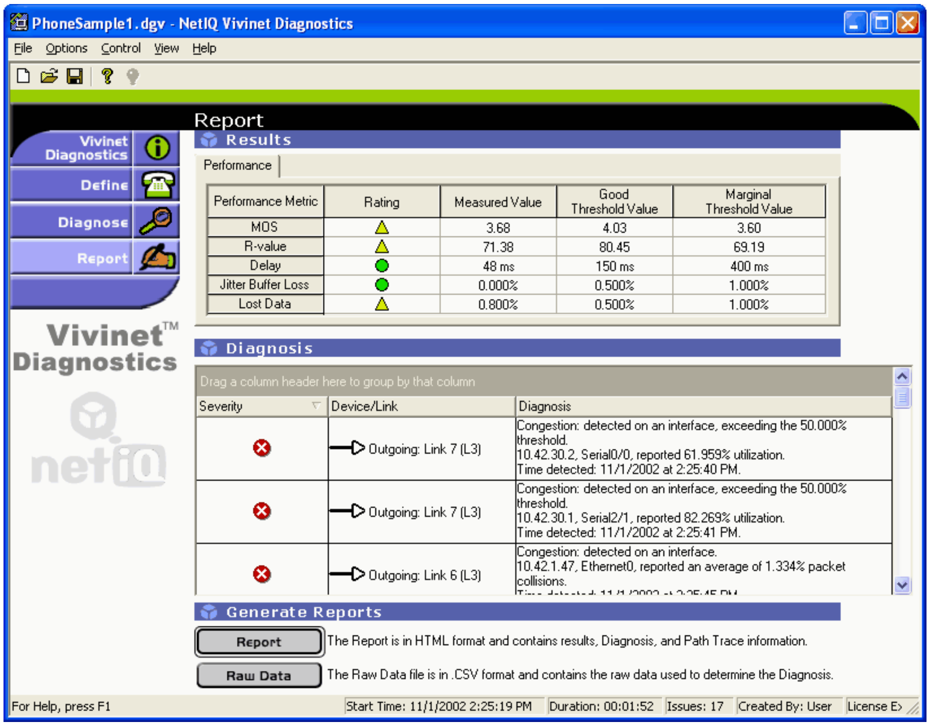
When you run a Diagnosis again, previous results are deleted.

Diagnose View Component	Description
Start Diagnosis button	Starts the Diagnosis. Becomes a **Stop Diagnosis** button while a Diagnosis is running.
View Error Log button	Accesses the Error Log Viewer, which lets you sort and filter errors and analyze their causes. This button is enabled only if errors exist. For more information, see Section 6.3, “Error Log Viewer,” on page 109.
Status field	The current status of the Diagnosis. The status reads “Diagnosis running” while the Diagnosis runs and “Diagnosis complete” when the Diagnosis has completed, as well as a list of all tasks that are performed.
Path Trace	A schematic diagram showing all devices and links that handle the VoIP traffic between the two Target Devices. Click the Outgoing and Incoming radio buttons to see the path in either direction. For more information, see Section 5.1, “Reviewing Path Trace Components,” on page 71.
Severity icons	Indicate a potential problem has been found in a device or link. Click these icons to view details about each problem. Press **[F1]** for help and advice.

3.8 Reporting the Results (Step 3)

As soon as a Diagnosis is complete, you can see a summary of the results and generate a report. For more information, see Chapter 5, “Understanding Results,” on page 71.

Click the **Report** tab to enter the Report view.



Performance Metric	Rating	Measured Value	Good Threshold Value	Marginal Threshold Value
MOS	△	3.68	4.03	3.60
R-value	△	71.38	80.45	69.19
Delay	●	48 ms	150 ms	400 ms
Jitter Buffer Loss	●	0.000%	0.500%	1.000%
Lost Data	△	0.800%	0.500%	1.000%

Drag a column header here to group by that column

Severity	Device/Link	Diagnosis
⊗	Outgoing: Link 7 (L3)	Congestion: detected on an interface, exceeding the 50.000% threshold. 10.42.30.2, Serial0/0, reported 61.959% utilization. Time detected: 11/1/2002 at 2:25:40 PM.
⊗	Outgoing: Link 7 (L3)	Congestion: detected on an interface, exceeding the 50.000% threshold. 10.42.30.1, Serial2/1, reported 82.269% utilization. Time detected: 11/1/2002 at 2:25:41 PM.
⊗	Outgoing: Link 6 (L3)	Congestion: detected on an interface. 10.42.1.47, Ethernet0, reported an average of 1.334% packet collisions. Time detected: 11/1/2002 at 2:25:45 PM

Report The Report is in HTML format and contains results, Diagnosis, and Path Trace information.

Raw Data The Raw Data file is in .CSV format and contains the raw data used to determine the Diagnosis.

For Help, press F1 | Start Time: 11/1/2002 2:25:19 PM | Duration: 00:01:52 | Issues: 17 | Created By: User | License E>

Report View Component	Description
Results table	Summarizes the call performance results of diagnostic tests run between the endpoints or, if your Diagnosis used phones, the call performance data collected from network devices. The Mean Opinion Score (MOS) is the overall estimation of VoIP call quality between the Target Devices. The remaining data shows how the MOS was derived, based on delay, jitter buffer loss, and lost data statistics. These statistics have been compared to the thresholds configured for each VoIP performance metric. The green, yellow, or red rating icons provide an instant sense of whether performance was acceptable. Any performance metrics gathered on the network are defined only as “issues” if they conform to the thresholds you set. For more information, see Section 3.5.5, “Setting Thresholds,” on page 37 and Section 5.2.1, “Interpreting the Results Table,” on page 88. **NOTE**: In a Cisco environment for which no endpoints are available in the subnets where you are performing the Diagnosis, you will receive results for, at most, “Lost Data” and “Delay.” The same is not true for a Nortel environment. Even without endpoints, `RTPStatShow` can provide R-value and MOS. And if the Diagnosis was launched by an R-value trap event in AppManager, you will receive all expected VoIP metrics.
Diagnosis table	Summarizes any issues found to provide a Diagnosis of the problem. The severity icons provide quick identification of problem. The issues are sorted by severity (high to low). Network problems can include major issues, minor configuration problems, unstable routing, excessive router delays, and more. All discovered issues are accompanied by an explanation. For more information, see Section 5.2.2, “Interpreting the Diagnosis Table,” on page 90.
Generate Reports	Offers two result formats: an HTML-formatted Report, and a Raw Data file in comma-separated values (CSV) format, suitable for a spreadsheet program, such as Microsoft Excel. For more information, see Section 3.8.1, “Diagnosis HTML Report,” on page 48 and Section 3.8.2, “Raw Data File,” on page 49.

3.8.1 Diagnosis HTML Report

After Vivinet Diagnostics has located one or more potential problems with your VoIP implementation, you can print or view a report of the findings. You can create an HTML report or a comma-separated values (CSV) file from the Report view. For more information, see Section 3.8.2, “Raw Data File,” on page 49.

The HTML report provides easy access to the highlights of the Diagnosis, along with details about how the Diagnosis was conducted.

The report summarizes the problem as you defined it, including the addresses or phone numbers of the Target Devices, presents a graphic depiction of the Path Trace it performed, and then lists and describes the probable sources of the problem.

To generate the HTML report:

1 In the Report view, click **Report**. The report is generated in HTML format so you can view it in your Web browser. You can regenerate the report at any time from a saved Diagnosis file.

2 To save the report while the report is open in your Internet Explorer browser window, click **Save As** on the File menu, and then choose one of the following options from the **Save As Type** list:

- **Save As Web page, complete** to save the Web page in its original format (`.htm`), including all graphics and style sheet files.
- **Save As Web page, archive** to save a snapshot of the current Web page in MHTML (`.mht`) format, including all graphics.

TIP: You can also generate the HTML report from a command-line interface on the Vivinet Diagnostics computer. Type the following at the prompt:

```
diagnostics.exe -h -v report -r html [name of diagnosis].dgv
```

3.8.2 Raw Data File

Although Vivinet Diagnostics contains expert-level information about the factors that affect VoIP call quality and performance, you cam perform your own analysis of the data the application has uncovered. If you want to independently analyze the data collected from your network during a Diagnosis, use the Raw Data file to gather data in a useful format.

When you click the **Raw Data** button, all of the data Vivinet Diagnostics used to create the report is exported to a text file in comma-separated values (`CSV`) format. Files in `CSV` format can be opened in Microsoft Excel.

TIP: Some spreadsheet programs, such as Microsoft Excel, may truncate the decimals in large numbers for display purposes. However, the actual full value is stored and used for calculations. If you suspect your spreadsheet is not displaying decimals, you can format the affected cells as “Numeric” and specify the number of decimal digits you want to display.

Understanding the Raw Data File

The Vivinet Diagnostics Raw Data file is a comprehensive collection of data gathered during a particular Diagnosis. When you first take a look at a Raw Data file from a typical Diagnosis, you may have a few questions about some of the abbreviations used and what is included in the file.

The Raw Data file, with file extension `.csv`, is saved by default to the `/My Documents` folder on the local computer. Again by default, this file has the same filename as the Diagnosis it reflects. Open this file using a compatible spreadsheet program, such as Microsoft Excel. It is divided into several major sections, designated by headings in all-capital letters.

The **Product Information** section provides version information about the Vivinet Diagnostics Console used to run the Diagnosis. Just below that is the **Diagnosis Summary**, with information about when the Diagnosis was run, the number of network issues it found, and any voice gateways discovered on the network.

Next is information about **Diagnosis Configuration**, divided into subsections:

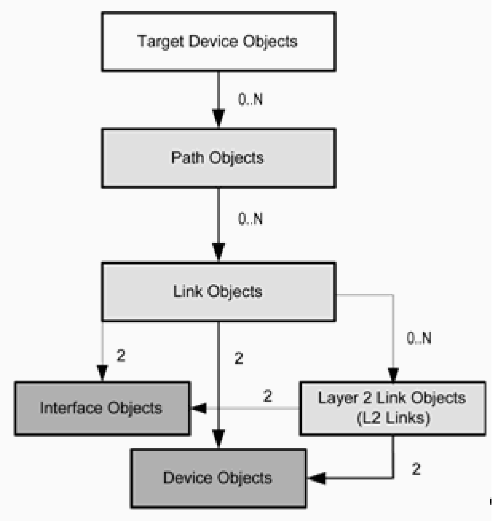
Subsection	Description
CallManagers	Lists the IP addresses or DNS hostnames of the Cisco CallManagers you added or that were discovered by Vivinet Diagnostics.
Call Servers	Lists the IP addresses of the Nortel Call Servers involved in the Diagnosis.
Signaling Servers	Lists the IP addresses of the Nortel Signaling Servers involved in the Diagnosis.
Firewall Port	Lists the port you designated for diagnostic traffic sent between the endpoints through a firewall.
Call Script	Provides the name of the call script (codec) used and indicates how call script parameters were set. **NOTE**: Very infrequently, the codec indicated in the **Call Script** section does not match the codec identified in the **Quality Stats** section. The Quality Stats section identifies the codec in use in your environment. If that codec is not supported, Vivinet Diagnostics uses G.711u to drive VoIP traffic. G.711u mimics the traffic behavior of the known unsupported codecs. For more information, see Section 4.2.2, “Reviewing Codecs,” on page 60.
QoS	Reports whether QoS was applied and what bit settings were used.
Thresholds	Shows all the thresholds configured for a Diagnosis.

The **Problem Definition** section lists the device type (endpoints, phones, or other — such as gateways and routers), each Target Device’s IP address or DNS hostname, the time the problem occurred, and, if endpoints were the Target Devices, the call script used for the simulated VoIP performance test traffic.

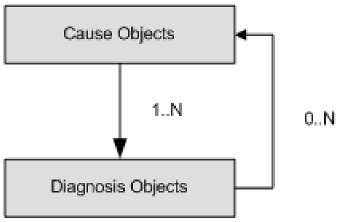
The last sections contain the **Results** and the **Quality Stats**. First, the results from VoIP performance tests are shown, including what was measured for each performance metric (MOS, R-value, Delay, Lost Data, and Jitter Buffer Loss), the severity rating of each measurement (such as “Marginal” or “Poor”), and the configured values for both Good and Marginal thresholds.

Next, the quality statistics for any Nortel devices are shown, followed by the addresses of any voice gateways discovered on the network during the Diagnosis are provided. And finally, raw results summarizing all the objects found in the path and their statistics are shown. For more information, see “Field Definitions for the Raw Data File” on page 51.

Within the Raw Data file, the following relationships organize the data objects you see:



The drawing shows that the Target Device Objects are treated as parents to all other object types. “Path Objects” define Path Traces that are generated whenever a Diagnosis is run and depicted graphically in the Diagnose view. They are owned by the two Target Devices whose VoIP data path they define. Numbers in the drawing above indicate the number of objects contained by each parent object. Furthermore, all Diagnoses contain 0 to *N* Diagnosis objects, 0 to *N* Stat (statistic) objects, and 0 to *N* Cause objects. All Cause objects must have at least one Diagnosis object.



All Vivinet Diagnostics objects, such as the two Target Devices you specified when you defined the problem on your network, are assigned an object ID number. Along with other statistics pertaining to an object, that object’s parent in the containment hierarchy is also indicated. The Target Devices are always assigned object IDs 1 and 2. So, for example, the endpoint named Device 1 (the first Target Device specified) with object ID 1 might be shown to have a parent link with object ID 5.

Field Definitions for the Raw Data File

The following table defines some of the unfamiliar fields in the Raw Data file.

For more information about what is shown in the `CSV` file, see the following related topics.

- Section 5.1.3, “Other Properties,” on page 75
- Section 5.1.5, “Router Properties,” on page 80
- Section 5.1.6, “Switch Properties,” on page 81
- Section 5.2.1, “Interpreting the Results Table,” on page 88
- Section 5.2.2, “Interpreting the Diagnosis Table,” on page 90
- Appendix A, “Cisco Unified CallManager Termination Codes,” on page 137

Field	Definition
ATM Objects	Owned by interface objects. Relevant properties are defined as follows: ◆ name—interface name ◆ hostname—interface's IP address ◆ idx—numeric index assigned to this interface in SNMP tables ◆ physaddr—physical (MAC) address of interface ◆ state—whether object is active or inactive ◆ uptime—number of seconds the interface has been active ◆ errors—number of hardware errors that have occurred ◆ qos—Quality of Service class specified for the interface
Call Objects	A single Cisco CallManager Call Detail Record representing information about a single VoIP call. For more information, see "Phone Call Details Tab" on page 78.
Cause Objects	The Probable Causes of issues flagged on the network during a Diagnosis. Relevant properties are defined as follows: ◆ name—probable cause of one or more diagnoses ◆ location—IP address of device, interface, or path where issue was flagged ◆ instance—specific instance information for the flagged issue ◆ diagnoses—issues caused by or related to this cause For more information, see "Probable Cause Definitions" on page 91.
CCME Devices	Devices for Cisco CallManager Express, also known as Unified Communications Manager Express
CCME Phones	Phones registered to Cisco CallManager Express devices
Device Objects	A router, a voice gateway, or a switch. For more information, see Section 5.1.5, "Router Properties," on page 80 and Section 5.1.6, "Switch Properties," on page 81.
Diagnosis Objects	A diagnostic response to issues flagged on the network during a Diagnosis. Relevant properties are defined as follows: ◆ severity—severity of the problem, based on the extent to which a performance metric exceeded a threshold: MAJ - Error MIN - Warning INF - Information ◆ location—IP address of device, interface, or path where issue was flagged ◆ instance—specific instance information for the flagged issue ◆ stat—name of statistic or other data that caused the issue to be flagged ◆ diagnosis—diagnosis provided by Vivinet Diagnostics ◆ causes—list of identifiers that caused (in part or whole) this diagnosis For more information, see Section 5.2.2, "Interpreting the Diagnosis Table," on page 90.

Field	Definition
Ethernet Objects	An Ethernet-enabled router or switch interface owned by interface objects. Relevant properties are defined as follows: ◆ state—device sending/receiving mode, such as full-duplex or half duplex ◆ uptime—number of seconds the device has been active ◆ errors—number of hardware errors that have occurred ◆ deferred—number of packets delayed due to link activity ◆ collisions—number of packets that experienced collisions ◆ multiple—number of packets that experienced multiple collisions ◆ lost—number of packets lost due to link activity
Frame Relay Objects	Owned by interface objects. Relevant properties are defined as follows: ◆ name—DLCI (data link connection identifier) ◆ state—status of the device, such as active or invalid ◆ uptime—number of seconds the device has been active ◆ fecns—forward explicit congestion notifications ◆ becns—backward explicit congestion notifications ◆ committed—circuit committed burst ◆ excess—circuit excess burst ◆ throughput—circuit throughput
GW Call Level Objects	Statistics from the voice gateway for recent POTS call legs
GW Call Objects	Statistics from the voice gateway for active POYTS and VoIP call legs
GW Call Stat Objects	Statistics from the voice gateway for recent VoIP call legs
Interface Objects	A router or switch interface owned by a link object or a Layer 2 link (L2 link) object. It may own Ethernet objects. Relevant properties are defined as follows. ◆ idx—numeric index assigned to this interface in SNMP tables ◆ mtu—maximum transmission unit or maximum frame payload size configured for this medium ◆ speed—media speed of interface in bits/second Properties not defined here are defined in the ATM Objects definition. Other properties are stat objects and are described in Appendix B, “Statistics Used in Diagnoses,” on page 145.
Link Objects	Defined by router interfaces. Vivinet Diagnostics finds links by running traceroute tests. The name property is derived from the resolved DNS hostname of the egress interface. For more information, see Section 5.1.2, “Link Properties,” on page 73.
L2 Link Objects	Defined by switch interfaces functioning at Layer 2 of the OSI (Open System Interconnection) Model. Some router interfaces may also function at Layer 2. For more information, see Section 5.1.2, “Link Properties,” on page 73.
Path Objects	Defines the Path Trace generated for a Diagnosis. Every Diagnosis has two path objects because the Path Trace can be shown from either direction between the two Target Devices. For more information, see Section 5.1, “Reviewing Path Trace Components,” on page 71.

Field	Definition
Phone Objects	Telephone used as Target Device in the Diagnosis. Parent of Path Objects. May be either an IP phone or a POTS phone. For more information, see Section 5.1.4, “Phone Properties,” on page 76.
RTP Objects	Values gathered by Nortel RTCP-XR or RTCP. Relevant properties are defined as follows: ◆ far end IP addr—IP address of the destination phone ◆ local packets sent—number of RTP packets sent by the source phone ◆ remote packets sent—number of RTP packets sent by the destination phone ◆ local packets received—number of RTP packets received by the source phone ◆ remote packets received—number of RTP packets received by the destination phone ◆ local packets received out of order—number of out-of-order RTP packets received by the source phone ◆ remote packets received out of order—number of out-of-order RTP packets received by the destination phone ◆ local packet loss—number of RTP packets sent by the source phone that were not received by the destination phone ◆ remote packet loss—number of RTP packets sent by the destination phone that were not received by the source phone ◆ local avg jitter—average jitter for the source phone ◆ remove avg jitter—average jitter for the destination phone ◆ local listening R-value—call quality R-value on the source phone ◆ remote listening R-value—call quality R-value on the destination phone ◆ local latency—amount of one-way network delay, packetization delay, and jitter buffer delay on the source phone ◆ remote latency—amount of one-way network delay, packetization delay, and jitter buffer delay on the destination phone ◆ local codec—codec in place on the source phone ◆ remote codec—codec in place on the destination phone ◆ local avg net loss rate—RTCP-XR statistic used to compute lost data value for source phone. This is a raw value as reported by the phone. Divide by 256 to determine the percentage value. ◆ remote avg net loss rate—RTCP-XR statistic used to compute lost data value for destination phone. This is a raw value as reported by the phone. Divide by 256 to determine the percentage value. ◆ local avg discard rate—RTCP-XR statistic used to compute jitter buffer loss value for source phone. This is a raw value as reported by the phone. Divide by 256 to determine the percentage value.

Field	Definition
RTP Objects	◆ remote avg discard rate—RTCP-XR statistic used to compute jitter buffer loss value for destination phone. This is a raw value as reported by the phone. Divide by 256 to determine the percentage value. ◆ local avg burst density—RTCP-XR statistic used to compute burst density for source phone. This is a raw value as reported by the phone. Divide by 256 to determine the percentage value. ◆ remote avg burst density—RTCP-XR statistic used to compute burst density for destination phone. This is a raw value as reported by the phone. Divide by 256 to determine the percentage value. ◆ local avg burst length—average length of a burst density period on the source phone ◆ remote avg burst length—average length of a burst density period on the destination phone ◆ local gap density—percentage of packet loss during a gap period, the period of time between bursts, for the source phone. This is a raw value as reported by the phone. Divide by 256 to determine the percentage value. ◆ remote gap density—percentage of packet loss during a gap period, the period of time between bursts, for the destination phone. This is a raw value as reported by the phone. Divide by 256 to determine the percentage value. ◆ local gap length—length of a gap period for the source phone ◆ remote gap length—length of a gap period for the destination phone ◆ local avg end system delay—average system delay for the source phone. System delay is the sum of jitter buffer and codec encoding and decoding. ◆ remote avg end system delay—average system delay for the destination phone. System delay is the sum of jitter buffer and codec encoding and decoding. ◆ local avg noise level—average level of interference present at the source phone. The lower the value, the less background noise present. ◆ remote avg noise level—average level of interference present at the destination phone. The lower the value, the less background noise present. ◆ local avg signal power—average signal strength for all received packets at the source phone. The higher the value, the stronger the signal. ◆ remote avg signal power—average signal strength for all received packets at the destination phone. The higher the value, the stronger the signal. ◆ local round trip time avg—average length of time for a call to travel to the destination phone and back ◆ remote round trip time avg—average length of time for a call to travel to the source phone and back ◆ local round trip hi—maximum length of time for a call to travel to the destination phone and back ◆ remote round trip hi—maximum length of time for a call to travel to the source phone and back ◆ source ip address—IP address of the source phone ◆ source port—port number of the source phone Properties not defined here are defined in “Phone Quality Stats Tab” on page 79. For more information, see Section 5.3.1, “Burst Density,” on page 100 and Section 5.3.9, “R-value,” on page 104.

Field	Definition
Serial Objects	Represent the basic Layer 2 “serial” interfaces for certain WAN links
Stat Objects	A type of statistic gathered by Vivinet Diagnostics during a Diagnosis. Relevant properties are defined as follows: ◆ device—type of object associated with the statistic, such as “Link” for a link object or “Path” for a path object ◆ interval—number of milliseconds between samplings ◆ attempts—number of sampling attempts made ◆ completed—number of successful sampling attempts ◆ smin—smallest value sampled ◆ tmin—number of milliseconds into the polling operation that the minimum value was sampled ◆ smax—largest value sampled ◆ tmax—number of milliseconds into the polling operation that the maximum value was sampled ◆ avg—average value sampled ◆ stdv—Standard Deviation of all sampled values For more information, see Appendix B, “Statistics Used in Diagnoses,” on page 145.
Target Objects	Devices selected as Target Devices. For more information, see Section 5.1.1, “Endpoint Properties,” on page 72 and Section 3.6, “Defining the Problem (Step 1),” on page 43.
Traffic Class Objects	Details about the traffic classes defined on Cisco devices
Voice Analog Objects	Details about the POTS interfaces used for voice traffic
Voice Dial Peer Objects	POTS dial peer definitions for a voice gateway
Voice Digital Objects	Details about the VoIP interfaces used for voice traffic
VoIP Dial Peer Objects	VoIP dial peer definitions for a voice gateway

4 Networking Guidance

The following topics discuss networking concepts related to VoIP implementations and provide guidance for planning and configuration as you begin VoIP diagnoses on your network.

4.1 Running a Diagnosis Through a Firewall

During a Diagnosis, Vivinet Diagnostics runs two simulated VoIP telephone calls, one in each direction, between two Target Devices on the network to test VoIP performance. If a firewall is present between these devices, you need to specify a port to use for this RTP traffic.

To set a specific port for test VoIP traffic, click **Firewall** on the Options menu. The **Call Traffic Port** value in the Firewall dialog box refers to the firewall port through which simulated VoIP traffic will travel during a Diagnosis.

The port setting you supply applies only to the present Diagnosis unless you select **Set As Default**. When you set a new port as the default, Vivinet Diagnostics uses it in any new Diagnosis you run. You can change this value at any point. Existing results will not be affected. Click **Restore Default** to replace any current value with the default value. Until you change the setting and select **Set As Default**, the default call traffic port is AUTO, which means the Target Devices select the port dynamically during VoIP performance testing.

Vivinet Diagnostics also runs traceroute tests using RTP or ICMP packets between the Target Devices. A firewall may prevent the traceroute from providing information about the path, so configure the firewall to allow the traceroute to work.

Finally, because Vivinet Diagnostics uses SNMP to query routers and switches along the path, configure the firewall to pass SNMP traffic.

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 Diagnostics Console and the Target Devices, or between the Target Devices themselves. However, for any firewall, click **Firewall** on the Options menu to ensure your firewall and Console settings are in agreement.

4.1.1 NAT-Enabled Firewalls

Network Address Translation (NAT) can disrupt VoIP networks because the addresses the firewall needs to translate are hidden within the payload of each VoIP packet. One solution 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 non-secure side. With *dynamic* NAT, in which all internal IP addresses are mapped to a single external address on the unsecure side, you are unable to run a Diagnosis through the firewall because you cannot send UDP (RTP) packets to an overloaded address.

With static NAT enabled between the Target Devices, provide the static NAT IP address as the address for Endpoint 2 when you configure a Diagnosis. Vivinet Diagnostics then communicates with Target Device 1 using TCP on the secure side of the firewall.

If the firewall is located between the Console and the Target Devices, see Section 4.1.2, “All Firewalls,” on page 58.

4.1.2 All Firewalls

Use the Firewall dialog box to configure a Call Traffic Port range. Call Traffic refers to bi-directional VoIP traffic between Target Devices using RTP, which is recognized as UDP by many firewalls.

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

Location	Configuration Details
Firewall located between the Console and the endpoints	Configure this firewall to pass TCP streams from the Console through port 10115 to the endpoints.
Firewall located between the endpoints	Configure this firewall to pass bi-directional VoIP (RTP) streams through a port. In addition, configure the firewall to pass bi-directional TCP and UDP streams through port 10115 — the endpoints need to be able to send setup and clock synchronization messages to each other through the firewall. In addition, configure the firewall to pass ICMP responses. On the Firewall dialog box, type the call traffic port you configured at the firewall for VoIP RTP (UDP) flows between the endpoints. The default **Call Traffic Port** setting, **AUTO**, lets the endpoints choose the port dynamically. For VoIP traffic, the endpoints use even-numbered ports between 16384 and 65534.
Firewall located between the Console and Cisco IP phones	Configure the firewall to pass TCP HTTP requests, through Port 80, to the phones selected as Target Devices. When you define the problem using phones, Vivinet Diagnostics needs to be able to contact the phones to extract information about their calls, about their network configuration, and about their CallManager.
Firewall located between the Console and one or more CallManagers	Configure the firewall to pass TCP through port 1433, the well-known port for SQL Server. Vivinet Diagnostics needs to be able to access the CallManager SQL database to retrieve CDRs. The firewall also needs to pass bi-directional UDP traffic using port 161.
Firewall located between the Console and the Signaling Server and Call Server	The telnet port (Port 23) for the Signaling Server must be open, as should the rlogin port (Port 513) for the Call Server. And, in order for AppManager to trigger a Diagnosis if the R-value trap is received, the SNMP trap port must be open. Otherwise, traps cannot pass from the Signaling Server to the trap receivers.
Firewall located between the Console and network devices along the path	Configure this firewall to pass bi-directional UDP traffic using the SNMP port (161) between the Console and network devices between the Target Devices. And it also needs to pass bi-directional UDP traffic using the TFTP port (69).

4.2 Working with Call Scripts

Vivinet Diagnostics call scripts emulate each of the following popular codec types: G.711u, G.711a, G.726, G.729, G.729A, G.723-ACELP, and G.723-MPMLQ. In each call script, parameters such as the size of the jitter buffer to emulate are selected for you. To change a parameter value, create a new call script based on one of the default scripts.

4.2.1 Creating or Editing a Call Script

By default, call scripts correspond to codecs, as indicated by their names. Although you cannot change default call scripts, you can create new call scripts based on the default scripts. After you create a call script with customized settings, you assign it a name to distinguish it from the default call script on which it was based. A call script you modify and rename is available in the Call Scripts List dialog box and can be edited.

To review a call script's parameters, click **Call Scripts** on the Options menu. Select a script and click **View**.

To create a new call script based on an existing script, click **Call Scripts** on the Options menu. Select the script you want to copy and click **Copy**.

To create a new call script from scratch, click **Call Scripts** on the Options menu and then click **Add**.

To modify a call script you created, click **Call Scripts** on the Options menu. Select the script you want to edit and click **Modify**. You cannot modify a default script.

To delete a call script you created, click **Call Scripts** on the Options menu. Select the script you want to delete and click **Delete**. You cannot delete a default script.

The following table defines the fields on the Add a Call Script dialog box. The default call script parameters affect how test traffic appears to devices on the network.

Field	Definition
Call Script name	The name of the call script. Can be the default name or one you assign to a new or copied script.
Codec	The type of codec used in your network. The default codec is G.711u. For more information, see Section 4.2.2, “Reviewing Codecs,” on page 60.
Packet Loss Concealment	Packet Loss Concealment (PLC) is enabled in the G.711 call scripts because VoIP phones that use this codec now perform PLC. For more information, see Section 4.2.3, “Understanding Packet Loss Concealment,” on page 60.
Use silence suppression	Emulates the effects of silence suppression, or voice activity detection, on the line during the Diagnosis. Disabled in all call scripts. For more information, see Section 4.2.4, “Understanding Silence Suppression,” on page 61.
Override delay between voice datagrams	Determines the datagram size to be used in the call script. 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 value is 30 ms. For all other codecs, the value is 20 ms.
QoS name	Emulates the effects of a Quality of Service (QoS) scheme for VoIP calls. To enable QoS, select a QoS setting that determines how the traffic will be marked. QoS is not supported by all endpoint operating systems. For more information, see Section 4.3, “Working with Quality of Service,” on page 61.
Jitter buffer	Emulates the effects of jitter buffering on your VoIP network. Jitter buffers can 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 jitter buffer of two voice datagrams. For more information, see Section 4.2.5, “Defining Jitter Buffer,” on page 61.
Additional fixed delay	Additional milliseconds of delay you choose to add to a call.

4.2.2 Reviewing Codecs

In a VoIP transmission, the codec, short for compressor/decompressor, samples the sound and determines the data rate. If you installed Performance Endpoints on your network, you can perform diagnoses using various codec types, which are represented by call scripts in Vivinet Diagnostics. For more information, see Section 4.2, “Working with Call Scripts,” on page 58.

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. Vivinet Diagnostics uses this codec when running diagnoses in environments that use unsupported codecs. G.711u mimics the traffic behavior of the known unsupported codecs.
G.711a	ITU standard for H.323-compliant codecs. Uses the A-law for companding, a popular standard in Europe.
G.726	A waveform codec 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, this is a less-complex version of the G.729 codec. Developed for simultaneous voice and data applications for which the G.729 codec is too complex. Speech quality is virtually indistinguishable between G.729 and G.729A.
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.

4.2.3 Understanding Packet Loss Concealment

Packet Loss Concealment (PLC) is an option for the G.711u and 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, Vivinet Diagnostics assumes the quality of your conversation would be improved, but this improvement is only factored into the MOS calculation if any data is lost.

In the following table, **Packetization Delay** refers to the delay a codec introduces as it converts a signal from analog to digital. This delay is included in the MOS and in delay diagnoses on the Target Devices, as is the **Default Jitter Buffer Delay**, the delay introduced by the effects of buffering to reduce inter-arrival delay variations.

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

Codec	Default Data Rate	Default Datagram Size	Packetization Delay	Default Jitter Buffer Delay	Theoretical Maximum MOS
G.723.1-ACELP	5.3kbps	30 ms	67.5 ms	3 datagrams (60ms)	3.69

4.2.4 Understanding Silence Suppression

Call scripts include an option to use silence suppression in the VoIP call traffic Vivinet Diagnostics sends on the network between endpoints. Silence suppression is disabled in all call scripts.

Silence suppression occurs when no data is sent on the network during periods of call silence, that is, when no one is “talking” in the simulated call.

4.2.5 Defining Jitter Buffer

To minimize voice disruptions from delay and jitter, VoIP equipment typically has a jitter buffer. A jitter buffer can be either frame-based or absolute. A *frame-based* jitter buffer holds a given number of voice datagrams. 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 variability in arrival times. An absolute jitter buffer, on the other hand, might be set to 43 ms, and, given a typical 20-ms speech frame size, could hold two speech frames and allow for an extra three milliseconds of variability.

All call scripts used in Vivinet Diagnostics call performance tests emulate a frame-based jitter buffer of two datagrams.

During a Diagnosis, Vivinet Diagnostics calculates packet loss due to the sizes of the jitter buffers between the Target Devices and uses this statistic in estimating the quality of simulated VoIP calls. If jitter occurs on the network, jitter buffers can smooth it out, but they also exacerbate data loss: datagrams not contained by the jitter buffer are discarded. The *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 also 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. Buffering not only causes loss, but also adds delay, which can offset the positive effects of smoothing out jitter. Check the “**Jitter Buffer Loss**” statistic in the Results table of the Report view to see whether jitter buffers are also adding data loss. For more information, see Section 5.3.5, “Jitter Buffer Loss,” on page 102.

4.3 Working with Quality of Service

Using a prioritization or Quality of Service (QoS) scheme can make an enormous difference in call quality, particularly if you are running VoIP on a crowded enterprise network. Typically, QoS for VoIP specifies each voice datagram to be:

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

If you installed Performance Endpoints on the network, you can add a QoS component to the VoIP performance tests that run during a Diagnosis. Vivinet Diagnostics lets you configure QoS definitions to determine how the endpoints produce packets that emulate QoS bit settings.

By default, none of the Vivinet Diagnostics call scripts uses QoS, so the simulated VoIP flows sent over the network to test the call quality between the Target Devices will not be marked for any special handling.

To use QoS during a Diagnosis:

1. Select **Endpoints** as the device type.
2. On the Options menu, click **Call Scripts**. The Call Scripts List shows the names of the codecs the call scripts emulate.
3. Highlight the codec you want to emulate. Click **Add**.
4. In the **Call Script name** field, type a name to identify the edited version of this call script.
5. In the **QoS name** field, select the **VoIPQoS** definition, or select a QoS definition you configured. For more information, see Section 4.2.1, "Creating or Editing a Call Script," on page 59 and Section 4.3.2, "Creating DiffServ Definitions," on page 63.
6. Make any other changes to the call script, and click **OK** to save your settings.
7. Run the **Diagnosis**.

You can run the same Diagnosis again using the default version of the call script, that is, with no QoS selected, and compare the results to see what effect QoS is having on VoIP performance, if any.

You can customize and rename QoS definitions. For more information, see Section 4.3.2, "Creating DiffServ Definitions," on page 63.

4.3.1 Configuring Endpoints for Diagnoses with QoS

You may need to configure endpoints to allow for diagnostic testing with a QoS component. Some endpoint operating systems supported by Vivinet Diagnostics do not allow for setting the necessary bits for DiffServ QoS. The following table provides a summary:

Endpoint Operating System	Supports DiffServ?	Notes
Windows XP Windows 2000 Windows Server 2003 Windows Server 2008 Windows 7	Yes	Requires Registry setting
Linux	Yes	
Sun Solaris	Yes	

To allow for diagnoses with DiffServ definitions on Windows servers, an addition to the Registry is required. In the Registry Editor, add the following `DWORD` value at the endpoints:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableUserT
OSSetting = 0
```

Restart the endpoint computers after you edit their Registry settings. Then start the Diagnosis.

4.3.2 Creating DiffServ Definitions

To run a Diagnosis using DiffServ QoS settings, create a new DiffServ QoS definition and then add a new call script that uses the new definition.

To create a DiffSerf definition:

1 On the Options menu, click **QoS Definitions**, and then click **Add.**

2 In the **QoS name** field, assign a name to your definition.

3 From the Predefined DiffServ codepoints list, select a DiffServ bit setting. When you make your selection, the graphic illustrating the bit field settings changes to reflect your choice.

   Or, select **User-defined DiffServ codepoints** and then click each **Bit field settings** button to change the codepoints.

   For more information, see Section 4.3.3, "Understanding DiffServ Settings," on page 63.

4 Click **OK** to save your definition and then click **OK** to close the QoS List dialog box.

5 Add a new call script, selecting the new definition from the **QoS name** field. For more information, see Section 4.2.1, "Creating or Editing a Call Script," on page 59.

6 *To modify an existing DiffServ definition*, click **QoS Definitions** on the Options menu, select the definition you want to modify, and then click **Modify**. Follow the procedures described in steps 2 - 4.

7 *To delete an existing DiffServ definition*, click **QoS Definitions** on the Options menu, select the definition you want to delete, and then click **Delete**.

NOTE: Some endpoint operating systems require extra configuration to support DiffServ bit settings. For more information, see Section 4.3.1, "Configuring Endpoints for Diagnoses with QoS," on page 62.

Vivinet Diagnostics ships with a default QoS definition that lets you skip a step. When you select **VoIPQoS** from the **QoS name** field in the Add or Edit a Call Script dialog box, Vivinet Diagnostics 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.

4.3.3 Understanding DiffServ Settings

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 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 (CIR). To ensure traffic that exceeds the CIR is 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.

The following table shows the DiffServ choices available in Vivinet Diagnostics. Type of Service (TOS)-only settings are indicated as such:

Bit Settings	PHB Class
000000	Best Effort. Default setting 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)

The predefined QoS definition that ships with Vivinet Diagnostics, VoIPQoS, is a DiffServ definition that marks bits for Expedited Flow: highest-priority service — a TOS-only setting.

4.3.4 Reviewing Class-Based QoS

Vivinet Diagnostics provides support for diagnosing class-based, weighted fair queuing (WFQ) QoS through the `CISCO-CLASS-BASED-QOS-MIB`. This MIB (management information base) is present on Cisco devices you configured for QoS through the IOS configuration interface using the Modular QoS command-line interface.

The Module QoS class-map commands allow you to name traffic classes and to create match statements used to define how the class traffic looks, such as marking the VoIP traffic class with DSCP 5. Use the policy-map and service-policy commands to attach a class’s policy information to an interface. The policy commands allow you to specify options such as limiting bandwidth for a particular class.

For more information about configuring QoS policies on Cisco devices, see www.cisco.com/en/US/products/sw/iosswrel/ps5014/products_feature_guide_chapter09186a008008813a.html.

You can use Vivinet Diagnostics to diagnose traffic class utilization, queue discard rate, and queue depth.

QoS Component	Description
Traffic class	A particular category of traffic on an interface. For example, voice and data may be classified as individual traffic classes. Vivinet Diagnostics can provide diagnoses only for those traffic classes for which priority queuing is enabled. For details about enabling priority queuing, see the QoS configuration documentation for your device.
Queue	The virtual buffer associated with a particular traffic class.
Dropped packet rate	The rate at which packets are dropped due to factors such as queuing, policing, early detection, or traffic shaping.
Queue depth	The number of packets in a queue.
Policy	The action QoS takes within a traffic class upon the traffic that enters the class, such as dropping packets. Pre-policy traffic is the traffic that flows into a traffic class, before QoS applies a policy. Post-policy is the traffic that leaves a traffic class after a policy has been applied.

Vivinet Diagnostics gathers the necessary information from the `CISCO-CLASS-BASED-QOS-MIB`. However, this MIB is not available in the following scenarios:

- Your Cisco devices are running a version of IOS earlier than 12.1(5)
- QoS is not configured on your Cisco devices
- QoS is not configured with MQC, the Cisco QoS configuration mechanism
- Your Cisco switches are running CatOS, which does not have the QoS MIB

4.4 Understanding Layer 2 Trace

The nature of a corporate Layer 2 Ethernet network topology is a complicated proliferation of transmission technologies, Layer 2 switches, Layer 2/3 hybrid devices and VLAN technologies. Layer 2 corporate networks have no standardized infrastructure for performing a Layer 2 trace, such as the standard traceroute for Layer 3. By nature, the data gathered from a Layer 2 corporate network is dynamic, especially with respect to the SNMP Port Forwarding Database in Layer 2 switches.

Vivinet Diagnostics uses SNMP as its primary method of retrieving data from the Layer 2 environment. Because SNMP-implementation standards vary by vendor, you may need to define in Vivinet Diagnostics all of the Layer 2 devices in your network.

By understanding and implementing the ideas discussed in the following topics, you enable Vivinet Diagnostics to fully employ your Layer 2 as a data source.

4.4.1 FAQs

To make the best of the data you can retrieve from your Layer 2 devices, review the answers to the following frequently asked questions.

When should I configure devices?

If your network does not support LLDP and contains all Nortel switches or a mix of vendor switches, configure your Layer 2 devices before running your first Diagnosis. For more information, see Section 4.4.2, "Device Configuration," on page 68. You can change your configuration information at any time.

If you open a saved Diagnosis, the configured Layer 2 devices are those that appear in the Layer 2 Switch dialog box, which you can access from the Options menu. These devices may not be the same devices configured at the time you saved the Diagnosis.

Which switches should I configure?

For Target Devices on different subnets: In an all-Nortel environment, configure at least one switch in each Layer 2 segment of the trace, as well as every switch that does not support SONMP or LLDP. In an all-Cisco environment, configure every switch that does not support CDP. In an environment that contains a mix of Nortel and Cisco switched equipment, configure all of the Layer 2 switches because CDP and SONMP do not interact.

If a switch seems to be missing after running a Diagnosis, you may need to configure the switch's management address. You definitely need to configure the switches for vendors other than Nortel or Cisco.

For Target Devices on the same subnet: In an all-Nortel or all-Cisco environment, configure at least one known switch in the path, as long as CDP, SONMP, or LLDP is enabled on all switches. In an environment that contains a mix of Nortel and Cisco switched equipment, configure all of the Layer 2 switches because CDP and SONMP do not interact.

If a switch seems to be missing after you run a Diagnosis, you may need to configure the switch's management address. You definitely need to configure the switches for vendors other than Nortel and Cisco.

Do Cisco and Nortel devices have special requirements?

CDP must be enabled on Cisco devices. SONMP or LLDP must be enabled on Nortel devices. For more information, see the next two questions, and review Section 1.3, "Cisco Discovery Protocol," on page 11, Section 1.5, "Nortel SONMP or NDP," on page 12, and Section 1.6, "Link Layer Discovery Protocol," on page 13.

Does CDP need to be enabled?

Vivinet Diagnostics queries the results of Cisco Discovery Protocol (CDP) processing to discover Cisco Layer 2 devices that might be relevant to the Diagnosis. Once these Layer 2 devices are discovered, Vivinet Diagnostics sends them SNMP queries to find out where network issues are occurring. If CDP is disabled, devices will probably drop CDP packets and the Layer 2 trace will not progress past the point where the packets were dropped.

If you disabled CDP on any Cisco router or switch, re-enable it. For more information, see Section 1.3, "Cisco Discovery Protocol," on page 11.

Does SONMP need to be enabled?

Vivinet Diagnostics queries the results of SynOptics Network Management Protocol (SONMP) processing to discover Nortel Layer 2 devices that might be relevant to the Diagnosis. Once these Layer 2 devices are discovered, Vivinet Diagnostics sends them SNMP queries to find out where network issues are occurring. If SONMP is disabled, devices will probably drop SONMP packets and the Layer 2 trace will not progress past the point where the packets were dropped.

SONMP is enabled by default on Nortel switches. If you disabled it on any switch, re-enable it. For more information, see Section 1.5, "Nortel SONMP or NDP," on page 12.

What happens if CDP or SONMP is not enabled?

If LLDP is not enabled, Layer 2 switches for which SONMP or CDP is not enabled will be invisible to a diagnostic test or can bring the test to a halt. When SONMP or CDP is enabled, Vivinet Diagnostics can automatically determine the management IP addresses of physically neighboring Layer 2 switches.

Why are some devices "unordered"?

Devices can be labeled as "unordered" for several reasons:

- If you did not configure your Layer 2 devices, Vivinet Diagnostics cannot precisely pinpoint their location and so labels them as unordered.
- If you have not enabled SONMP, CDP, or LLDP, even configured devices are labeled as unordered.
- If your environment contains devices that do not support SONMP, CDP, or LLDP, such as devices from vendors other than Cisco and Nortel, Vivinet Diagnostics cannot pinpoint their location and so labels them as unordered.
- In a mixed-vendor Layer 2 environment in which Cisco devices run CDP and Nortel devices run SONMP, a Cisco switch will not know its neighbor is a Nortel switch — CDP and SONMP do not interact. In this situation, Vivinet Diagnostics cannot determine the correct placement for some devices.

Icons representing the unordered devices are displayed in a table below the Path Trace in the Diagnose view. For more information, see Section 5.1.7, "Unordered Devices," on page 82.

Why doesn't my device show up in a Path Trace or in the unordered device list?

Your Layer 2 device may not show up in a Path Trace or in the unordered list, for one or more of several reasons:

- Vivinet Diagnostics was unable to find references to the Target Device's MAC addresses in the Port Forwarding Database (PFD) of the switch.
- Vivinet Diagnostics was unable to determine the MAC address of the Target Device itself.
- Vivinet Diagnostics assumes recent traffic between Target Devices will leave entries in the Layer 2 device's PFD. If PFD entries have timed out, Vivinet Diagnostics is unable to determine whether the device was part of the Path Trace. The standard SNMP time-out for PFD entries is five minutes.

If one of the aforementioned errors occurs, a message is logged in the Error Log as a "not found" error for the `SNMP_Get_Forwarding_Port` action. The Error Log also lists all of the switch IP addresses for which Vivinet Diagnostics did not find a MAC address.

If an expected device does not appear in the Path Trace and its IP address does not appear in the Error Log, manually configure the device in Vivinet Diagnostics. If the device's IP address is not listed, then Vivinet Diagnostics did not query it. Manual configuration will make the device visible to Vivinet Diagnostics. However, if the IP address *is* listed, then the device was queried. Manual configuration will not make it any more visible to Vivinet Diagnostics.

For more information, see Section 4.4.2, "Device Configuration," on page 68.

4.4.2 Device Configuration

Vivinet Diagnostics has a stateless design. It does not retain knowledge learned between diagnoses. So when it runs diagnostic tests of Layer 2 devices, it performs a CDP/SONMP/LLDP discovery on every device associated with the Layer 2/Layer 3 path, looking for problems with VoIP quality. However, your Layer 2 could be so extensive as to cause Vivinet Diagnostics to perform a Diagnosis for longer than the expected three to ten minutes, thereby unduly burdening your network with diagnostic traffic.

Visible (configured) Layer 2 devices prevent Vivinet Diagnostics from overburdening your network when it performs sweeps of subnets during diagnoses. You can configure Vivinet Diagnostics with a list of the devices it should query for Layer 2 data and topology information.

NOTE

- Configuring many Layer 2 switches generally results in shorter diagnostic jobs. However, configuring many Layer 2 switches can result in more SNMP traffic because Vivinet Diagnostics queries every configured switch, even those not applicable to the current Diagnosis.
- Configuring a minimal number of Layer 2 switches results in less SNMP traffic, but a Diagnosis will take longer to run because Vivinet Diagnostics will have to perform more CDP/SONMP discoveries.
- The Vivinet Diagnostics Layer 2 trace implementation includes a throttle that prevents your network from being inundated with heavy SNMP traffic if many switches are manually configured.

Configure Layer 2 devices through the Options menu of the Vivinet Diagnostics Console, or create a text file that identifies every Layer 2 device in your network. This latter option is useful when you have more devices than you can conveniently enter through the Options menu.

To configure Layer 2 devices using the Options menu:

1. On the Options menu, click **Layer 2 Switch**, and then click **Add**.
2. In the **Layer 2 Switch** field, type the IP address or DNS hostname of a Layer 2 device in your network.

To create a text file identifying Layer 2 devices:

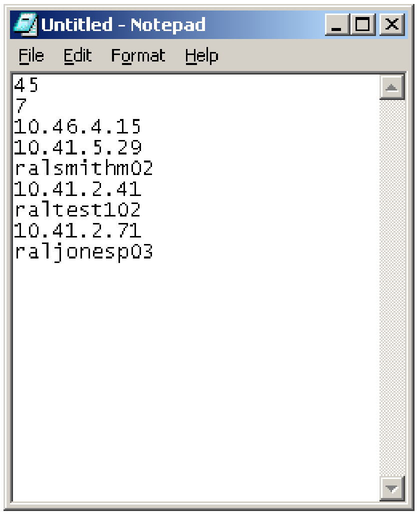
1. Using a text editor, such as Microsoft Notepad, create a blank text file.
2. Save it as `switchConfig.txt` into the following directory on the Vivinet Diagnostics Console computer:

   ```
   \Documents and Settings\All Users\Application Data\NetIQ\Vivinet Diagnostics
   ```

3. In the body of the text file, type a list of Layer 2 devices, using the following format:

   ```
   45
   X
   switch1IPaddressOrhostname
   switch2IPaddressOrhostname
   …
   switchXIPaddressOrhostname
   ```

where `X` = the number of switches. The "`45`" is a required entry that facilitates consistency checking, an internal function of Vivinet Diagnostics. The following is an example:



```
45
7
10.46.4.15
10.41.5.29
ralsmithm02
10.41.2.41
raltest102
10.41.2.71
raljonesp03
```

4 Save the text file as specified in Step 2. Vivinet Diagnostics cannot locate the file if you save it with any other name or in any other directory.

4.4.3 Limitations

So as to better evaluate the results of a Path Trace involving Layer 2 devices, review the following limitations.

- A Layer 2 trace is performed only on the first and last Layer 3 links in a path. The direction of the trace is represented by the direction of the link arrows in the Path Trace of the Diagnose view.
- Vivinet Diagnostics provides limited support for devices on the same subnet, a situation in which calls do not go through a router. When targets are on the same subnet, Vivinet Diagnostics does not run a traceroute. It relies entirely on third-party activity, such as a recent phone call, to populate the Port Forwarding Database.
- Vivinet Diagnostics provides only basic gap-handling support: the trace stops after encountering the first gap in the path and all switches after the gap remain unordered. For more information, see Section 5.1.7, "Unordered Devices," on page 82.

4.5 Working with Intercluster Trunks

An *intercluster trunk* allows two or more Cisco CallManager clusters to route calls among one another over an IP network. Vivinet Diagnostics fully supports route patterns along intercluster trunks for CallManager 4.x and 5.x deployments, but provides only limited support for intercluster trunks in CallManager 3.x deployments.

Vivinet Diagnostics queries a CallManager for its route patterns in order to determine the address of the CallManager with which a phone is registered. A route pattern may be configured to route certain calls to another CallManager cluster via an intercluster trunk, a function supported in CallManager 4.x and 5.x deployments. Vivinet Diagnostics can follow this extended route pattern.

In CallManager 3.x deployments, however, Vivinet Diagnostics can determine the CallManager address *only* if the gateway or trunk device is configured in the following manner:

When you configure the gateway device (for CallManager 3.1 or 3.2) or the trunk device (for CallManager 3.3), ensure the **Device Name** field contains the hostname or IP address of the CallManager. In 3.1 or 3.2 deployments, the **Device Name** field is likely to contain the hostname or IP address, anyway. In 3.3 deployments, this occurrence is less likely because the hostname or IP address is already specified in the **Remote Cisco CallManager Information** fields.

If the **Device Name** field does not contain a hostname or IP address, Vivinet Diagnostics may not be able to determine a phone’s CallManager and will report errors such as the following:

```
"CHR0142: The hostname specified could not be found by the name server."
"CHR0154: Sockets failure. errno is 11001 on call gethostbyname."
```

5 Understanding Results

Results of a Diagnosis are shown on both the Diagnose and Report views and include the following components:

- **Path Trace** — a graphical illustration of the path VoIP (RTP) data takes between the Target Devices on your network. Shown on the Diagnose view. For more information, see Section 5.1, “Reviewing Path Trace Components,” on page 71.
- **Severity icons** — clickable icons along the Path Trace if any network issues are found during a Diagnosis. For more information, see Section 5.1.9, “Severity,” on page 86.
- **Results table** — contains results from VoIP call performance testing performed as part of the Diagnosis. Shown on the Results view. For more information, see Section 5.2.1, “Interpreting the Results Table,” on page 88.
- **Diagnosis table** — displays any VoIP performance problems or network issues uncovered during the Diagnosis. Shown on the Results view. For more information, see Section 5.2.2, “Interpreting the Diagnosis Table,” on page 90.
- **Unordered Devices table** — appears in the Diagnose view only when the position of Layer 2 devices cannot be determined. For more information, see Section 5.1.7, “Unordered Devices,” on page 82.

5.1 Reviewing Path Trace Components

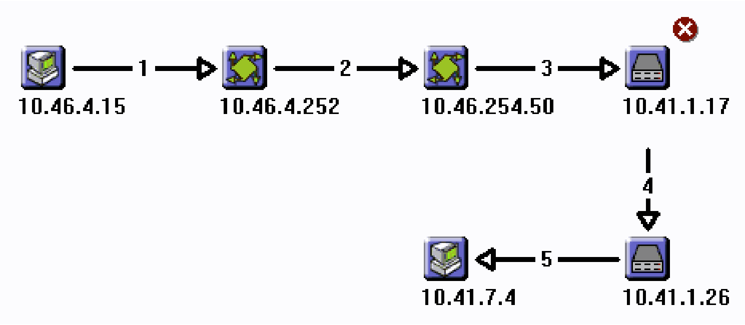
As soon as you initiate a Diagnosis, Vivinet Diagnostics attempts to determine which devices and links lie between the Target Devices you selected. If your Target Devices are endpoints, or if endpoints are installed in the same subnet as the phones you selected, Vivinet Diagnostics sends simulated VoIP RTP traffic between the devices. The traffic acts as a traceroute test to find routers or voice gateways in the path between the Target Devices. Using CDP, SONMP, or LLDP, the traffic finds any switches in the path. For more information, see Section 1.1, “How Vivinet Diagnostics Works,” on page 9.

Vivinet Diagnostics relies on a series of Cisco Ping and IOS IP SLA tests, or the Nortel R-value trap and `RTPStatShow` command, to find devices in the path when no endpoints are installed.

NOTE: An RTP traceroute is available only when the detected endpoints are at least version 4.5. If the endpoints are earlier than version 4.5, the traceroute defaults to the ICMP protocol.

As results about network devices and links become available, Vivinet Diagnostics builds them into the graphical Path Trace, a picture of your network that distinguishes between switches and routers, and begins and ends with your Target Devices. Click any router or switch to find out more information about it, such as its manufacturer or operating system. Select **Outgoing** or **Incoming** above the Path Trace to change the direction of the path as it is shown.

The Path Trace numbers each link in the path between the Target Devices. This number becomes the “position” of the link, used as an identifier in the Diagnosis table and in the Report. Use the Path Trace to keep track of each link’s position so you can better understand the Diagnosis and determine the location of any issues it uncovered.



If network issues are found, the Path Trace displays an icon indicating their severity. Three levels of severity are indicated, depending on the degree to which a performance metric exceeds one of the thresholds you configured or one of the Vivinet Diagnostics thresholds. You can, for example, set a threshold to determine how much data loss triggers a severity of “Warning.” Similarly, Vivinet Diagnostics’ internal logic determines when the number of network links the simulated VoIP traffic had to traverse is excessive and presents a Diagnosis of “Too many links.” Click a severity icon for more information about the flagged issue. For more information, see Section 5.1.9, “Severity,” on page 86.

From any device, link, or severity properties dialog box, press `[F1]` to view definitions of the data shown and get help with diagnostic information.

NOTE: If you run a Diagnosis between endpoints connected only by switches, in other words, there are no routers in the path, your Diagnosis produces a Path Trace showing the source and destination endpoints with no devices between them. Vivinet Diagnostics still generates metric data, but does not generate a warning or error about an empty path.

5.1.1 Endpoint Properties

Vivinet Diagnostics displays the following properties for endpoints in the graphical Path Trace in the Diagnose view. Where applicable, the property’s abbreviation, which also appears in the Raw Data file, is indicated in parentheses.

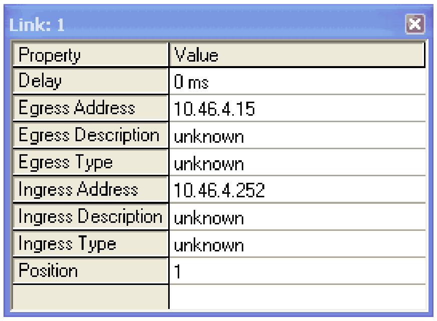
Click the **Endpoint** icon to display the Properties dialog box.

Endpoint Property	Description
Name	Domain name assigned to the endpoint computer
Physical Address (physaddr)	Endpoint computer’s MAC address, the physical-layer (OSI Layer 1) address of its NIC card
IP Address (ipaddr)	Endpoint computer’s IP network address
Endpoint Version	Should be 4.5 or later to support Vivinet Diagnostics functionality
Operating System	The operating system of the endpoint computer.

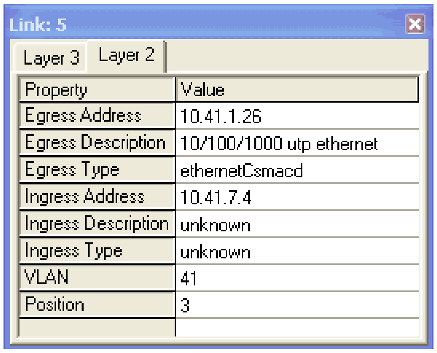
5.1.2 Link Properties

Vivinet Diagnostics displays the following properties for links in the graphical Path Trace in the Diagnose view. Some properties are switch-specific, others are router-specific.

Click the link between two devices to display the Properties dialog box. When Layer 2 devices are present, the dialog box displays two tabs of information.

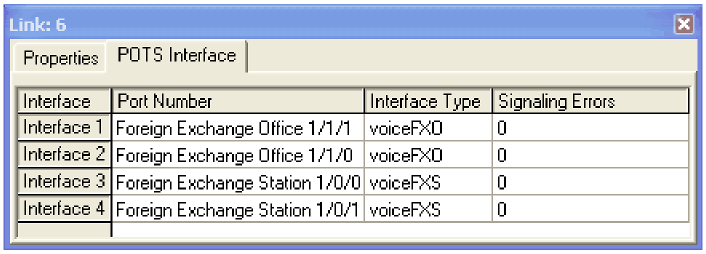


Property	Value
Delay	0 ms
Egress Address	10.46.4.15
Egress Description	unknown
Egress Type	unknown
Ingress Address	10.46.4.252
Ingress Description	unknown
Ingress Type	unknown
Position	1



Property	Value
Egress Address	10.41.1.26
Egress Description	10/100/1000 utp ethernet
Egress Type	ethernetCsmacd
Ingress Address	10.41.7.4
Ingress Description	unknown
Ingress Type	unknown
VLAN	41
Position	3

When a link connects a gateway with a POTS (plain old telephone service) phone, the dialog box presents two different tabs: **Properties** and **POTS Interface**.



Interface	Port Number	Interface Type	Signaling Errors
Interface 1	Foreign Exchange Office 1/1/1	voiceFXO	0
Interface 2	Foreign Exchange Office 1/1/0	voiceFXO	0
Interface 3	Foreign Exchange Station 1/0/0	voiceFXS	0
Interface 4	Foreign Exchange Station 1/0/1	voiceFXS	0

The following definitions indicate the property's abbreviation, which also appears in the Raw Data file. Not all properties appear on each tab. Therefore, the following table lists the properties in alphabetical order to simplify your search for a definition.

Link Property	Description
Bearer Channel	Type of bearer channel associated with the POTS interface: slot, port, or channel. Bearer channels are the channels in a T1 or E1 circuit that carry phone calls.
Link State	Status of the link associated with the POTS interface, such as inactive or active.
Delay	One-way delay measured for VoIP traffic — actual or simulated — on this link. Shown in milliseconds (ms).
Egress Address (egress)	IP address of the device through which traffic entered the link (that is, the transmission interface from which traffic exited the device at the beginning of the link). Should match a router or switch in the Path Trace. "Unknown" indicates SNMP access to the egress device was denied.
Egress Description (ename)	Default interface name assigned to a device at the time of installation.
Egress Type	Media type through which traffic entered the link (for example, Ethernet). "Unknown" indicates SNMP access to the egress device was denied.

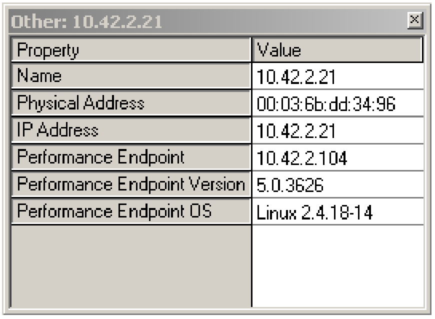
Link Property	Description
Egress VLAN	Virtual LAN number, if any, from which traffic entered this link and exited the previous device. It is possible for this number to differ from the Ingress VLAN number. Hybrid switches and routing switches can accommodate a change of VLAN in a Layer 2 trace.
Ingress Address (ingress)	IP address of the device through which traffic exited this link (that is, the transmission interface going into the device at the end of the link). Should match a router or switch in the Path Trace.
Ingress Description (iname)	Default interface name assigned to a device at the time of installation.
Ingress Type	Media type through which traffic exited this link (for example, Ethernet). "Unknown" indicates SNMP access to the ingress device was denied.
Ingress VLAN	Virtual LAN number, if any, from which traffic exited this link and entered the next device. It is possible for this number to differ from the Ingress VLAN number. Hybrid switches and routing switches can accommodate a change of VLAN in a Layer 2 trace.
Interface	Position of a POTS interface along the link between the gateway and the POTS phone. It is a number iteratively assigned to an interface as a result of the way traceroute tests were run between the devices. Functions as an identifier for diagnostic purposes.
Interface Type	Type of physical media associated with the POTS interface, such as ISDN, T1, E1, FXO, or FXS.
Port Number	Slot and port number of the POTS interface.
Position	Position of a hop in the path between the Target Devices. It is a number iteratively assigned to a link as a result of the way traceroute tests were run between the devices. Functions as an identifier for diagnostic purposes. The position number for each link also appears in the Diagnosis table in the Report view. Position numbers in the graphical Path Trace may not match the numbers shown in the informational dialog box because position numbers identify either Layer 2 or Layer 3 links. The links shown in the Path Trace do not distinguish between layers. Instead, they show a path between the Target Devices through every intervening device, regardless of the layer at which the device functions.
Signaling	Identifies the type of signaling channel used by the POTS interface: ◆ t1CcsBearerChan: A T1 common channel signaling bearer channel ◆ e1CcsBearerChan: An E1 common channel signaling bearer channel ◆ t1CasChan: A T1 channel associated signaling channel ◆ e1CasChan: AN E1 channel associated signaling channel
Signaling Errors	Number of signaling errors for the POTS interface.
Unordered Devices	Comma-separated list of all unordered devices associated with a Layer 2 device. An unordered device is one for which Vivinet Diagnostics cannot determine its exact position in the path. Layer 2 links that do not support CDP or SONMP or do not have either enabled are not detectable by Vivinet Diagnostics. You must enable your Layer 2 devices. For more information, see Section 4.4.2, "Device Configuration," on page 68.

5.1.3 Other Properties

When Vivinet Diagnostics cannot identify a device, the “other” icon appears in the graphical Path Trace in the Diagnose view. If Vivinet Diagnostics is unable to determine whether the destination address is a phone, for instance a VGMC or a voice application such as Call Pilot, the destination address is labeled as “other.” Ensure you have completely configured your Call and Signaling Servers. The configuration information will help Vivinet Diagnostics identify the devices in your network. For more information, see Section 3.5.6, “Configuring Nortel CS1000 Call and Signaling Servers,” on page 40.

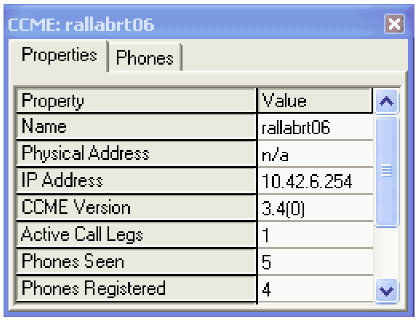
The “other” category also provides details for Cisco CallManager Express devices. In this case, the Properties dialog box is titled “CCME” and contains two tabs of information: **Properties** and **Phones**. The definitions below indicate whether they apply to CallManager Express.

☎ Click the **Other** icon to display the Properties dialog box.



Other: 10.42.2.21

Property	Value
Name	10.42.2.21
Physical Address	00:03:6b:dd:34:96
IP Address	10.42.2.21
Performance Endpoint	10.42.2.104
Performance Endpoint Version	5.0.3626
Performance Endpoint OS	Linux 2.4.18-14



CCME: rallabrt06

Property	Value
Name	rallabrt06
Physical Address	n/a
IP Address	10.42.6.254
CCME Version	3.4(0)
Active Call Legs	1
Phones Seen	5
Phones Registered	4

Other Properties Tab

Properties Tab Property	Description
Name	Domain name assigned to the device
Physical Address	Device’s MAC address, the physical-layer (OSI Layer 1) address of its NIC card
IP Address	Device’s IP network address
CCME Version	Version of CallManager Express on the device
Active Call Legs	Number of active CallManager Express call legs at the time of the Diagnosis. This number matches the number of “offhook” designations on the **Phones** tab.
Phones Seen	Number of phones identified by the CallManager Express device, regardless of the phones’ registration status
Phones Registered	Number of phones registered to the CallManager Express device
Performance Endpoint	IP address of the Performance Endpoint installed closest to the phone and was therefore used to run VoIP performance tests to aid in diagnosing the problem.
Performance Endpoint Version	Should be 4.5 or later to support Vivinet Diagnostics functionality
Performance Endpoint OS	Operating system of the computer on which the endpoint is installed

Other Phones Tab

Phones Tab Property	Description
Extensions/DNs	Phone number for all phones associated with a CallManager Express device, which is identified in the **Device Type** field.
Activity	Indicates whether a CallManager Express phone is active (offhook) or inactive (onhook). The number of offhook phones matches the number of Active Call Legs on the Properties tab.
Active DN	Phone number active for a particular CallManager Express device. A device can have more than one phone number.
User Name	Name of the user on the active phone number.
Registration	Indicates whether the phone number is registered to the CallManager Express device. The number of registered phone numbers matches the number in the Phones Registered field on the Properties tab.
Device Name	Name of the CallManager Express device.
IP Address	IP address of the CallManager Express device.
Device type	Type of CallManager Express device.
Key Phone?	Indicates whether the CallManager Express phone number has been designated as a key phone.

5.1.4 Phone Properties

Vivinet Diagnostics displays the following properties for phones in the graphical Path Trace in the Diagnose view.

☎ Click the **Phone** icon to display the Properties dialog box.

- See "Phone Properties Tab" on page 77 for definitions of the fields on the Properties tab.
- See "Phone Call Details Tab" on page 78 for definitions of the fields on the Call Details tab, which appears only for Cisco phones.
- See "Phone Quality Stats Tab" on page 79 for definitions of the fields on the Quality Stats tab, which appears only for Nortel phones.

These tabs may also contain fields for properties associated with POTS phone calls. You can find definitions of those fields in "Active and Recent Call Legs Tabs" on page 83 and in "Voice Gateway Performance Stats Section" on page 85.

Phone Properties Tab

The following are definitions for each row of the Properties tab. Many fields are not populated for a PSTN (public switched telephone network) phone. The properties displayed vary according to the vendor of the phone you selected. If the phone did not respond to queries, the Properties dialog box displays no value for any property.

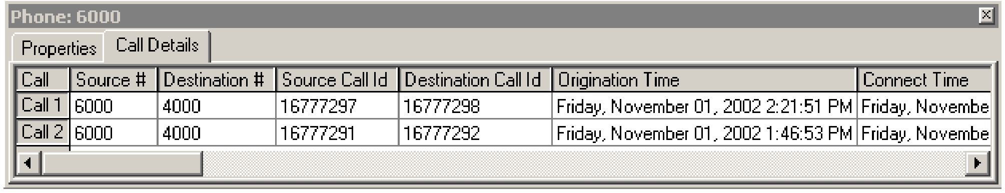
The names of properties differ for Cisco phones and Nortel phones. The following table describes them all.

Properties Tab Property	Description
Name	DNS hostname you entered on the Define view.
Internal Host Name	Unique identifier assigned by Cisco.
Call Server	Nortel Call Server that handled the most recent call from this phone.
Signaling Server	Nortel Signaling Server that handled the most recent call from this phone.
CallManager	Cisco CallManager server that handled the most recent call from this phone.
Publisher	Cisco CallManager server the phone normally uses to make calls.
SNMP Index	Phone’s SNMP index in its CallManager.
IP Address	Network IP address of the phone.
Subnet Mask	IP network subnet to which the phone belongs.
Terminal Number	Terminal number assigned to the Nortel phone.
Codec	Voice codec the phone used to make calls.
DNS Server	Phone’s Domain Naming System server, which registers its location and allows it to find other servers and hosts on the network.
HW Revision	Hardware version.
Extension	Telephone extension assigned to this phone. For Nortel phones, the extension number is the same as the DN (directory number).
Type	Identification string assigned to the phone by its manufacturer.
TFTP Server	Phone’s Trivial File Transfer Protocol server. On a Cisco VoIP network, the TFTP server provides the phone with critical information on configuration updates and allows it to register itself on the network.
Serial Number	Phone’s serial number.
Vendor	Phone’s manufacturer.
Version	Phone’s firmware version.
User	Current user assigned to this phone.
Status	Phone’s current up or down status.
Up Time	Number of hours:minutes:seconds that have elapsed since the Nortel phone was last rebooted.
Time of Last Registration	Last time the phone registered with its CallManager. Because this information is not available for CallManager version 3.x, this field always indicates “n/a” for CallManager 3.x environments.

Properties Tab Property	Description
Time of Last Error	Time of the last error the phone reported. Because this information is not available for CallManager version 3.x, this field always indicates “n/a” for CallManager 3.x environments.
Last Error	Error code of the last error the phone reported. Because this information is not available for CallManager version 3.x, this field always indicates “n/a” for CallManager 3.x environments.
Voice Gateway	Voice gateway this phone uses to make PSTN calls. Applies only to PSTN phones.
Gateway Router	Default gateway router configured for this phone.
Performance Endpoint	IP address of the Performance Endpoint installed closest to the phone and therefore used to run VoIP performance tests to aid in diagnosing the problem.
Performance Endpoint Version	Version of the endpoint software.
Performance Endpoint OS	Operating system of the computer where the endpoint is installed.
VRRP Master	The management address of the current VRRP Master router for the virtual address of a gateway router (if the gateway router is a VRRP virtual address).

Phone Call Details Tab

The following are definitions of each column shown in the Call Details tab, which appears only for Cisco devices. Each type of information is taken from CallManager Call Detail Records (CDRs).



Call	Source #	Destination #	Source Call Id	Destination Call Id	Origination Time	Connect Time
Call 1	6000	4000	16777297	16777298	Friday, November 01, 2002 2:21:51 PM	Friday, Novembe
Call 2	6000	4000	16777291	16777292	Friday, November 01, 2002 1:46:53 PM	Friday, Novembe

Call Details Tab Property	Description
Source #	Phone number or extension that initiated the call.
Destination #	Phone number or extension that received the call.
Source Call Id	Identifier of the call traffic stream going from source to destination.
Destination Call Id	Identifier of the call traffic stream going from destination to source.
Origination Time	Time of day the call was attempted.
Connect Time	Time of day the call was actually connected.
Disconnect Time	Time of day the call was disconnected.
Source Codec	Codec used by the phone that initiated the call.
Destination Codec	Codec used by the phone that received the call.

Call Details Tab Property	Description
Termination Code	CallManager-specific code that shows how the call was terminated. For more information, see Appendix A, "Cisco Unified CallManager Termination Codes," on page 137.
Sent Packets	Number of RTP packets sent between the phones during the call.
Sent Octets	Number of bytes sent between the phones during the call.
Lost Packets	Number of packets sent by one phone (during the call) never received by its partner phone.
Avg Jitter	Average jitter measured during the call.
Avg Latency	Average packet latency (delay) measured during the call.

Phone Quality Stats Tab

The following are definitions of each row shown in the Quality Stats tab, which appears only for Nortel devices. Each type of information is taken from RTCP-XR and RTCP statistics returned by the latest sampling of `RTPStatShow`.

Call details vary depending on which version of the Nortel CS1000 firmware you are running. Unless otherwise noted, the following details are available for all supported versions.

Quality Stats Tab Property	Description
Local Codec	Codec in use at the source of the call. This field appears only when a Nortel Diagnosis has been triggered by an event in NetIQ AppManager. For more information, see Chapter 8, "Working with NetIQ AppManager," on page 129.
Local Listening R-value	Call quality R-value for the source of the call as provided by RTCP-XR. RTCP does not provide an R-value. For more information, see Section 5.3.9, "R-value," on page 104.
Local Avg Net Loss Rate	RTCP-XR statistic used to compute a lost data value for the source phone. This detail became available in version 4.5.
Local Avg Discard Rate	RTCP-XR statistic used to compute a jitter buffer loss value for the source phone. This detail became available in version 4.5.
Local Avg Burst Density	RTCP-XR statistic used to compute burst density for the source phone. This detail became available in version 4.5. For more information, see Section 5.3.1, "Burst Density," on page 100.
Local Avg Burst Length	Average length of a burst density period on the source phone. This detail became available in version 4.5.
Local Gap Density	Percentage of packet loss during a gap period, the period of time between bursts, for the source phone. This detail became available in version 4.5.
Local Gap Length	Length of a gap period for the source phone. This detail became available in version 4.5.
Local Avg End System Delay	Average system delay for the source phone. System delay is the sum of jitter buffer and codec encoding and decoding. This detail became available in version 4.5.

Quality Stats Tab Property	Description
Local Avg Noise Level	Average level of interference present at the source phone. The lower the value, the less background noise present. This detail became available in version 4.5.
Local Avg Signal Power	Average signal strength for all received packets at the source phone. The higher the value, the stronger the signal. This detail became available in version 4.5.
Local Round Trip Time Avg	Average length of time for a call to travel to the destination phone and back. This detail became available in version 4.5.
Time Stamp	Date and time of day `RTPStatShow` was used to collect call quality statistics. `RTPStatShow` provides the most recent set of quality statistics for a phone. Therefore, statistics could be for a phone call that just recently occurred, or for a call that happened days ago.
Far End IP Address	IP address of the destination device.
Far End Port	Port number of the destination device.
Local Packets Sent	Number of RTP packets sent by the source phone.
Local Packets Received	Number of RTP packets received by the source phone.
Local Packets Received Out of Order	Number of incorrectly sequenced RTP packets received by the source phone.
Local Packet Loss	Number of packets sent by the source phone never received by its partner phone. This statistic is provided by the RTCP-XR Avg Net Loss Rate value or the RTCP Packet Loss value.
Local Avg Jitter	Average jitter for the source phone.
Local Latency	Packet latency (delay) for the source phone. This statistic is provided by the RTCP-XR End System Delay value or the RTCP Latency value.
Local Round Trip Time High	Longest length of time for a call to travel to the destination phone and back. This detail became available in version 4.5.

5.1.5 Router Properties

Vivinet Diagnostics displays the following properties for routers in the graphical Path Trace in the Diagnose view. If applicable, the property's abbreviation, which also appears in the Raw Data file, is indicated in parentheses.

Click the **Router** icon to display the Properties dialog box.

If the detected router did not respond to traceroute queries, the device icon on the Path Trace looks like a cloud, and the Properties box reads, "Device did not respond to traceroute queries." The message "Device did not respond to SNMP queries" indicates Vivinet Diagnostics was unable to get information from the device using SNMP queries.

Router Property	Description
System Name (sysname)	Internal administrative name (not the DNS hostname) for this device

Router Property	Description
Layer	Layer of the OSI model at which the router operates. Should be Layer 3 for routers.
Contact	Optional field in the device properties indicating the person or department to contact if the router needs servicing.
Model	Vendor and model number of the router
OS Version (osversion)	Version of the router operating system. Also indicates service packs, if any have been applied.
Services	List of the services supported by this device. Examples include Cisco Responder and VoiceGateway.
Up Time	Amount of time elapsed since the router was last rebooted
Vendor	Manufacturer of the router
Location	Internally configured. The place where the router is installed.

5.1.6 Switch Properties

Vivinet Diagnostics displays the following properties for switches in the graphical Path Trace in the Diagnose view. If the switch detected in the path did not respond to SNMP queries, the Properties box reads "Device did not respond to SNMP queries."

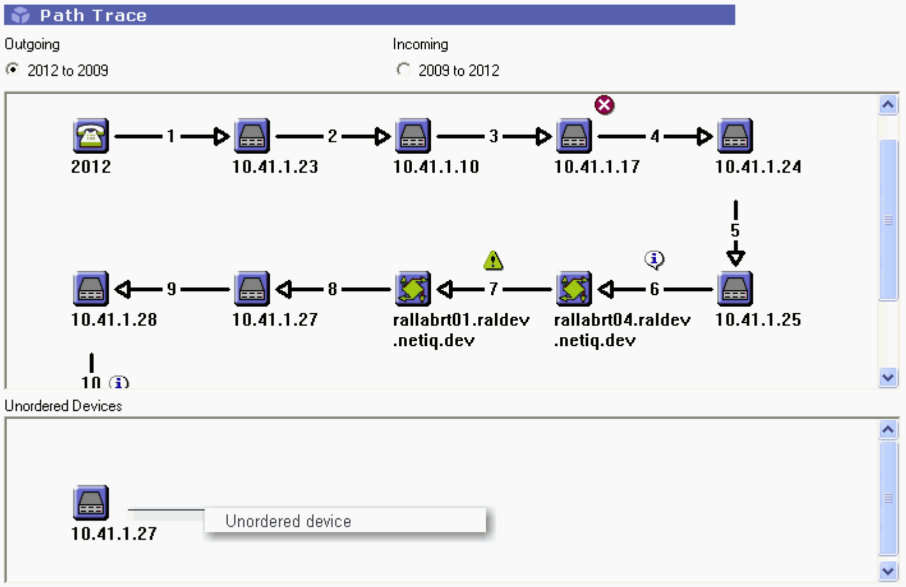
Click the **Switch** icon to display the Properties dialog box.

Switch Property	Description
System Name	Internal administrative name (not the DNS hostname) for this device
Layer	Layer of the OSI model at which the switch operates. Should be Layer 2 for switches.
Contact	Optional field in the device properties indicating the person or department to contact if the switch needs servicing.
Model	Vendor and model number of the switch
OS Version	Version of the switch operating system. Also indicates service packs, if any have been applied
Up Time	Amount of time elapsed since the switch was last rebooted
Vendor	Manufacturer of the switch
Location	Internally configured. The place where the router is installed
The following properties appear in the Switch properties dialog box when the switch is *unordered*. For more information, see Section 5.1.7, "Unordered Devices," on page 82.	
Egress Description	Default interface name assigned to a device at the time of installation
Egress Type	Media type through which traffic entered the switch, for example, Ethernet. "Unknown" indicates SNMP access to the device containing the egress was denied.
Ingress Description	Default interface name assigned to a device at the time of installation

Switch Property	Description
Ingress Type	Media type through which traffic exited the switch, for example, Ethernet. "Unknown" indicates SNMP access to the device containing the egress was denied.
L3 Link Position	Position of a Layer 3 hop in the path between the Target Devices associated with this switch. It is a number iteratively assigned to a link as a result of the way traceroute tests were run between the devices. Functions as an identifier for diagnostic purposes. The position number for each link also appears in the Diagnosis table in the Report view. Position numbers in the graphical Path Trace may not match the numbers shown in the informational dialog box because position numbers identify either Layer 2 or Layer 3 links. The links shown in the Path Trace do not distinguish between layers. Instead, they show a path between the Target Devices through every intervening device, regardless of the layer at which the device functions.

5.1.7 Unordered Devices

Vivinet Diagnostics may not be able to identify the location of some devices in the path. For instance, if you have not configured some Layer 2 devices, Vivinet Diagnostics cannot precisely pinpoint their location. Icons representing the unordered devices appear in a panel below the Path Trace.


Path Trace

Outgoing ● 2012 to 2009

Incoming ○ 2009 to 2012

Unordered Devices

Whether a device is ordered or unordered is irrelevant to the results of the Diagnosis. The Unordered Devices panel merely helps you visualize the Layer 2 path taken by voice packets.

Click each device in the panel to reveal the properties, which vary depending on the type of device.

NOTE: A device can appear twice in the Unordered Devices panel. Duplication can occur when the device is in the Layer 2 path on the left and right sides of the trace. In other words, the device exists between the source target and the source target's router as well as between the destination target and the destination target's router.

For more information, see Section 4.4, "Understanding Layer 2 Trace," on page 65.

5.1.8 Voice Gateway Properties

Vivinet Diagnostics displays the following properties for voice gateways in the graphical Path Trace in the Diagnose view. If applicable, the property's abbreviation, which also appears in the Raw Data file, is indicated in parentheses.

☎ Click the **Voice Gateway** icon to display the Properties dialog box.

A voice gateway provides so much information about the gateway and its call legs and dial peers that the Voice Gateway Properties dialog box is divided into tabs and sections, making the information easier to find.

Voice Gateway Properties Tab

The Properties tab presents basic information relating to the voice gateway itself.

Properties Tab Property	Description
System Name (sysname)	Internal administrative name (not the DNS hostname) for the voice gateway
Layer	Layer of the OSI model at which the voice gateway operates
Contact	Optional field in the device properties indicating the person or department to contact if the voice gateway needs servicing
Model	Vendor and model number of the voice gateway
OS Version (osversion)	Version of the voice gateway's operating system. Also indicates service packs, if any have been applied.
Services	List of the services supported by the voice gateway. Examples include Cisco Responder and VoiceGateway.
Up Time	Amount of time elapsed since the voice gateway was last rebooted
Vendor	Manufacturer of the voice gateway
Location	Internally configured. The place where the voice gateway is installed.

Active and Recent Call Legs Tabs

The Active Call Legs and Recent Call Legs tabs contain all or some of the following properties. The data in the Active Call Legs tab relates to legs of calls active on the voice gateway at the time of the Diagnosis. The data in the Recent Call Legs tab relates to legs of calls that occurred during the last 15 minutes (approximately). Not all fields in the tabs apply to both VoIP and POTS call legs. Fields display "n/a" if they do not apply to the call leg in question.

These tabs highlight all active and recent calls on the voice gateway, regardless of the PSTN phone number.

Call Legs Tabs Property	Description
Leg	Unique numeric identifier for the call leg
Type	Indicates whether the call leg belongs to a VoIP or POTS segment
Call ID	Unique alphanumeric identifier for the call

Call Legs Tabs Property	Description
Dial Peer ID	Numeric identification assigned to a dial peer in a voice gateway IOS configuration.
Peer Number	Called phone number **Important** The peer numbers you see may not be the same numbers you input for the Diagnosis. POTS phones, especially those with MGCP-configured gateways, may have dial peers whose pattern-matching fields are blank. Any phone number will match a blank pattern. In this scenario, all active or recent calls appear on the Call Legs tabs.
Interface Name	Name of the physical media interface mapped to the dial peer
Interface Type	Type of physical media interface mapped to the dial peer, such as FXO or FXS
Call Origin	Indicates whether the call leg originated or answered a call
Duration	For active calls, indicates the number of seconds the call has been active. For recent calls, indicates the total duration.
Call Status	Indicates whether the call is active or in the process of connecting
Disconnect Cause	Text string identifying why the call disconnected, usually “normal call clearing.” The actual value depends on the protocol and protocol version in use on the interface.
Remote IP Address	IP address of the VoIP dial peer, usually a CallManager
Remote UDP Port	UDP port number of the VoIP dial peer, usually a CallManager
Session Protocol	Name of the session protocol in use for the call leg, such as Other, Cisco, SDP, SIP, or Multicast
Selected QoS	QoS selected for the call leg. Can be bestEffort, guaranteedDelay, or controlledLoad.

POTS and VoIP Dial Peer Tabs

A dial peer is a device that originates or receives a call in a telephone network. Dial peers are categorized as either voice-network dial peers or POTS dial peers. Voice-network dial peers include VoIP-capable computers, routers, and gateways within a network. POTS dial peers include traditional telephone network devices such as phone sets, cell phones, and fax machines.

There is one dial peer per call leg. The Dial Peer tabs highlight all peers defined in the voice gateway relevant to the direction of voice calls.

Dial Peer Tabs Property	Description
Peer ID	Numeric identification assigned to a dial peer in a voice gateway IOS configuration.
Dial Pattern	String of characters, similar to a regular expression, used to match phone numbers with dial peers. A blank string matches any number and is normally associated with an MGCP gateway.
Peer Media	Identifies the type of physical network interface to which the logical interface is mapped. Can be VoIP, FXO, FXS, ISDN, T1, or E1.

Dial Peer Tabs Property	Description
Peer Status	Status of the dial peer at the time of the Diagnosis, such as active, not in service, or not ready.
Session Target	Destination of the dial peer, such as the IP address of the CallManager.
Prefix Digits	Digits to be sent to the telephony interface before the real phone number, such as country code 011.
Forward Digits	Number of digits from the dialed phone number that should be sent on to the destination phone number.
Session Protocol	Name of the session protocol in use for the dial peer, such as Other, Cisco, SDP, SIP, or Multicast.
Desired QoS	Requested QoS for the dial peer. Can be bestEffort, guaranteedDelay, or controlledLoad.
Encapsulation Name	Name of the voice encapsulation interface mapped to the dial peer. Voice encapsulation is the logical network interface created for each dial peer by the voice gateway, in essence, a mapping of the dial peer to its physical interface.
Encapsulation Type	Type of voice encapsulation interface mapped to the dial peer. Could be Voice or VoIP.
Interface Name	Name of the physical media interface mapped to the dial peer.
Interface Type	Type of physical media interface mapped to the dial peer, such as FXO or FXS.

Voice Gateway Performance Stats Section

In addition to the data displayed on the Active Call Legs and Recent Call Legs tabs, Vivinet Diagnostics provides performance statistics for the legs of active and recent calls. Click **View Performance Stats** to expand the Voice Gateway Properties dialog box and review the additional statistics.

For each *active* call statistic, the Average, Minimum, Maximum, and Standard Deviation value is shown, as well as the time the minimum value occurred and the time the maximum value occurred. The values for the **Time of Min** and **Time of Max** fields represent the number of milliseconds that elapsed between the start of polling and the time the minimum or maximum value occurred.

For each *recent* call statistic, only the final Average value is shown. There are no final values for ERL, Signal In, and Signal Out. Recent calls do not record values for those statistics.

Performance Statistic	Description
ACOM	Short for ACombined, the ACOM value is equal to ERL + ERLE (Echo Return Loss Enhancement) for the indicated call leg. ERLE is the amount of echo provided by an echo canceller. Measured in decibels.
ERL	For each call leg, Echo Return Loss is the ratio of the power level of the transmitted voice signal to the power level of the echo signal generated by the VoIP gateway. ERL varies greatly depending on the switched telephone network connected to the VoIP gateway. There will always be echo whenever you have an analog trunk line connected to a digital network.
Signal In	Active input signal level from the telephony interface used by the call leg. Measured in decibels relative to one milliwatt.

Performance Statistic	Description
Signal Out	Active output signal level from the telephony interface used by the call leg.
Round Trip Delay	End-to-end delay, or latency, as measured on the call leg, in milliseconds. For more information, see Section 5.3.3, “Delay,” on page 100.
Jitter Buffer Loss	Percentage of datagrams that overran or underran the jitter buffer during the call leg. For more information, see Section 5.3.5, “Jitter Buffer Loss,” on page 102.
Lost Data	Percentage of datagrams lost during the call leg. For more information, see Section 5.3.6, “Lost Data,” on page 102.
MOS	Mean Opinion Score (MOS) calculated for the call leg. For more information, see Section 5.3.7, “Mean Opinion Score,” on page 103.

5.1.9 Severity

The presence of a severity icon on the Path Trace in the Diagnose view indicates that Vivinet Diagnostics found issues that might affect the performance of VoIP calls on your network. The severity of an issue is determined by the threshold levels configured in the Thresholds dialog box, or by one of the Vivinet Diagnostics internal thresholds, which are derived from its rules about high-quality VoIP performance.

Severity levels are mapped to the thresholds you set for “Marginal” or “Good” performance. For example, if a performance metric recorded by a diagnostic test exceeds your Marginal threshold for Jitter Buffer Loss, the Path Trace shows the Error severity icon next to the device or link where the metric was recorded. If the metric meets or falls below your Marginal threshold while exceeding your Good threshold, the Path Trace shows the Warning icon. For more information, see Section 3.5.5, “Setting Thresholds,” on page 37.

Severity may be one of three levels:

Severity Icon	Meaning
⊗	Error. Highest severity. Requires immediate attention. Click the icon to review details about the issue, such as `Congestion: detected on an interface. 10.42.1.47, Ethernet0, reported an average of 1.334% packet collisions.`
⚠	Warning. Medium severity. Will probably adversely affect VoIP call quality. Click the icon to review details about the issue, such as `Congestion: detected on an interface. 10.42.1.249, FastEthernet1/0, reported a multiple collision ration of 64.904%.`
ℹ	Information. Lowest severity. Does not require immediate attention. Click the icon to review details about the issue, such as `Configuration: problem detected on an interface. 10.42.1.249, FastEthernet1/0, does not have RTCP enabled.`

5.2 Understanding the Report View

The Report view tab provides the results of a completed Diagnosis.

The **Results** table appears first, providing a summary of the values Vivinet Diagnostics calculated by measuring simulated VoIP traffic sent over the network between the Target Devices. The Mean Opinion Score (MOS) and R-value Vivinet Diagnostics calculated are shown first to summarize the performance of the simulated traffic. Next, any delay, jitter buffer loss, or lost data values used to calculate the MOS are shown. For more information, see Section 5.2.1, "Interpreting the Results Table," on page 88.

The **Diagnosis** table summarizes the findings. In a Nortel environment, the table also includes an identification of the Probable Cause of a Diagnosis. Icons indicate the severity of any issues uncovered on the network between the Target Devices. Issues are aspects of the Diagnosis that differ from the performance results found in the Results table. An issue might be, for example, a router whose utilization statistics exceed an appropriate threshold, or a congested WAN link. Such findings are provided to help you troubleshoot the problem. For more information, see Section 5.2.2, "Interpreting the Diagnosis Table," on page 90.

NOTE: Vivinet Diagnostics generates diagnoses for all problems that match the instructions in its rules file: diagnostics.bin. If you do not want Vivinet Diagnostics to generate all possible diagnoses, you can alter the rules file to disable the unwanted diagnoses. For more information, see Section 6.4, "Disabling Selected Diagnoses," on page 110.

In addition to viewing results in the Report and Diagnosis tables, you can also generate the results in two different formats: the Report and the Raw Data file. Two buttons are displayed at the bottom of the Report view:

- **Report** — provides a summary of the Diagnosis, showing how you defined the problem and naming the components or conditions that most directly contributed to the problem on your network. The Report is available in HTML format so you can view, print, and save it from your Web browser. For more information, see Section 3.8.1, "Diagnosis HTML Report," on page 48.
- **Raw Data File** — provides the data Vivinet Diagnostics collected and used to make the Diagnosis. The Raw Data file is available in a comma-separated values (CSV) format so you can import it into a spreadsheet program, such as Microsoft Excel. For more information, see Section 3.8.2, "Raw Data File," on page 49.

5.2.1 Interpreting the Results Table

The Results table shows results from VoIP performance tests. These tests are more likely to succeed and to collect results for every VoIP performance measurement type if your problem definition included endpoints, or if you installed endpoints on the same subnet as the phones used as Target Devices. Even if they are not used as Target Devices, endpoints can conduct accurate VoIP performance tests while the Diagnosis is running.

Depending on your phone vendor, either the Results Performance tab or the Results Quality Stats tab is displayed.

Results Performance Tab

The first column of the Performance tab contains performance icons indicating whether call quality metrics met or fell below the performance thresholds configured for the Diagnosis. For more information, see Section 3.5.5, "Setting Thresholds," on page 37.

Without endpoints, Vivinet Diagnostics attempts to get performance measurements using Cisco IOS IP SLA, a Cisco active call query (an SNMP query of router tables), or Nortel `RTPStatShow`. But if Vivinet Diagnostics cannot obtain results for a particular performance metric, the Performance tab shows "n/a" to indicate the statistic was not available. For more information, see Section 5.3, "Reviewing Factors in VoIP Performance Diagnoses," on page 100.

Consider the following when you scan the Performance tab:

- A result of "n/a" (not available) in the Measured Value column could indicate several scenarios in which a VoIP test was not attempted. The most common scenarios are described below:
  - You used phones instead of endpoints as Target Devices. Or you did not install endpoints in the same subnet as the phones. Endpoints can gather every metric needed to calculate the results shown here. Vivinet Diagnostics cannot collect them all without endpoints.
  - No router, or only one router, was found between the Target Devices. This scenario is applicable only when Vivinet Diagnostics was attempting a Cisco IOS IP SLA test between routers. A minimum of two routers is required for Cisco IOS IP SLA testing.
  - Vivinet Diagnostics could run the necessary VoIP performance tests only in a single direction between the Target Devices. Tests must be run in both directions to get aggregate measurements.
  - No SNMP community string with read/write access was provided. This scenario is applicable only when Vivinet Diagnostics was attempting a Cisco IOS IP SLA test between routers.
  - The Diagnosis ended before the VoIP test was attempted.
- For most diagnoses between Cisco devices or NetIQ Performance Endpoints, the values shown in the Performance tab represent aggregated measurements from performance tests run in two directions to mimic bi-directional VoIP call traffic. But when Cisco active calls are discovered in a VoIP-to-POTS phone Diagnosis, values for active calls reflect one-way measurements only. Delay, jitter buffer loss, and lost data are one-way metrics based on the delay metrics, and early, late, lost, and received packets (on their way to the POTS phone) detected by the voice gateway.
- For diagnoses between Nortel devices, the values shown in the Performance tab are gathered in one of two ways:
  - **Diagnosis triggered by AppManager Knowledge Script**. The AppManager NortelCS_Alarms Knowledge Script can launch the Action_DiagnoseNortelIPT script when one of the following SNMP trap is raised after a voice quality metric exceeds a designated threshold: QOS0022, QOS0024, QOS0026, QOS0028, QOS0030, QOS0032, and QOS0034. For more information, see Chapter 8, "Working with NetIQ AppManager," on page 129.

    Vivinet Diagnostics uses the voice quality metrics from the trap to create the Diagnosis statistics in the Performance and Quality Stats tabs on the Results table. However, it uses the metrics from `RTPStatShow` to populate the Quality Stats tab in the Phone details pop-up dialog box in the Path Trace of the Diagnose view.

    - **Diagnosis triggered by Define view configuration**. Vivinet Diagnostics collects voice quality metrics from `RTPStatShow` for both devices you configure in the Define view. It then determines which device has the worst voice quality. These "worst" values are used to create the Diagnosis statistics in the Performance and Quality Stats tabs on the Report table. The metrics from `RTPStatShow` also populate the Quality Stats tab in the Phone details pop-up dialog box in the Path Trace of the Diagnose view.

- The performance metric that exceeded the threshold by the highest percentage is probably the cause of the problem. If a probable cause has been determined, it will appear in the Diagnosis table. However, always read the rest of the results from the Diagnosis. They may provide clues as to why that particular metric was so poor.
- A **MOS** or call quality measured value of only 4.0 indicates tolerable, but not excellent, call quality. A MOS below 3.6 indicates conversation quality would be considered poor for many listeners. For more information, see Section 5.3.7, "Mean Opinion Score," on page 103.
- With enough **delay**, a conversation can sound like a walkie-talkie, discouraging the speakers from talking out of fear of speaking simultaneously. For more information, see Section 5.3.3, "Delay," on page 100.
- As a rule of thumb (or in this case, roughly an industry standard), **jitter buffer loss** values for a VoIP telephone call should remain below 0.5% of all datagrams sent if call quality is to remain high. For more information, see Section 4.2.5, "Defining Jitter Buffer," on page 61.
- It is generally agreed that a **lost data** value greater than 1% usually indicates poor call quality, although loss of 0.5% to 1% also indicates some deterioration in quality. High loss values are typically caused by network congestion. For more information, see Section 5.3.6, "Lost Data," on page 102.

For each metric discussed in the Performance tab, Vivinet Diagnostics assigns VoIP performance ratings based on the thresholds you configured for the Diagnosis. For example, if you set a Good threshold of 1% for Lost Data, and performance tests turned up a 1.5% data loss statistic, you would see a "Marginal" icon, a yellow triangle, next to "Lost Data" in the Performance tab. For more information, see Section 3.5.5, "Setting Thresholds," on page 37.

Performance ratings comprise three categories:

Category	Icon	Explanation
Good	🟢	VoIP performance statistics fell within acceptable parameters.
Marginal	⚠	Reconfiguration or upgrades are necessary to achieve voice compliance or good call quality.
Poor	🚫	Call-quality statistics were not within acceptable parameters.

Like the severity ratings in the Diagnosis table in the Report view, the performance ratings let you know at a glance if a problem exists on the network.

Results Quality Stats Tab

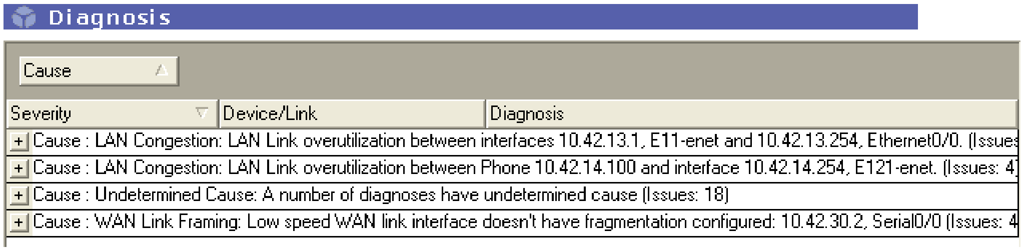
The Quality Stats tab appears only for diagnoses between Nortel devices. The contents of the tab varies depending on whether a trap event in AppManager triggered the Diagnosis or you defined the Diagnosis in the Define view. The following table defines all possible properties.

Quality Stats Tab Property	Description
Local Codec	Codec in use at the source of the call.
Local Avg Burst Density	Average amount of burst density (a variation of data loss) on the source phone. For more information, see Section 5.3.1, “Burst Density,” on page 100.
Local Avg Burst Length	Average length of a burst density period on the source phone.
Local Gap Density	Percentage of packet loss during a gap period, the period of time between bursts, for the source phone.
Local Gap Length	Length of a gap period for the source phone.
Local Avg Noise Level	Average level of interference present at the source phone. The lower the value, the less background noise present.
Local Avg Signal Power	Average signal strength for all received packets at the source phone. The higher the value, the stronger the signal.
Local Round Trip Time Avg	Average length of time for a call to travel to the destination phone and back.

5.2.2 Interpreting the Diagnosis Table

The following definitions help you analyze the contents of the Diagnosis table of the Report view: Probable Causes and Diagnoses. Where appropriate, information is included to help you begin troubleshooting the problem.

When Probable Causes are available, the Diagnosis table is sorted by cause.



Diagnosis

Cause

Severity | Device/Link | Diagnosis

+ Cause : LAN Congestion: LAN Link overutilization between interfaces 10.42.13.1, E11-enet and 10.42.13.254, Ethernet0/0. (Issues

+ Cause : LAN Congestion: LAN Link overutilization between Phone 10.42.14.100 and interface 10.42.14.254, E121-enet. (Issues: 4)

+ Cause : Undetermined Cause: A number of diagnoses have undetermined cause (Issues: 18)

+ Cause : WAN Link Framing: Low speed WAN link interface doesn't have fragmentation configured: 10.42.30.2, Serial0/0 (Issues: 4

You can change how the table is sorted by dragging a column heading up to the dark gray area of the table. Drag the column heading back to the table to return to the default sorting order. To change the order in which columns are displayed, drag a column to a new position in the table.

Probable Cause Definitions

The Diagnosis table may include the Probable Cause of an associated Diagnosis of Nortel devices. The cause indicates which network problem is the source of poor VoIP quality, as indicated by the Diagnosis, and tells you where to look to fix the problem.

The Probable Cause in a Nortel Diagnosis is provided by Proactive Voice Quality Management (PVQM), a solution Nortel co-developed with NetIQ that gives network managers the ability to ensure the overall quality of their IP Telephony deployments. PVQM continuously and passively measures the user Quality of Experience (QoE) for all IP telephony communications, conducts system health checks for IP telephony servers, and provides troubleshooting and resolution for any performance degradation or fault conditions.

Not every Diagnosis is associated with a Probable Cause, but every cause is associated with at least one Diagnosis. The following list describes every possible Probable Cause.

Probable Cause	Definition
Duplex configuration	The indicated link has a duplex configuration problem. At least one of the interfaces has been operating in half-duplex mode, which is inappropriate for VoIP traffic. Full-duplex mode, sending and receiving simultaneously, is recommended for VoIP traffic. Half-duplex mode has resulted in your Diagnosis of congestion, burst density, and/or data loss. A very common situation is one in which a VoIP phone is configured to auto-negotiate speed and duplex settings, while its corresponding switch port is configured as full duplex. In this scenario, the phone defaults to using half-duplex mode. Most vendors recommend configuring interfaces to auto-negotiate. If that is not possible, configure full-duplex mode for all of your interfaces.
WAN link without QoS	QoS is not provisioned properly. The indicated interface either had a QoS setting that assigns VoIP traffic a lower priority than recommended, or had no QoS setting at all. Review the individual diagnoses to determine which QoS settings are incorrect. The help for each Diagnosis contains additional information. Follow your network vendor’s recommendations for configuring VoIP QoS.
WAN link speed - framing	A low-speed (less than 1024kbps) WAN link interface is not configured to support fragmentation (framing) and interleaving (LFI). LFI reduces VoIP delay and jitter by breaking up large datagrams and interleaving VoIP datagrams with the resulting smaller datagrams. The lack of fragmentation and LFI has resulted in your diagnoses of jitter buffer loss and/or burst density. Configure your WAN links to use LFI and fragmentation. Refer to your network vendor’s documentation for instructions.
Frame relay multiplexing	Inappropriate frame relay traffic shaping is the cause of your jitter, lost data, and/or burst density diagnoses. Traffic shaping determines which packets are dropped due to congestion and which packets receive priority. Correctly configure the committed information rate on your frame relay devices. Refer to your network vendor’s documentation for instructions.

Probable Cause	Definition
WAN link congestion	The indicated interfaces have not been configured with sufficient bandwidth to ensure a quality VoIP transmission. Insufficient bandwidth has resulted in your diagnoses of lost data, jitter buffer loss, and/or burst density. Ensure you have properly configured QoS and LFI (fragmentation and interleaving) across the WAN. Review the bandwidth requirements for VoIP and other applications. If your WAN does not have sufficient bandwidth for your needs, try tuning the applications to reduce the needed bandwidth. For example, you can configure a different codec, albeit at the expense of voice quality.
LAN link congestion	Either link utilization is high or QoS has not been configured for the indicated interfaces. Link congestion has resulted in your diagnoses of lost data, jitter buffer loss, and/or burst density. Ensure you have properly configured QoS or duplex settings across your LAN links. Excessive broadcast traffic is another reason for congestion. Minimize the use of applications that use broadcast traffic. Ensure your LAN bandwidth can handle the amount of application traffic, VoIP or otherwise.
Undetermined cause	Vivinet Diagnostics has uncovered a Probable Cause of your VoIP problem that cannot be grouped with any of the other Probable Causes. Although its category is undetermined, the cause still merits investigation.

Diagnosis Definitions

Diagnoses describe the what, where, when, and severity of a condition in the network. In other words, a Diagnosis describes a symptom. The following list describes every possible Diagnosis.

Diagnosis	Definition
ACOM	Short for ACombined, the ACOM value (measured in decibels) is equal to ERL + ERLE (Echo Return Loss Enhancement) for the indicated call leg. ERLE is the amount of echo provided by an echo canceller. The Diagnosis detected either the average or standard deviation ACOM value failed to meet the threshold for an active or recent POTS call leg. For more information, see Section 3.5.5, “Setting Thresholds,” on page 37.
Asymmetric routing	When traceroute tests were run between the Target Devices, the identified paths for each direction were different. The paths differed because the path in one direction included more links, or because the path in each direction involved different device interfaces. The differences indicate an asymmetric network configuration. Asymmetric routing may point to a loop in your network and can degrade VoIP call quality because the conversation may take longer to travel from one conversant to the other, creating a “walkie-talkie” effect (delayed speech). If you run a Diagnosis using endpoints on multi-homed computers — computers that use multiple network adapters — you may see this Diagnosis. A multi-homed endpoint computer actually bridges network segments, so you will receive an “asymmetric routing” Diagnosis if the Path Trace in each direction produces a different, although valid, route. In such a case, the Diagnosis does not necessarily indicate a problem.

Diagnosis	**Definition**
Broadcast traffic	At least one interface along the path between the Target Devices has received a fairly large number of broadcast packets, as a percentage of all packets received recently. Broadcast packets, sent over an Ethernet segment by shared media, such as printers, to advertise services, are seen by all nodes on the LAN segment and can create congestion. Routers can be configured to drop them. Further segmenting the network using a router can help reduce broadcast traffic.
Burst density	A variation of data loss, burst density is the longest sequence of data, beginning and ending with a loss, during which the number of consecutive received packets is less than the threshold. Bursty packet loss has a severe impact on VoIP call quality. Even if the average packet loss rate for a call is low (say one percent), the lost packets are likely to occur during short dense periods, resulting in short periods of degraded quality. For more information, see Section 5.3.1, “Burst Density,” on page 100.
Call failure	A search of CallManager Call Detail Records found a phone call that failed between the Target Devices. For more information, see Appendix A, “Cisco Unified CallManager Termination Codes,” on page 137.

Diagnosis	Definition
Configuration	Vivinet Diagnostics detected a configuration problem with a VoIP device. For example, a router may not be configured to handle the QoS settings you selected in the Define view. A configuration problem may be diagnosed due to a number of different issues. The salient one is indicated in the Diagnosis table. The following are definitions of these issues. ◆ **Cisco IOS IP SLA disabled**—The IOS IP SLA helps diagnose a VoIP problem by running jitter and delay tests on Cisco routers. The necessary tests could not be run because the IOS IP SLA on a router between the Target Devices had been disabled. For more information, see Section 1.2, “Cisco IOS IP Service Level Agreement,” on page 10. ◆ **Half-duplex network traffic was detected**—The indicated interface has been operating in half-duplex mode, which is inappropriate for VoIP traffic. Full-duplex mode (sending and receiving simultaneously) is recommended for VoIP traffic. ◆ **Insufficient bandwidth detected**—The indicated interface was configured with insufficient bandwidth to ensure quality VoIP transmissions. ◆ **Insufficient Quality of Service detected**—The indicated ATM interface had a QoS setting that assigns VoIP traffic a lower priority than recommended. The recommended QoS setting for VoIP traffic on an ATM interface is Class B VBR or better. ◆ **Interface does not have any traffic classes defined with priority queuing enabled**—The defined traffic classes for the indicated interface do not have priority queuing enabled. For details about enabling priority queuing, see the QoS configuration documentation for the interface. For more information, see Section 4.3.4, “Reviewing Class-Based QoS,” on page 64. ◆ **Interface does not have RTP Priority or LLQ configured**—The indicated interface is not giving voice traffic expedited handling. RTP priority works when routers identify voice traffic by its RTP port numbers and place it in a priority queue, giving it preferential treatment over all other traffic. Low Latency Queuing (LLQ) reduces latency for voice traffic by classifying it and allowing packets in the voice class to be sent before packets in other queues are sent. ◆ **Interface does not have strict priority queuing configured**—The indicated interface is not giving voice traffic expedited handling. Strict priority queuing works when routers and switches place VoIP packets in a priority queue, giving them preferential treatment over all other packets. This Diagnosis is applicable only for diagnoses involving Nortel phones and devices. ◆ **Interface does not have WAN link fragmentation and interleaving configured**—The indicated interface does not have WAN link fragmentation and interleaving (LFI) configured. LFI reduces VoIP delay and jitter by breaking up large datagrams and interleaving VoIP datagrams with the resulting smaller datagrams. Vivinet Diagnostics flags this issue only if the WAN link in question is slower than or equal to 768 kbps (for Cisco devices) and 1024 kbps (for Nortel devices). ◆ **One link interface is running in full-duplex mode and the other in half-duplex mode**—The indicated interfaces are configured differently. One of them has been operating in half-duplex mode, which is inappropriate for VoIP traffic. Full-duplex mode (sending and receiving simultaneously) is recommended for VoIP traffic. A mismatch between the two interfaces in the link can lead to data loss. ◆ **Only one link interface has header compression configured**—The indicated link has a header compression mismatch. An interface on one side of the link is performing RTP header compression (cRTP), while the interface on the other side is not. Thus cRTP is not improving VoIP performance. This Diagnosis is applicable only for diagnoses involving Cisco phones and devices.

Diagnosis	Definition
Congestion	May be diagnosed due to a number of different issues. The salient one is indicated in the Diagnosis table and defined below. Occasionally a Diagnosis of “Congestion” might be based on inaccurate information. You may have incorrectly configured an interface’s bandwidth by using the Cisco IOS “bandwidth” command. If the bandwidth value in the device MIB is lower than the device’s actual bandwidth, Vivinet Diagnostics might conclude that the interface is congested, even if it is not. To avoid this problem, keep the “bandwidth” value up to date. Following are definitions of the issues that may have led to a congestion Diagnosis. The term “device” here is interchangeable with “interface.” ◆ **Device reported N% utilization**—Refers to bandwidth utilization levels that approach link capacity, which can add to delay. In most instances, this Diagnosis carries a severity of Major/Minor. However, if traffic class priority queuing is enabled for the affected interface, this Diagnosis is downgraded to an Informational severity level. When priority queuing is enabled, Vivinet Diagnostics can detect more specific voice-related conditions, making this Diagnosis less urgent. For more information, see Section 4.3.4, “Reviewing Class-Based QoS,” on page 64 and Section 5.3.8, “Network Congestion,” on page 103. ◆ **Device reported traffic queued for transmission**—The queue length on a router or switch is a good indicator of congestion. Buffer queues swell when too many packets enter a device, which cannot forward them all immediately and must instead cache some. Queues that exceed a certain length can lead to delay or jitter. In most instances, this Diagnosis carries a severity of Major/Minor. However, if traffic class priority queuing is enabled for the affected interface, this Diagnosis is downgraded to an Informational severity level. When priority queuing is enabled, Vivinet Diagnostics can detect more specific voice-related conditions, making this Diagnosis less urgent. For more information, see Section 4.3.4, “Reviewing Class-Based QoS,” on page 64. ◆ **Device reported discarding packets for unknown protocols**—Frequently discarding packets whose protocols are unknown is an indication that a network device or service is filling the pipes with unnecessary packets. This type of congestion may indicate a configuration issue. ◆ **Device reported** *N* **packet collisions**—Packet collisions can occur whenever a shared medium, such as an Ethernet cable, is oversubscribed or congested. In general, shared media need to be segmented by routers so VoIP traffic can yield high call quality. And collisions are an indication that a device on the Ethernet is only operating in half-duplex mode. Collisions should be less than 1% on an Ethernet segment. Ethernet collisions are a common cause of delay and jitter. ◆ **Device reported a multiple collision ratio of** *N*—The collision ratio refers to the rate at which packets experienced multiple collisions — collided more than once before they could be sent successfully — as compared to the total number of collisions detected. Multiple collisions occurring at this rate suggest this link is congested. The collision ratio on an Ethernet segment should be less than 60%. ◆ **Device reported** *N* **multiple collisions**—During polling intervals, the maximum number of packets that experienced multiple successive collisions before they could be successfully transmitted exceeded a threshold. Ethernet collisions, which indicate congestion, are a common cause of individual packet delay and jitter. ◆ **Device reported** *N* **deferred packets**—Deferred packets have been buffered. They could not be sent when the initial request was made because a collision occurred (due to network congestion). Packet deferrals can exacerbate jitter and data loss

Diagnosis	Definition
Congestion	- **Device reported pre-policy utilization of *N*%**—Pre-policy utilization refers to the utilization of a traffic class's allocated bandwidth before the execution of QoS policies. As capacity is consumed (in other words, as utilization approaches the threshold), congestion may occur and the device may not be able to guarantee delivery bandwidth for the traffic class. An average utilization above the threshold indicates a sustained problem. A maximum utilization above the threshold may indicate a temporary spike in usage. - **Device reported post-policy utilization of *N*%**—Post-policy utilization refers to the utilization of a traffic class's allocated bandwidth after the execution of QoS policies. As capacity is consumed (in other words, as utilization approaches the threshold), congestion may occur and the device may not be able to guarantee delivery bandwidth for the traffic class. An average utilization above the threshold indicates a sustained problem. A maximum utilization above the threshold may indicate a temporary spike in usage. - **Device reported queue depth of *N* packets**—The queue length on a router or switch is a good indicator of congestion. Buffer queues swell when too many packets enter a device, which cannot forward them all immediately and must instead cache some. Queues that exceed a certain length can lead to delay or jitter. - **Device reported *N*% channel utilization**—Channel utilization refers to the percentage of bearer channels in use for a T1 or E1 circuit. As channel utilization approaches the threshold you set, congestion may occur. For more information, see Section 3.5.5, "Setting Thresholds," on page 37.
CPU utilization	Vivinet Diagnostics calculates CPU utilization from one-second, five-second, and one- and five-minute samples and then reports a maximum percentage (to show spikes in utilization), an average (to give a sense of normal utilization), or a standard deviation (to give a sense of the frequency of spikes in utilization). For more information, see Section 5.3.2, "CPU Utilization," on page 100.
Delay	One of the greatest impairments of call performance, delay can be measured on a link or device on the network between the Target Devices. For more information, see Section 5.3.3, "Delay," on page 100 and Section 1.1, "How Vivinet Diagnostics Works," on page 9.
Device did not respond	The operation failed when Vivinet Diagnostics attempted to gather data from a network device, a phone, a CallManager, a Signaling Server, or a Call Server. Often this Diagnosis indicates you need to do some extra configuration. For more information, see Section 3.5.1, "Configuring SNMP Permissions," on page 32. If any error message was provided as part of the Diagnosis, click **View Error Log** in the Diagnose view to find out what happened.
Down recently	The number of seconds of uptime reported by the indicated device or interface indicates it has been down within the past hour. The device or interface that was recently down may have caused the VoIP problem you are diagnosing.
ERL	Echo Return Loss is the ratio of the power level of the transmitted voice signal to the power level of the echo signal generated by the VoIP gateway. The Diagnosis detected either the average or standard deviation ERL value failed to meet the threshold for an active or recent POTS call leg. For more information, see Section 3.5.5, "Setting Thresholds," on page 37.
High hop count	The Diagnosis detected a large number of router hops between the Target Devices. Network configuration may be an issue, or the routers that usually carry this traffic were down.

Diagnosis	Definition
Incomplete path	Vivinet Diagnostics was unable to determine the complete path between the devices you specified because the indicated device did not respond to traceroute queries.
Insufficient bandwidth	The bandwidth detected on the indicated device or link fell below the Marginal threshold for insufficient bandwidth. For more information, see Section 5.3.4, “Insufficient Bandwidth,” on page 101.
Jitter buffer loss	Jitter refers to excessive variation in delay values among datagrams in a single transmission. Jitter buffers smooth out these variations by holding some datagrams to feed them to the application sequentially. Datagrams not contained by the jitter buffer due to excessive delay variation would be lost to the application and are thus called jitter buffer lost datagrams. This statistic includes datagrams with delay too great for the jitter buffer you set (“overruns”) as well as those that arrive too quickly, while the jitter buffer is still full, and must be discarded (“underruns”). For more information, see Section 4.2.5, “Defining Jitter Buffer,” on page 61.

Diagnosis	Definition
Lost data	May be diagnosed due to a number of different issues, but the pertinent one is indicated in the Diagnosis table. For more information, see Section 5.3.6, “Lost Data,” on page 102. The following are definitions of these issues. The term “device” here is interchangeable with “link” or “interface.” ◆ **_N_% average packet loss measured on device**—Average data loss recorded during the polling period exceeded a threshold for Lost Data. In most instances, this Diagnosis carries a severity of Major/Minor. However, if traffic class priority queuing is enabled for the affected interface, this Diagnosis is downgraded to an Informational severity level. When priority queuing is enabled, Vivinet Diagnostics can detect more specific voice-related conditions, making this Diagnosis less urgent. For more information, see Section 4.3.4, “Reviewing Class-Based QoS,” on page 64. ◆ **_N_% maximum packet loss measured on device**—Maximum data loss during the polling period exceeded a threshold for Lost Data. The ◆ **Packet loss due to collisions detected**—Ethernet collisions have occurred along this segment recently. Collisions cause packet loss. ◆ **Test detected packet loss at a rate of _N_%**—Data loss greater than 0% was measured by the indicated test between the Target Devices. ◆ **N average Ethernet media errors detected**—Average number of media errors that have occurred since the device has been active. These errors did not necessarily occur during the run of the Diagnosis. Errors that occur at a switch or router interface cause packets to be discarded. ◆ **N maximum Ethernet media errors detected**—Highest number of media errors reported during a single device-polling interval on the indicated Ethernet segment. The maximum statistic indicates spikes in media errors. Errors that occur at a switch or router interface cause packets to be discarded. ◆ **N total Ethernet media errors detected**—Total number of media errors that have occurred since the device has been active. These errors did not necessarily occur during the run of the Diagnosis. Errors that occur at a switch or router interface cause packets to be discarded. ◆ **N discards detected at device**—The indicated device reports discarded packets. ◆ **Performance test detected loss**—A VoIP performance test starting from the Source Target detected lost packets at a rate that exceeded a Lost Data threshold. ◆ **Packet loss caused by drops due to policy, random detect, etc.**—The application of a policy to a traffic class caused the indicated device to drop packets. An average packet-loss measurement above the threshold indicates a sustained problem. A maximum measurement above the threshold may indicate a temporary spike. ◆ **Packet loss caused by drops due to lack of buffers**—A lack of SRAM buffers during output processing caused the indicated device to drop packets for this traffic class. An average packet-loss measurement above the threshold indicates a sustained problem. A maximum measurement above the threshold may indicate a temporary spike.
Memory utilization	If the memory utilization is maximized on a switch or router, calls may be processed more slowly, and network delay may increase. The affected memory pool is indicated. Memory utilization should remain below 90% for high-quality VoIP calls.

Diagnosis	Definition
MOS estimate	A MOS estimate (as converted from an R-value) failed to meet the MOS threshold. The estimate was either calculated during a VoIP test, a Cisco IOS IP SLA operation, or a Ping test, or it was reported by the Nortel R-value trap or RTCP-XR. For more information, see Section 5.3.7, “Mean Opinion Score,” on page 103 and Section 5.3.9, “R-value,” on page 104.
No bandwidth	Circuit throughput was insufficient to allow test VoIP traffic. For more information, see Section 5.3.4, “Insufficient Bandwidth,” on page 101.
No connectivity	Test traffic sent by Vivinet Diagnostics was unable to traverse the indicated network segment because the network was down. A router, switch, or target is probably offline or powered off.
No likely causes	No issues were detected. All metrics conformed to expectations for high-quality VoIP traffic.
Phone down	The “phone down” Diagnosis varies slightly depending on the phone vendor you selected: ◆ **The CallManager reports the phone is currently inactive**—Queries sent to the Target Device’s CallManager determined the phone is currently inactive. It may be unplugged, or it may have a network connectivity problem. ◆ **The Signaling Server reports the phone is not currently online**—The Signaling Server for the Nortel Target Device reports the phone is not currently online. It may be unplugged or have a network connectivity problem.
Recent error	Queries sent to the Target Device’s CallManager determined the phone has recently reported an error. For more information, see Appendix A, “Cisco Unified CallManager Termination Codes,” on page 137.
R-value	The R-value failed to meet the threshold you set. R-value is a call quality score derived from delays and equipment impairment. R-value is either reported by `RTPStatShow` or it is calculated during a VoIP test, a Cisco IOS IP SLA operation, or a Ping test. For more information, see Section 5.3.9, “R-value,” on page 104.
Signal errors	The voice gateway indicates signal errors occurred before or during a Diagnosis.
Signal level	Vivinet Diagnostics identifies the input and output signal levels from the telephony interface used by the active POTS call leg. Signal levels are measured in decibels relative to one milliwatt. The Diagnosis detected either the average or standard deviation values for input and output signal levels failed to meet the threshold for an active POTS call leg. For more information, see Section 3.5.5, “Setting Thresholds,” on page 37.
Too many links	Simulated VoIP traffic traversed an excessive number of network links, which could cause excessive delay.
Unstable routing	When traceroute tests were run multiple times in each direction between the Target Devices, the identified network paths changed. The disparities indicate an unstable or variable routing pattern, which is most likely to occur over a WAN link. Network congestion can cause unstable routing, which can result in the loss of router control packets. If routing patterns are unstable, related issues may be increased by delay and/or jitter. A Diagnosis of unstable routing may also be generated if your network is experiencing unusually high traffic, thereby causing traceroute requests to be discarded. This situation is probably a short-term problem with your network.

5.3 Reviewing Factors in VoIP Performance Diagnoses

To determine the relative quality of a simulated VoIP call made during a Diagnosis, Vivinet Diagnostics measures the call performance metrics described in the following topics.

5.3.1 Burst Density

A variation of data loss, burst density is the longest sequence of data, beginning and ending with a loss, during which the number of consecutive received packets is less than the threshold. Bursty packet loss has a severe impact on VoIP call quality. Even if the average packet loss rate for a call is low (say one percent), the lost packets are likely to occur during short dense periods, resulting in short periods of degraded quality.

To calculate burst density between Nortel Target Devices, Vivinet Diagnostics uses data from the Nortel R-value trap, which was raised because a voice quality threshold was crossed, or the RTCP-XR Average Burst Density value. RTCP does not provide a value for burst density.

The burst density threshold is static in Vivinet Diagnostics. You cannot change it.

5.3.2 CPU Utilization

Any applications installed on the same computer might at any point be required to compete with each other for processing time — for the use of the chip or central processing unit (CPU). Codecs require a fair amount of CPU processing time because of the compression they perform, so CPU utilization can become an issue on any softphones you are running. And if you add RTP header compression as part of a Quality of Service scheme on your network, VoIP will require even more CPU at the routers, which perform this compression. Finally, call performance will not be excellent if VoIP servers do not have enough extra CPU cycles to accommodate call processing as quickly and efficiently as possible. Competition for CPU time can add to delay.

Therefore, always keep track of CPU utilization statistics on routers and on critical VoIP servers. By default, Vivinet Diagnosis flags an issue on your network if router or switch CPU utilization exceeds 80%. Set a new threshold for CPU utilization by clicking **Thresholds** on the Options menu and then clicking the **Device/Link** tab.

5.3.3 Delay

End-to-end delay, or latency, as measured between the Target Devices is a key factor in diagnosing a problem with VoIP call quality. Using test traffic, Vivinet Diagnostics takes a delay measurement for datagrams traveling between the devices in a single direction. The delay measured includes the several factors:

Delay Type	How It Is Calculated
Network delay (one direction)	Datagram’s RTP timestamp subtracted from the time it was received by the target endpoint. Endpoints must synchronize their high-precision timers to calculate one-way delay. This delay factor actually includes the propagation delay (time spent on the actual network) and the transport delay (time spent getting through intermediate network devices).

Delay Type	How It Is Calculated
Packetization delay	Fixed value. Dependent on the selected codec. **NOTE**: If the RTP priority for some packets is set higher than the RTP priority for other packets, it is possible for packets from hops that are farther away to arrive earlier than packets from closer hops. To avoid delay caused by inconsistent prioritization, ensure RTP priority is set appropriately.
Jitter buffer delay	Fixed value of two datagrams for each codec. The amount of delay depends on the datagram size in milliseconds each codec uses. For example, for the G.711 codecs, which use a 20-ms datagram size, a two-datagram jitter buffer adds 40 ms of delay.

By default, Vivinet Diagnostics uses a threshold value of 350 ms to determine when delay on your network is considered an issue. Change the default threshold by clicking **Thresholds** on the Options menu. Most callers notice round-trip delays when they exceed 250 ms. ITU-T standard G.114 specifies 150 ms as the maximum one-way delay tolerable for high-quality VoIP, so consider these factors when configuring a delay threshold.

Delay is calculated between the Target Devices regardless of whether you selected a phone, an endpoint, or a generic device as the Device Type. Delay values have different sources depending on whether you are calculating delay between Cisco IP phones or Nortel devices.

- Vivinet Diagnostics uses Cisco IOS IP SLA to calculate delay between Cisco IP phones. But if you are using endpoints, the endpoints acting as Target Devices must continuously synchronize their high-precision clocks. Endpoints maintain virtual (software) clocks for each partner, and they compare their respective versions of the clocks before the start of each diagnostic test and periodically thereafter.
- To calculate delay between Nortel Target Devices, Vivinet Diagnostics uses the Nortel R-value trap, which was raised because a voice quality threshold was crossed, the RTCP-XR End System Delay value, or the RTCP Latency value.

5.3.4 Insufficient Bandwidth

The amount of WAN or LAN bandwidth your VoIP traffic needs depends on the type of codec you are using. The codecs with the highest theoretical maximum Mean Opinion Score (MOS) use the most bandwidth. For more information, see Section 4.2.2, “Reviewing Codecs,” on page 60.

Vivinet Diagnostics checks each WAN or LAN interface between the two Target Devices you included in the problem definition and reports an issue if bandwidth falls below the threshold.

You can change the default threshold of 35 by clicking **Thresholds** on the Options menu. Keep in mind, the G.726, G.729, and G.723 codecs require substantially less than 50 kbps of bandwidth. However, other network traffic on these links may take up a large amount of the available bandwidth, particularly during the busiest hours of the day. Vivinet Diagnostics also takes network congestion into consideration when diagnosing a problem. For more information, see Section 5.3.8, “Network Congestion,” on page 103.

5.3.5 Jitter Buffer Loss

As simulated calls run during a Diagnosis, the endpoints calculate jitter, a factor known to adversely affect call quality. Jitter, also called delay variation, indicates the differences in arrival times among all datagrams sent during a simulated VoIP call.

When a datagram is sent, the sender gives it a timestamp. When a datagram 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 video application, jitter manifests itself as a flickering image, while in a telephone call, its effect may be similar to the effect of packet loss: some words may be missing or garbled.

VoIP equipment typically has a jitter buffer that holds datagrams, buffering them until a segment of the voice transmission can be reassembled to reduce inter-arrival time variability. For more information, see Section 4.2.5, "Defining Jitter Buffer," on page 61.

If Vivinet Diagnostics detects jitter on the network, it measures jitter buffer loss — the percentage of datagrams that overran or underran the jitter buffer emulated by the call script used in a Diagnosis. Jitter buffer overruns or underruns are equivalent to lost data, which is a source of call-quality impairment. For more information, see Section 5.3.6, "Lost Data," on page 102. The jitter buffer loss statistic is shown in the Results table as part of the MOS calculation during a Diagnosis.

The measurement/gathering method varies slightly by phone vendor. In a **Cisco environment** this statistic is measured only if you are using endpoints for the Diagnosis. In a **Nortel environment**, this statistic, called "average discard rate," is gathered when an AppManager event triggers a Diagnosis.

To calculate jitter buffer loss between Nortel Target Devices, Vivinet Diagnostics uses the RTCP-XR Average Discard Rate value. RTCP does not provide a value for jitter buffer loss.

Vivinet Diagnostics uses a default threshold of 0.5000% to determine when jitter buffer datagram loss is considered an issue. You can determine what levels of jitter are acceptable on your network by configuring thresholds. For more information, see Section 3.5.5, "Setting Thresholds," on page 37.

5.3.6 Lost Data

In diagnosing a problem on your network, Vivinet Diagnostics weighs relevant statistics on lost datagrams, expressed as a percentage of all test data sent between the Target Devices. If the Target Devices are Performance Endpoints, these statistics are also used to calculate a MOS score for VoIP calls between these devices.

When a datagram 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 Diagnostics therefore includes packet loss in calculating a MOS for each simulated VoIP call.

To measure packet loss using endpoints as the Target Devices, one endpoint computer in each pair of devices keeps track of how many bytes of data it sent. The sending endpoint reports the number of sent bytes to the receiving endpoint, and the receiver compares that value to the actual number of bytes received to determine whether data was lost.

You can get packet loss values without using endpoints as the Target Devices. The measurement/gathering method varies slightly according to your phone vendor. In a **Cisco environment**, Vivinet Diagnostics uses Cisco IOS IP SLA tests to find out how much data was lost between Cisco routers. In a **Nortel environment**, Vivinet Diagnostics uses the "Avg. Network Loss Rate" value from the R-value trap. Or, if a trap did not trigger the Diagnosis, Vivinet Diagnostics can use the "Pkt Loss" value from `RTPStatShow`.

Vivinet Diagnostics flags data loss as an issue only if it exceeds the configured threshold for packet loss. By default, this threshold is .500%, reflecting general industry standards for VoIP. Set a new threshold by clicking **Thresholds** on the Options menu.

For more information, see Section 3.5.5, “Setting Thresholds,” on page 37.

5.3.7 Mean Opinion Score

As part of any Diagnosis involving Performance Endpoints, Vivinet Diagnostics sends simulated VoIP traffic between the Target Devices and measures its performance. Using the performance metrics collected from the test traffic, Vivinet Diagnostics then calculates an estimated Mean Opinion Score (MOS), which summarizes the quality of the test VoIP transmission.

NetIQ uses a modified version of the ITU G.107 standard E-Model equation to calculate a MOS estimate for a pair of endpoints. The E-Model, developed by the European Telecommunications Standards Institute, is an algorithm developed to evaluate the quality of a voice transmission by factoring in the “mouth-to-ear” characteristics of a speech path. These characteristics were in turn derived from studies of user satisfaction with varying levels of transmission clarity and stability.

The E-Model takes as input an R-value, which correlates directly with the MOS. The factors of network delay in a single direction, delay introduced by the codec’s packetization technique, lost data packets, and datagram loss due to jitter and jitter buffer size are measured between the endpoints and then used to calculate the R-value (and thus, the MOS).

A MOS of 5 is excellent. A MOS of 1 is unacceptably bad. The following table, taken from ITU G.107, summarizes the relation between the MOS and user satisfaction:

Mean Opinion Score	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 Diagnostics considers a MOS of less than 4.03 to be an issue. However, you can determine at what level a MOS is considered problematic in your diagnoses. Click **Thresholds** on the Options menu to change the MOS threshold.

5.3.8 Network Congestion

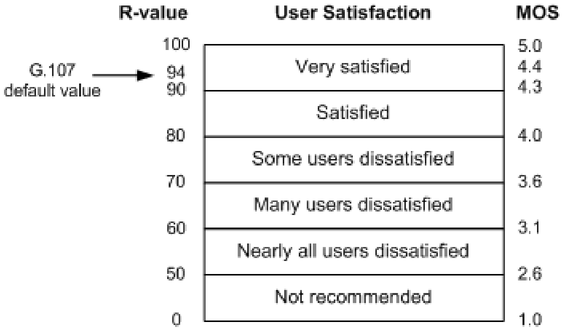
To find out how much of a particular network link’s capacity is being filled with network traffic, including VoIP and any other concurrently running applications, Vivinet Diagnostics uses SNMP to query router and switch network interfaces. Each interface supplies information about the number of bytes that have passed through it, as well as indicating its bandwidth.

Because VoIP traffic is extremely sensitive to delay, it is never a good idea for it to be traveling over WAN links that consistently experience more than 50% utilization. For LAN links, more than 25% utilization often inhibits VoIP call quality because most LANs are collision-prone, and collisions add plenty of delay while contributing to packet loss. For more information, see Section 5.3.6, “Lost Data,” on page 102.

When checking bandwidth on a link, Vivinet Diagnostics reports the maximum bandwidth utilization in one direction. If 80% of the link is used in one direction and 50% of the link is used in the other direction, the bandwidth utilization will be reported as 80%.

5.3.9 R-value

Defined by ITU (International Telecommunication Union) recommendation G.107, the E-Model is a complex calculation, the output of which is a single score called an R-value that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor). As shown below, an estimated MOS can be directly calculated from an R-value:



Cisco IOS IP SLA does not generate R-value metrics. When diagnosing call quality between Nortel Target Devices, Vivinet Diagnostics uses the data from one of two places: the Nortel R-value trap or the R-value metric provided by RTCP-XR. RTCP does not provide an R-value.

6 Troubleshooting

You can avoid most errors by correctly configuring such vital options as addressing and security information for Cisco CallManagers and Nortel phones and network devices. For more information, see Section 3.4, “Tips for a Successful Diagnosis,” on page 30.

The **View Error Log** button is enabled in the Diagnose view when an error occurs during a Diagnosis. Click the button to access the Error Log Viewer, which not only indicates why you received the message, but suggests how to correct the problem.

Click the **Details** button in the Error Log Viewer to see a detailed explanation of the highlighted message. Then click **Help for Message** to see whether any corrective actions are suggested.

Some errors, such as “action errors,” also cause an error message to appear. In addition, you probably will not see a Path Trace between the Target Devices if any errors occur.

6.1 Endpoint Errors

The most common errors occur when the endpoint is not installed or is installed improperly. If this is the case, you will see error **CHR0200**: “`The TCP connection attempt timed out`,” or **CHR0204**: “`No partner program is waiting to accept this TCP sockets connection`.”

If you see either of these errors, check the endpoint computers included in the Diagnosis and ensure the endpoint is installed and running. The endpoint documentation includes advice for ensuring the endpoint is running and for restarting it, if necessary. For more information, see Section 1.7, “NetIQ Performance Endpoints,” on page 13.

Equally, you may see **CHR0401**: “`Vivinet Diagnostics could not discover a Performance Endpoint near phone or voice gateway %1 with subnet mask %2`.” This error may occur when you run a Diagnosis using telephones as Target Devices. For such diagnoses, Vivinet Diagnostics still attempts to locate endpoints to run diagnostic testing. If you have not installed endpoints in the subnets where the IP phones are located, or in the same subnet as a POTS phone’s voice gateway, you will see this message. Just install an endpoint in the subnet indicated in the message and run the Diagnosis again.

Occasionally Vivinet Diagnostics detects an error in an endpoint computer’s high-precision timers and generates error **CHR0359**. If you see this error, run the Diagnosis again.

Other types of common errors invalidate or impede the Diagnosis unless you make configuration changes. For example, when one of the endpoints is powered off while the Diagnosis is running, your results will show **CHR0200**. Similarly, error **CHR0125** indicates an endpoint included in the Diagnosis is an older endpoint version and does not support the necessary diagnostic testing performed by Vivinet Diagnostics. Install the latest version of the endpoint on the affected computer. For more information, see Section 1.7, “NetIQ Performance Endpoints,” on page 13.

If you installed Performance Endpoints on computers running Microsoft Vista, you will get the following error when performing endpoint-to-endpoint diagnoses between those computers:

```
Layer 2 Trace could not be performed starting from a Phone or Endpoint because the
MAC Address is unknown. Check the Error Log for further details.
```

The built-in security in Microsoft Vista prevents Vivinet Diagnostics from completing a Diagnosis between endpoints. Performance Endpoints are not supported on Microsoft Vista.

In the unlikely event you are unable to synchronize the clocks on both endpoint computers, it is possible you will not get performance results for certain call quality metrics. However, Vivinet Diagnostics will not report an error if your clocks are not synchronized. You will notice only that expected results do not appear in the Results tab. If synchronization seems to be the problem, rerun the Diagnosis.

If you receive endpoint errors, save your Diagnosis configuration first, and then debug the endpoint problem.

For truly severe errors or exceptional circumstances, contact NetIQ Technical Support. For more information, see Section 6.5, "Getting Technical Support," on page 113.

6.2 Diagnostic Errors

Vivinet Diagnostics logs system errors to the `diagnostics.log` file. To read this log file, use the command-line program `fmtlog.exe`. For more information, see Section 2.4, "Reviewing Directories and File Types," on page 20 and Section 6.2.6, "Formatting Error Logs," on page 108.

Often, an error indicates the need for a configuration change, such as entering information about CallManagers or Signaling Servers at the Console or enabling a service on a router. If, for example, Vivinet Diagnostics cannot find the Target Devices, the Error Log Viewer or a Diagnosis Tips dialog box pops up instead of a Path Trace. For more information, see Section 3.4, "Tips for a Successful Diagnosis," on page 30.

6.2.1 SNMP Errors

Configure accurate SNMP community strings at the Console before you run a Diagnosis to avoid SNMP-related errors. The two most common errors are:

- **CHR0392**: "`An SNMP request sent to x.x.x.x timed out.`"
- **CHR0403**: "`The request for egress interface address from device x.x.x.x failed.`"

Even if SNMP communication is inhibited because of the lack of the proper community string, Vivinet Diagnostics can still find switches and routers and place their addresses or DNS hostnames on the Path Trace. You can then consult with a network administrator to find out why communications with them were not successful.

In some cases, communications over SNMP fail because a firewall is active on the network. For more information, see Section 4.1, "Running a Diagnosis Through a Firewall," on page 57 if you see the SNMP-related message **CHR0386**: "`An SNMP request to %2 failed.`"

6.2.2 CallManager Errors

During a Diagnosis using IP phones, you may see error **CHR0400**: "`Vivinet Diagnostics could not find a CallManager via DHCP.`" This message can indicate your Console computer is not configured to use DHCP, which is used to locate CallManagers. Or it can indicate the DHCP server could not be found. Regardless, configure CallManager DNS hostnames or IP addresses at the Vivinet Diagnostics Console. For more information, see Section 3.5.3, "Adding or Deleting a CallManager," on page 36.

Similarly, if you neglected to supply information about CallManager security, including the user ID/password combination that gives Vivinet Diagnostics access to CallManager information, or if you supplied this information incorrectly, you may see error **CHR0365**: "`An error was detected by OLE DB while accessing the SQL database for a Vivinet product`." The error occurred because the Console failed in an attempt to retrieve data from a CallManager SQL Server database. For more information, see Section 3.5.4, "Configuring CallManager User IDs and Passwords," on page 36.

6.2.3 Cisco IOS Errors

Cisco has confirmed a bug (ID number CSCsa92212) in almost all of the 12.3 IOS versions, which can adversely affect diagnoses. You may see the following symptoms in your diagnoses:

- Path trace is missing one or more hops.
- The following messages appear in the Error Log Viewer:

- **CHR0403**: "`The request for egress interface address from device <device IP address> failed`."
- **CHR0386**: "`An SNMP request to <device IP address> failed, returning (noSuchName). There is no such variable name in this MIB`."

To obtain a fix for the bug, contact Cisco and reference CSCsa92212.

Cisco also has confirmed a bug in IOS version 12.3(14)T1. If you are using this version of IOS, your diagnoses may generate error messages indicating Vivinet Diagnostics cannot retrieve configuration information from a device.

- **CHR0403**: "`The request for device configuration from device <device IP address> failed`."
- **CHR0386**: "`An SNMP request to <device IP address> failed, returning (badValue). The value given has the wrong type or length`."

Vivinet Diagnostics uses the device configuration to diagnose problems with QoS settings. Without the configuration information, you may not be notified about important QoS problems in your network.

To obtain a fix for the bug, contact Cisco and reference ID number CSCsa5373.

6.2.4 Router Memory

In addition to the router configuration outlined in Section 3.4, "Tips for a Successful Diagnosis," on page 30, you should ensure routers on the network have enough memory allocated for IOS IP SLA tests.

Vivinet Diagnostics gathers some diagnostic information from IOS IP SLA tests. Occasionally a router may not have enough memory available to run an IOS IP SLA test. The amount of memory available to IOS IP SLA (in this case, RTR) operations is a configurable value. About 25% of the router's total memory is the recommended amount. For more information, see Section 1.2, "Cisco IOS IP Service Level Agreement," on page 10.

To set or change the amount of memory available to IOS IP SLA RTR operations, issue the following commands:

- To show the largest process memory block available, issue `show memory summary`
- To show the current memory water mark setting, issue `show rtr application`
- To set the memory watermark from router configuration, issue `rtr low-memory` <*value*>

6.2.5 Packet Loss Errors

A Diagnosis may indicate packet loss you cannot confirm by an IOS `show` command. Specifically, an IOS `show` command produces no packet loss information, even though the Diagnosis does indicate packet loss.

Various diagnoses are based on the sum of various `dot3Stats` from a device's MIB (management information base):

- `dot3StatsAlignmentErrors`
- `dot3StatsFCSErrors`
- `dot3StatsSQETestErrors`
- `dot3StatsInternalMacTransmitErrors`
- `dot3StatsCarrierSenseErrors`
- `dot3StatsFrameTooLongs`
- `dot3StatsInternalMacReceiveErrors`

If these stats report non-zero values, Vivinet Diagnostics infers packet loss has occurred. In this instance, the Diagnosis is informational only, because the errors happened in the past and not necessarily during any VoIP traffic.

6.2.6 Formatting Error Logs

When Vivinet Diagnostics encounters a system problem, it logs the problem information to an error log file (`diagnostics.log`) on the Console computer. Similarly, when an endpoint program encounters a problem it cannot report to the Console, it logs that problem to an error log file on the endpoint computer: `endpoint.log`, in the endpoint's directory.

Use the Error Log Viewer to view the error log stored at the Console. To view any error log, use the command-line program named `fmtlog`, which is installed in the root directory where you installed Vivinet Diagnostics. For more information, see Section 6.3, "Error Log Viewer," on page 109.

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 `Program Files\NetIQ\Vivinet Diagnostics` and is also installed at the endpoints. See the *User Guide for Performance Endpoints,*

included in the Vivinet Diagnostics download package, for additional information on running `fmtlog` on the platform you are using.

6.3 Error Log Viewer

The Error Log Viewer helps you read and organize error information. To open the Error Log Viewer, click the **View Error Log** button.

The Error 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 a Diagnosis is not saved to disk as a separate file. Instead, it is stored in the Vivinet Diagnostics Knowledge Engine.

The Error Log Viewer is available only if errors occurred during the current diagnostic test. Errors that occurred during a previous diagnostic test are erased when a Diagnosis is run for a second time.

6.3.1 Reviewing an Error Log

Click the **View Error Log** button to review the entries shown in the Error Log Viewer. These entries can help you determine why errors occurred during a Diagnosis.

Click a column heading to sort the entries by that column. By default, entries are sorted by record number.

Error Log Component	Description
Record column	Shows the order in which errors were detected. Record numbers do not change when sorting or filtering is applied.
Date/Time columns	The date and time the error was detected.
Detected By column	The component that detected the error: either the Vivinet Diagnostics Console or the endpoints.
Action Name column	The Vivinet Diagnostics action that encountered the error.
Description column	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 Error 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 Error Log Viewer. For more information, see Section 6.3.3, “Filtering Log Entries,” on page 110.
Find button	Helps you find a specific string in the Log Details. Highlights the record containing the string. Double-click the highlighted record to view the details.
Refresh button	Refreshes the Log Viewer dialog box with any errors detected since you opened the dialog box.

6.3.2 Viewing Error Details

To get more information about an entry in the Error Log Viewer, highlight the entry and click **Details** on the Log Viewer dialog box.

The Log Details dialog box for the selected entry shows detailed information about the selected entry.

Log Details Component	Description
Help for Message button	Provides more information about the error, including the steps you can take to avoid it.
Close button	Closes the Log Details dialog box and returns to the Error Log Viewer.
Next button	Shows details about the next entry in the Error Log.
Previous button	Shows details about the previous entry in the Error Log.

6.3.3 Filtering Log Entries

Click **Filter** in the Log Viewer dialog box to determine which entries in the error log are shown in the Error 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. To allow the Error Log Viewer to show the first entry generated during the Diagnosis, select **First Record**. Select **Records On** to 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	To allow the Error Log Viewer to show only entries containing a specific error message, select **Message=CHR**. Then enter the message number. You can also filter the error log entries by the name of the Action that detected the error. Select **Action Name=** and then select the Action name from the list.

Record numbers remain unchanged after filters are applied to the Error Log Viewer. Their order indicates how the filter is being applied and which records have been filtered out.

6.4 Disabling Selected Diagnoses

Vivinet Diagnostics generates diagnoses for *all* problems that match the instructions in its rules file: `diagnostics.bin`. However, you can instruct the rules file to disable any unwanted diagnoses.

To disable selected diagnoses, edit the `CancelDiagnosesConfig.txt` file, which ships with Vivinet Diagnostics and is installed by default in `C:\Documents and Settings\All Users\Application Data\NetIQ\Vivinet Diagnostics`.

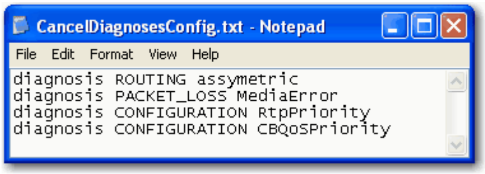
When editing `CancelDiagnosesConfig.txt`, use the following format:

- Limit your changes to one entry per line.
- Ensure the first word in the line is "diagnosis."

- Ensure the second word in the line is the keyword of the Diagnosis you want to disable.
- Use the third word in the line to disable a Diagnosis subtype. Omit the third word to disable *all* diagnoses identified by the second word.
- Ensure case-sensitivity for the first, second, and third words.

In the following example, four diagnoses have been disabled:

- Asymmetric routing
- Lost data: *n* total Ethernet media errors detected
- Configuration: Interface does not have RTP Priority configured
- Configuration: Interface does not have any traffic classes defined with priority queuing enabled


CancelDiagnosesConfig.txt - Notepad
File Edit Format View Help

```
diagnosis ROUTING assymetric
diagnosis PACKET_LOSS MediaError
diagnosis CONFIGURATION RtpPriority
diagnosis CONFIGURATION CBQoSPriority
```

The following table lists the keywords and subtypes for the diagnoses you can disable:

Keyword	Subtype
GWCALL_ACOM	ACOM
GWCALL_ERL	ERL
GWCALL_INSIGNAL	InSignal
GWCALL_OUTSIGNAL	OutSignal
BROADCAST	BroadcastRate
BURST_DENSITY	BurstDensity
COMPLETION	Assistant
COMPLETION	Diagnosis
COMPLETION	NortelDiagnosis
COMPLETION	Path
COMPLETION	Resolve
COMPLETION	Subnet
COMPLETION	VoIPPerf
COMPLETION	SameAsst
COMPLETION	NortelServer
COMPLETION	NortelFirmware
COMPLETION	MacUnknown
COMPLETION	NoL2Trace
CONFIGURATION	Bandwidth
CONFIGURATION	NoBandwidth

Keyword	Subtype
CONFIGURATION	DuplexMode
CONFIGURATION	HeaderCompress
CONFIGURATION	Mismatch
CONFIGURATION	Responder
CONFIGURATION	RtpPriority
CONFIGURATION	StrictPriority
CONFIGURATION	CBQoSPriority
CONFIGURATION	WanLfi
CONGESTION	Bandwidth
CONGESTION	CollRate
CONGESTION	CollRatio
CONGESTION	ECNS
CONGESTION	ECNSRate
CONGESTION	MultRate
CONGESTION	Position
CONGESTION	QLen
CONGESTION	Speed
CONGESTION	PreUtil
CONGESTION	PostUtil
CONGESTION	ChannelUtil
CPU_UTILIZATION	Cpu1min
CPU_UTILIZATION	Cpu5min
CPU_UTILIZATION	Cpu5sec
DELAY	Anomalous
DELAY	Delay
DELAY	Ping
DELAY	Reach
DOWN_RECENTLY	UpTime
JITTER	JitterBufferLoss
MEM_UTILIZATION	MemI/O
MEM_UTILIZATION	MemProcessor
MOS	Mos
NOT_ACCESSIBLE	CcmDbRead

Keyword	Subtype
NOT_ACCESSIBLE	CcmMibRead
NOT_ACCESSIBLE	HttpRead
NOT_ACCESSIBLE	SnmpRead
NOT_ACCESSIBLE	SnmpWrite
NOT_ACCESSIBLE	NortelRead
PACKET_LOSS	Discards
PACKET_LOSS	Errors
PACKET_LOSS	LostData
PACKET_LOSS	LossRate
PACKET_LOSS	MediaError
PACKET_LOSS	MediaRate
PACKET_LOSS	DroppedPacketsPct
PACKET_LOSS	NoBufPacketsPct
PHONE_STATUS	CallFail
PHONE_STATUS	LastErr
PHONE_STATUS	Status
PHONE_STATUS	SignalErrors
RVALUE	RValue
ROUTING	ASymmetric
ROUTING	Links
ROUTING	Incomplete
ROUTING	Unstable

6.5 Getting Technical Support

If you are unable to resolve your problem using the topics in the Troubleshooting chapter or the rest of the *User Guide*, contact NetIQ Technical Support.

Telephone	713-418-5555 In North, Central, and South America, and in the Caribbean
Support	www.netiq.com/support/vd Provides a complete list of support phone numbers, as well as access to the NetIQ Knowledge Base and Technical Support
Registration	www.netiq.com/register/nw

6.5.1 Problem Sleuth

In many cases, Technical Support personnel ask you to gather certain files from your computer to determine the sort of problem you are experiencing. Vivinet Diagnostics 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 Technical Support personnel, who can find a quick solution. For example, it collects configuration and trace files, log files, and the `assert.err` and `drwatson` files from the directories where they are written.

After it builds a list of files, it zips them within a directory created during product installation. You can then FTP the ZIP file to Technical Support.

To run GanyPS, type the following at a command prompt in the directory where you installed Vivinet Diagnostics:

```
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 FTP site. A Technical Support representative will supply a URL.

7 Working with the Sample Diagnoses

This chapter discusses the Sample Diagnoses that ship with Vivinet Diagnostics. A review of the Sample Diagnoses will acquaint you with the kind of data you can expect from your own Diagnosis.

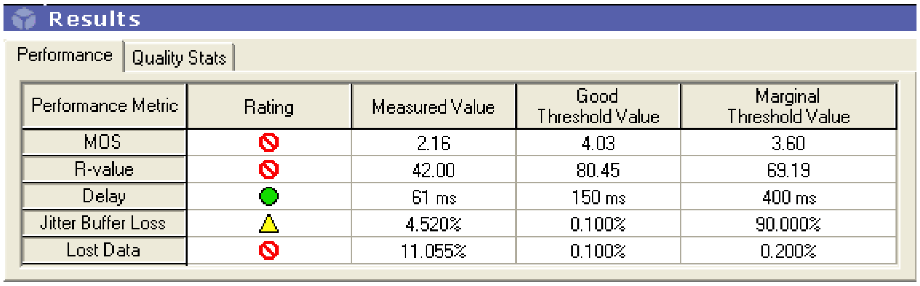
7.1 Sample Diagnosis Between Endpoints

This topic discusses one of the sample Diagnosis files that ship with Vivinet Diagnostics. The file `EndpointSample1.dgv` is stored in the `Program Files\NetIQ\Vivinet Diagnostics\Samples` folder. In the Vivinet Diagnostics Console, click **Open** on the File menu and browse to it. Then use the following topics to navigate the Console and understand the Diagnosis process.

7.1.1 Diagnosis

First, click the **Report** view tab. The Report view includes two tables that provide quick insight into the VoIP problem being diagnosed.

Take a look at the Results table:



Performance Metric	Rating	Measured Value	Good Threshold Value	Marginal Threshold Value
MOS	⊘	2.16	4.03	3.60
R-value	⊘	42.00	80.45	69.19
Delay	●	61 ms	150 ms	400 ms
Jitter Buffer Loss	⚠	4.520%	0.100%	90.000%
Lost Data	⊘	11.055%	0.100%	0.200%

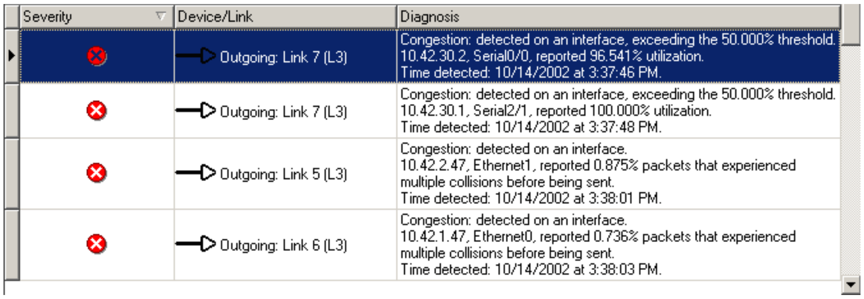
The values shown in this table were measured during VoIP performance tests that ran between the two endpoints as part of the Diagnosis. The first thing you notice is the terrible **MOS** (Mean Opinion Score): only **2.21**, a value far below the “Marginal” threshold of 3.60.

NOTE: The R-value calculation is based on the MOS score.

VoIP performance tests consist of simulated, bi-directional calls. An estimated MOS for the calls summarizes their quality based on listener satisfaction. According to the ITU standard for a MOS, a score of 2.21 for a call means nearly every listener would report unsatisfactory call quality. For more information, see Section 5.3.7, “Mean Opinion Score,” on page 103.

Jitter buffer-related datagram loss is quite high. The threshold for determining “Good” performance specified a jitter buffer loss of less than .500%, but the performance tests found a loss of 3.25%. And Lost Data also merits a warning. At .950%, it is awfully close to the “Marginal” threshold value of 1.000%.

These performance metrics are certainly causes for concern. Look at the Diagnosis table to find out why call quality was so poor:



Severity	Device/Link	Diagnosis
⊗	Outgoing: Link 7 (L3)	Congestion: detected on an interface, exceeding the 50.000% threshold. 10.42.30.2, Serial0/0, reported 96.541% utilization. Time detected: 10/14/2002 at 3:37:46 PM.
⊗	Outgoing: Link 7 (L3)	Congestion: detected on an interface, exceeding the 50.000% threshold. 10.42.30.1, Serial2/1, reported 100.000% utilization. Time detected: 10/14/2002 at 3:37:48 PM.
⊗	Outgoing: Link 5 (L3)	Congestion: detected on an interface. 10.42.2.47, Ethernet1, reported 0.875% packets that experienced multiple collisions before being sent. Time detected: 10/14/2002 at 3:38:01 PM.
⊗	Outgoing: Link 6 (L3)	Congestion: detected on an interface. 10.42.1.47, Ethernet0, reported 0.736% packets that experienced multiple collisions before being sent. Time detected: 10/14/2002 at 3:38:03 PM.

In this case, the issues on the network that contributed to the poor call quality stem from network **congestion**. The jitter-buffer loss, for example, was surely caused by congested links that held up some packets while others passed through more quickly. And you can see that the congestion problems on Link 7's serial interfaces are the most urgent.

Now that you know the results, you need to see how it all started. What VoIP-related problem did a user report, and how did someone configure Vivinet Diagnostics to diagnose it?

7.1.2 The Problem

The Senior Network Administrator is on vacation, and Hugh, a Network Engineer, has been left holding the pager and accepting incoming help-desk requests. When a coworker reports choppy, garbled calls on her IP phone, Hugh decides to investigate.

The coworker's phone has the IP address `10.42.6.18`. She reports that another coworker in the Raleigh office, on the subnet `10.42.4.x`, could barely understand her when she called him half an hour ago. Hugh starts up Vivinet Diagnostics and accesses a list of endpoint IP addresses the IT team maintains.

7.1.3 Define View

Click the **Define** view tab to see how Hugh defined the problem diagnosed in `EndpointSample1.dgv`.

The **Performance Endpoints** banner indicates endpoints acted as Target Devices for this Diagnosis. Hugh supplied the IP addresses of computers on which NetIQ Performance Endpoints had been installed several weeks ago.

Endpoint 1, which acted as the caller when generating test VoIP traffic, has an IP address of `10.42.6.104`, the same subnet as the phone that experienced the problem. **Endpoint 2**, the called party in the test traffic streams, has an IP address of `10.42.4.81`, the same subnet as the person on the receiving end who had trouble understanding the call.

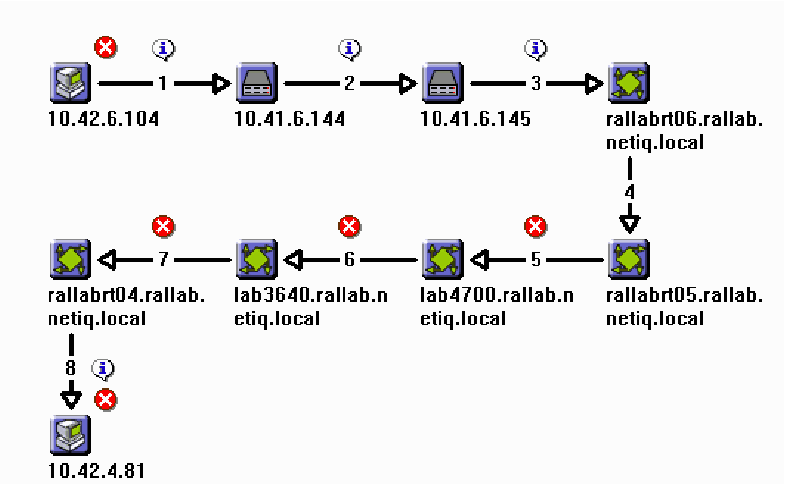
The **Call Script** field indicates the **G.711a** call script, which emulated the G.711a codec in the VoIP performance tests, was selected. The G.711a codec is a high-performance codec that needs 64 kbps of bandwidth in each call direction, which is a fair amount of bandwidth if the network is heavily utilized. For more information, see Section 4.2.2, "Reviewing Codecs," on page 60.

Click **View** to see whether any optional parameters were selected. Note that no QoS was selected in the **QoS name** field. Hugh's problem definition matches the corporate VoIP network, where no QoS scheme was active when the poor VoIP call performance was reported.

With the problem definition complete, Hugh is ready to start the Diagnosis. Now click the **Diagnose** view tab to view the path the simulated VoIP calls took between the endpoints when Hugh ran the Diagnosis.

7.1.4 Diagnose View

The Path Trace for the `EndpointSample1` Diagnosis looks like this:

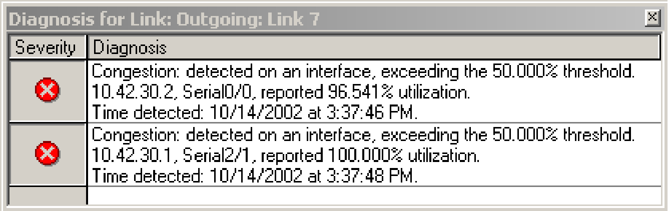

1
2
3
10.42.6.104
10.41.6.144
10.41.6.145
rallabrt06.rallab.netiq.local
4
7
6
5
rallabrt04.rallab.netiq.local
lab3640.rallab.netiq.local
lab4700.rallab.netiq.local
rallabrt05.rallab.netiq.local
8
10.42.4.81

As you can see, the path contained several hops, and quite a few issues were found. Every severity icon indicates at least one issue. Any issue Vivinet Diagnostics flagged during the Diagnosis could have contributed to the problem Hugh is troubleshooting.

The following topic looks more closely at just a few of the issues.

7.1.5 Issue Details

Looking at the Path Trace showing the Outgoing direction, click the red severity icon at **Link 7**, which flags an issue with a severity level of “Error.” You see the following Diagnosis:

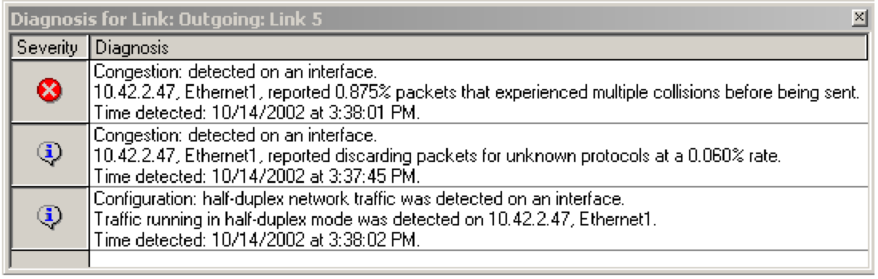


Diagnosis for Link: Outgoing: Link 7

Severity	Diagnosis
⊗	Congestion: detected on an interface, exceeding the 50.000% threshold. 10.42.30.2, Serial0/0, reported 96.541% utilization. Time detected: 10/14/2002 at 3:37:46 PM.
⊗	Congestion: detected on an interface, exceeding the 50.000% threshold. 10.42.30.1, Serial2/1, reported 100.000% utilization. Time detected: 10/14/2002 at 3:37:48 PM.

Although the industry recommendation for utilization on a VoIP network is 50%, one serial interface on Link 7 was reporting **100% utilization**, while another serial interface on this link was reporting **96.541% utilization**. This congestion problem is probably so severe because Link 7, a frame relay link, has less bandwidth than the links directly upstream.

More symptoms of congestion were also flagged on the Path Trace. Click the severity icon at **Link 5**:



Diagnosis for Link: Outgoing: Link 5

Severity	Diagnosis
⊗	Congestion: detected on an interface. 10.42.2.47, Ethernet1, reported 0.875% packets that experienced multiple collisions before being sent. Time detected: 10/14/2002 at 3:38:01 PM.
ⓘ	Congestion: detected on an interface. 10.42.2.47, Ethernet1, reported discarding packets for unknown protocols at a 0.060% rate. Time detected: 10/14/2002 at 3:37:45 PM.
ⓘ	Configuration: half-duplex network traffic was detected on an interface. Traffic running in half-duplex mode was detected on 10.42.2.47, Ethernet1. Time detected: 10/14/2002 at 3:38:02 PM.

The Ethernet link to the router **10.42.2.47** reports two symptoms: a high rate of multiple collisions, and an elevated rate of discarding packets with unknown protocols. Both are associated with congestion:

- multiple collisions occur when a device has to re-send packets several times because they have collided with other packets crowding the segment.
- packets whose protocols are "unknown" were probably sent by a network device, such as a server or printer, to advertise services. Because they are overloading the Ethernet segment, these packets are being discarded from router queues.

Press `[F1]` to view the Help for this window. The Help topic contains alphabetized explanations of all possible diagnoses. Scroll down to the **Congestion** diagnoses to find the following definitions:

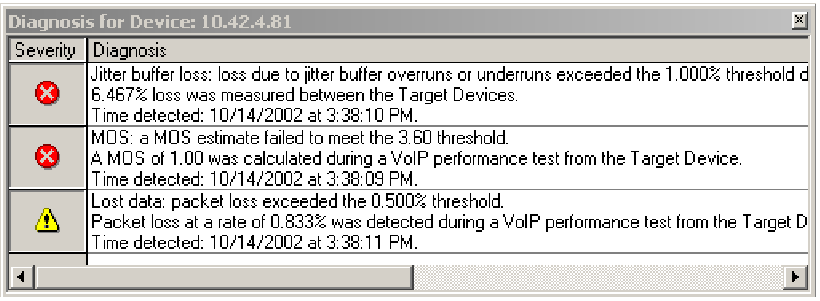
- **Device reported discarding packets for unknown protocols** — Frequently discarding packets whose protocols are unknown is an indication a network device or service is filling the pipes with unnecessary packets. This type of congestion may indicate a configuration issue.
- **Device reported N multiple collisions** — Ethernet collisions, which indicate congestion, are a common cause of individual packet delay and jitter.

The white severity icon next to the "Configuration" Diagnosis for Link 5 indicates an issue with a severity level of Info. In the Help, find the series of **Configuration** diagnoses and read the following definition:

- **Half-duplex network traffic was detected** — The indicated interface has been operating in half-duplex mode, which is inappropriate for VoIP traffic. Full-duplex mode (sending and receiving simultaneously) is recommended for VoIP traffic.

A configuration problem on an interface on the router specified in the Diagnosis is contributing to the congestion problem. Half-duplex configuration probably caused the multiple collisions.

Now click the very last **Error** icon, next to the Endpoint 2 Target Device, to view the following Diagnosis:



Diagnosis for Device: 10.42.4.81

Severity	Diagnosis
⊗	Jitter buffer loss: loss due to jitter buffer overruns or underruns exceeded the 1.000% threshold d 6.467% loss was measured between the Target Devices. Time detected: 10/14/2002 at 3:38:10 PM.
⊗	MOS: a MOS estimate failed to meet the 3.60 threshold. A MOS of 1.00 was calculated during a VoIP performance test from the Target Device. Time detected: 10/14/2002 at 3:38:09 PM.
⚠	Lost data: packet loss exceeded the 0.500% threshold. Packet loss at a rate of 0.833% was detected during a VoIP performance test from the Target D Time detected: 10/14/2002 at 3:38:11 PM.

The severity icons have drawn Hugh's attention to the most alarming problems on this path: exceptionally high datagram loss due to **jitter buffer underruns**, and plenty of **lost data**. The datagram loss that occurred at the Target Device was assigned a severity of **Error**. An actual loss rate of **0.833%** has been measured within the last few minutes, during a VoIP performance test Vivinet Diagnostics just ran. By contrast, some less-severe data loss flagged on Links 1-3 was deduced from a few Ethernet media errors that occurred on the devices at some point since they came online.

When a datagram is lost during a VoIP transmission, a conversation can lose an entire syllable or word. Packet loss is one of the statistics Vivinet Diagnostics uses to calculate a MOS for each simulated VoIP call it sends between the endpoints. For more information, see Section 5.3.7, "Mean Opinion Score," on page 103.

Due to datagram loss, the call quality measured from test traffic sent over this path was abysmal, resulting in an extremely low **MOS** of only **1.00**.

7.1.6 Conclusions

Our Network Engineer, Hugh, has his work cut out for him. The issues flagged on this network point to a severe VoIP performance problem with poor call quality. In addition to the myriad "**Congestion**" diagnoses, several other factors also lead us to conclude the network is congested. Congestion is the likely cause of the jitter buffer underruns. If datagrams are queued in an overtaxed router, they fill up the jitter buffer at the receiving phone and have to be discarded. Similarly, the Ethernet media errors and multiple collisions associated with switches on this network also point to switch congestion.

Hugh can do a couple of things right away to improve call quality. Remember, the problem definition did not include any QoS. This network would likely benefit from the implementation of a VoIP-specific QoS scheme. To see whether the IT Team should take steps toward implementing QoS on the network, Hugh can run the same Diagnosis again, but with a QoS scheme applied to the call script. If call quality improves, it is probably time to configure the routers for QoS.

And Hugh also needs to reconfigure the interfaces on the router **10.42.2.47** and the switch **10.41.6.144** so they are operating in full-duplex, not half-duplex mode.

However, because the call quality measured was so very low, additional bandwidth may be needed. After all, the G.711 codecs take more bandwidth than other codecs and usually deliver the highest-quality calls. Call quality might have been even worse if a lower-performing codec, such as one of the G.723.1 codecs, had been used. For example, the theoretical maximum MOS achievable by the G.723.1-ACELP codec is only 3.69, without any other factors — such as packet loss — to impede call quality.

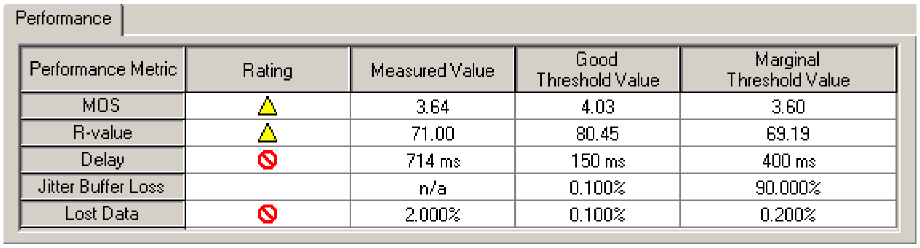
7.2 Sample Diagnosis Between Nortel Phones

The "Section 7.1, "Sample Diagnosis Between Endpoints," on page 115" topic discussed a scenario in which Vivinet Diagnostics uses endpoints to troubleshoot a problem with VoIP call performance. This next topic discusses some of the data you can get from a Diagnosis using Nortel phones instead of endpoints as Target Devices.

Our discussion focuses on one of the sample Diagnosis files that ship with Vivinet Diagnostics. The file `NortelPhone2PhoneSample1.dgv` is stored in the `Program Files\NetIQ\Vivinet Diagnostics\Samples` folder. In the Vivinet Diagnostics Console, click **Open** on the File menu and browse to it. Then use the following topics to navigate the Console and understand the Diagnosis process.

7.2.1 Diagnosis

First, click the **Report** view tab to check the results from the VoIP performance tests used to flag the issues on the network. Take a look at the Results table:

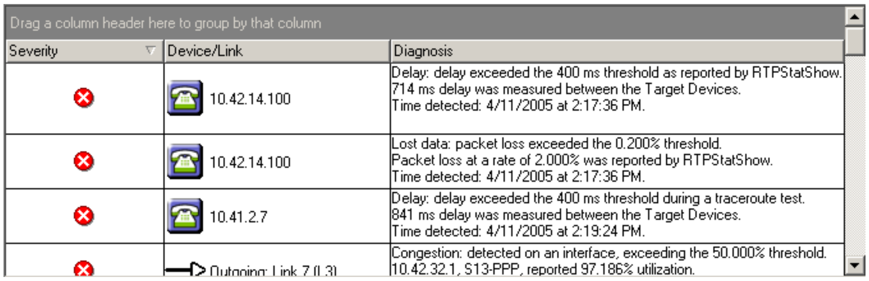


Performance

Performance Metric	Rating	Measured Value	Good Threshold Value	Marginal Threshold Value
MOS	⚠	3.64	4.03	3.60
R-value	⚠	71.00	80.45	69.19
Delay	⊘	714 ms	150 ms	400 ms
Jitter Buffer Loss		n/a	0.100%	90.000%
Lost Data	⊘	2.000%	0.100%	0.200%

The red performance rating icons indicate Delay and Lost Data were the worst of the performance metrics used in calculating the MOS and R-value. The substantial rates of delay and packet loss raised the MOS and made some calls on this network sound choppy or garbled.

Now look at the Diagnosis table:



Drag a column header here to group by that column

Severity	Device/Link	Diagnosis
⊗	☎ 10.42.14.100	Delay: delay exceeded the 400 ms threshold as reported by RTPStatShow. 714 ms delay was measured between the Target Devices. Time detected: 4/11/2005 at 2:17:36 PM.
⊗	☎ 10.42.14.100	Lost data: packet loss exceeded the 0.200% threshold. Packet loss at a rate of 2.000% was reported by RTPStatShow. Time detected: 4/11/2005 at 2:17:36 PM.
⊗	☎ 10.41.2.7	Delay: delay exceeded the 400 ms threshold during a traceroute test. 841 ms delay was measured between the Target Devices. Time detected: 4/11/2005 at 2:19:24 PM.
⊗	Outgoing: Link 7 (L3)	Congestion: detected on an interface, exceeding the 50.000% threshold. 10.42.32.1, S13-PPP, reported 97.186% utilization.

The worst problem on the network is delay and the most congested link is Link 7, a serial link with high utilization.

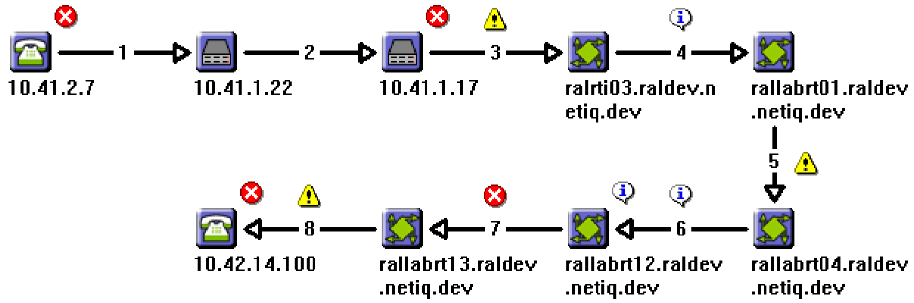
7.2.2 Define View

Click the **Define** view tab. The **Phones** banner indicates telephones acted as Target Devices for this Diagnosis.

In this sample Diagnosis, **Phone 1** is considered the caller. It has an IP address of `10.41.2.7`. **Phone 2**, the called party, has an IP address of `10.42.14.100`. Therefore, Vivinet Diagnostics requested records pertaining to calls made from `10.41.2.7` to `10.42.14.100`.

7.2.3 Diagnose View

The Path Trace for the `NortelPhone2PhoneSample1` Diagnosis depicts the following items:

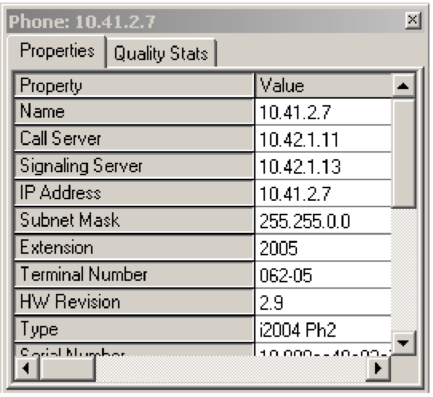


1
10.41.2.7
2
10.41.1.22
3
10.41.1.17
4
ralrti03.raldev.netiq.dev
rallabrt01.raldev.netiq.dev
5
6
rallabrt04.raldev.netiq.dev
7
rallabrt12.raldev.netiq.dev
8
rallabrt13.raldev.netiq.dev
10.42.14.100

Twenty-three issues were found (represented by the ten severity icons), five of which received a severity rating of Error. Review the following topics to take a closer look at some of the issues Vivinet Diagnostics flagged on the network.

Phone and Call Details

Starting with the Path Trace showing the Outgoing direction, click the first Target Device icon. The Phone properties provide general information about Phone 1, as well as specific information about any calls recently made by this phone on the Properties tab. The **Type** field reveals Phone 1 was an i2004 Phase 2 phone.

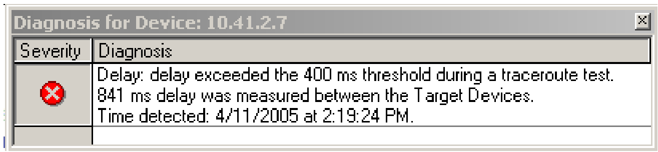


Property	Value
Name	10.41.2.7
Call Server	10.42.1.11
Signaling Server	10.42.1.13
IP Address	10.41.2.7
Subnet Mask	255.255.0.0
Extension	2005
Terminal Number	062-05
HW Revision	2.9
Type	i2004 Ph2
Serial Number	[illegible]

On the Quality Stats tab, scroll through the rows of information. Notice Local Packet Loss registered as 0.000% for Phone 1. Remember, overall Lost Data for the call was 2.000% (as shown on the Report view). Therefore, the lost data that contributed to the less-than-acceptable MOS score of 3.64 did not occur at this end of the Path Trace, but occurred elsewhere in your network.

Issue Details

The first severity icon flags an issue at the Phone 1 Target Device with a severity level of **Error**. Click the icon to see the following Diagnosis.

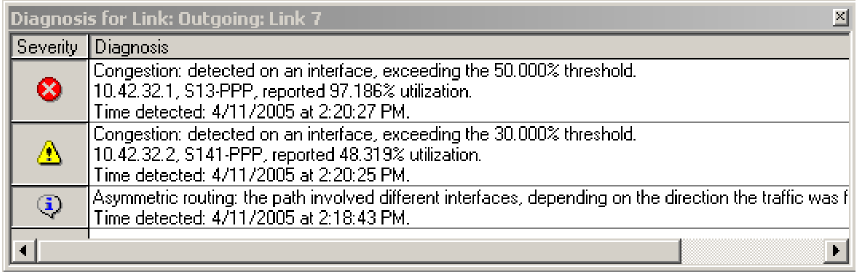


Diagnosis for Device: 10.41.2.7

Severity	Diagnosis
⊗	Delay: delay exceeded the 400 ms threshold during a traceroute test. 841 ms delay was measured between the Target Devices. Time detected: 4/11/2005 at 2:19:24 PM.

The issue was flagged because "delay exceeded the 400-ms threshold" during a traceroute test. In fact, at Phone 1, delay was more than twice the acceptable limit, hence the "Error" warning icon. The Diagnosis of delay on Phone 1 placed third on the list of diagnoses on the Diagnosis table on the Report view.

Now click the Error icon at **Link 7**, the congested interface, to view its Diagnosis:



Diagnosis for Link: Outgoing: Link 7

Severity	Diagnosis
⊗	Congestion: detected on an interface, exceeding the 50.000% threshold. 10.42.32.1, S13-PPP, reported 97.186% utilization. Time detected: 4/11/2005 at 2:20:27 PM.
⚠	Congestion: detected on an interface, exceeding the 30.000% threshold. 10.42.32.2, S141-PPP, reported 48.319% utilization. Time detected: 4/11/2005 at 2:20:25 PM.
ℹ	Asymmetric routing: the path involved different interfaces, depending on the direction the traffic was f Time detected: 4/11/2005 at 2:18:43 PM.

The network is quite congested. Vivinet Diagnostics found congestion statistics with a severity of "Error" and "Warning" on an interface on each side of the link.

The Diagnosis for Link 7 also highlights an asymmetric routing issue. Press `[F1]` for help, and scroll down to the **Asymmetric routing** diagnoses. You see the following definition:

- **Asymmetric routing** — When traceroute tests were run between the Target Devices, the identified paths for each direction were different. The paths differed because the path in one direction included more links, or because the path in each direction involved different device interfaces. The differences indicate an asymmetric network configuration. Asymmetric routing may point to a loop in your network and can degrade VoIP call quality because the conversation may take longer to travel from one conversant to the other, creating a "walkie-talkie" effect (delayed speech).

Clicking other severity icons reveals several instances of the same configuration problem discovered during device polling. Links 3, 4, and 6 do not have RTP Priority or LLQ configured. These devices are not giving voice traffic expedited handling. RTP priority works when routers identify voice traffic by its RTP port numbers and place it in a priority queue, giving it preferential treatment over all other traffic. Low Latency Queuing (LLQ) reduces latency for voice traffic by classifying it and allowing packets in the voice class to be sent before packets in other queues are sent.

7.2.4 Conclusions

Like the network discussed in Section 7.1, “Sample Diagnosis Between Endpoints,” on page 115, this congested network is not ready to carry high-quality VoIP calls. In fact, users on this network are likely to find the calls slightly garbled due to packet loss. The situation is not nearly as serious as the congestion problem diagnosed in the endpoint-to-endpoint Diagnosis, however, where a MOS of 1.00 was calculated for simulated VoIP calls.

Similar to the network situation discussed in the endpoint Diagnosis, the Nortel VoIP network is not configured to use a QoS scheme, which would probably improve things. Because call quality is not terrible — the MOS measured value of 3.64 corresponds to “Marginal” call quality — implementing QoS would very likely allow the network to carry VoIP calls without the need for additional bandwidth.

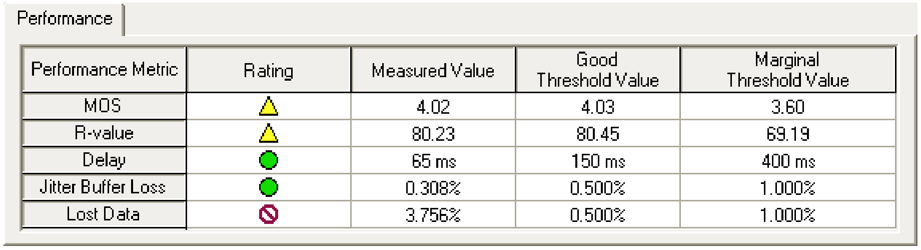
7.3 Sample Diagnosis Between VoIP and POTS Phones

This topic discusses some of the data you can get from a Diagnosis between a POTS (Plain Old Telephone Service) phone and a VoIP phone, and shows you how to use that data to improve the quality of calls on your network.

The discussion focuses on one of the sample Diagnosis files that ship with Vivinet Diagnostics. The file, `VoIP2POTSSample1.dgv`, is stored in the `Program Files\NetIQ\Vivinet Diagnostics\Samples` folder. In the Vivinet Diagnostics Console, click **Open** on the File menu and browse to it. Then use the following topics to navigate the Console and understand the Diagnosis process.

7.3.1 Diagnosis

First, click the **Report** view tab to check the results from the VoIP performance tests used to flag the issues on the network. Take a look at the Results table:

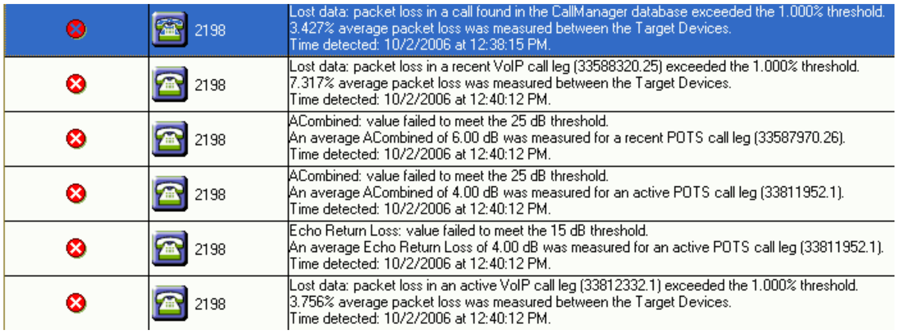


Performance

Performance Metric	Rating	Measured Value	Good Threshold Value	Marginal Threshold Value
MOS	△	4.02	4.03	3.60
R-value	△	80.23	80.45	69.19
Delay	●	65 ms	150 ms	400 ms
Jitter Buffer Loss	●	0.308%	0.500%	1.000%
Lost Data	⊘	3.756%	0.500%	1.000%

Notice the MOS value of 4.02 rates a yellow performance icon, which indicates a marginal value. Delay and Jitter Buffer Loss are good, as indicated by the green performance rating icon, so these values are not contributing to the marginal MOS value. The red performance rating icon indicates Lost Data was the worst of the performance metrics used in calculating the MOS. So the substantial rate of packet loss (3.756%) is what affected the MOS and made the active call on this network sound choppy or garbled.

Now look at the Diagnosis table:

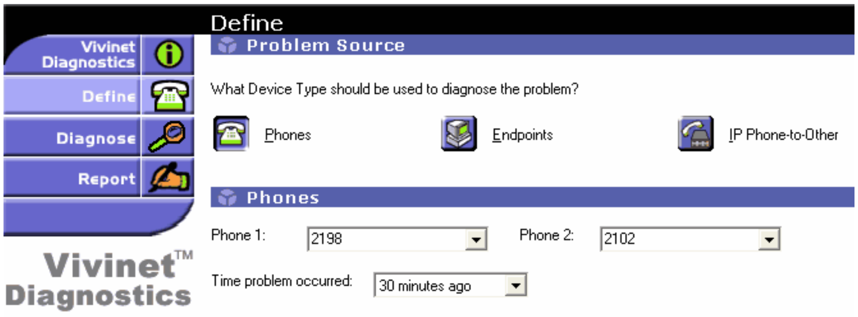


⊗	☎ 2198	Lost data: packet loss in a call found in the CallManager database exceeded the 1.000% threshold. 3.427% average packet loss was measured between the Target Devices. Time detected: 10/2/2006 at 12:38:15 PM.
⊗	☎ 2198	Lost data: packet loss in a recent VoIP call leg (33588320.25) exceeded the 1.000% threshold. 7.317% average packet loss was measured between the Target Devices. Time detected: 10/2/2006 at 12:40:12 PM.
⊗	☎ 2198	ACombined: value failed to meet the 25 dB threshold. An average ACombined of 6.00 dB was measured for a recent POTS call leg (33587970.26). Time detected: 10/2/2006 at 12:40:12 PM.
⊗	☎ 2198	ACombined: value failed to meet the 25 dB threshold. An average ACombined of 4.00 dB was measured for an active POTS call leg (33811952.1). Time detected: 10/2/2006 at 12:40:12 PM.
⊗	☎ 2198	Echo Return Loss: value failed to meet the 15 dB threshold. An average Echo Return Loss of 4.00 dB was measured for an active POTS call leg (33811952.1). Time detected: 10/2/2006 at 12:40:12 PM.
⊗	☎ 2198	Lost data: packet loss in an active VoIP call leg (33812332.1) exceeded the 1.000% threshold. 3.756% average packet loss was measured between the Target Devices. Time detected: 10/2/2006 at 12:40:12 PM.

Calls originating from phone number 2198 seem to be suffering from data loss, at least during two recent calls and in the active call. In fact, the active VoIP call leg (33812332.1) suffered 3.756% data loss, the same rate of data loss that affected the MOS result. Review the next topic to analyze the problem itself and see how it was defined.

7.3.2 Define View

Click the **Define** view tab. The Problem Source section indicates telephones acted as Target Devices for this Diagnosis.



Define

Problem Source

What Device Type should be used to diagnose the problem?

Phones   Endpoints   IP Phone-to-Other

Phones

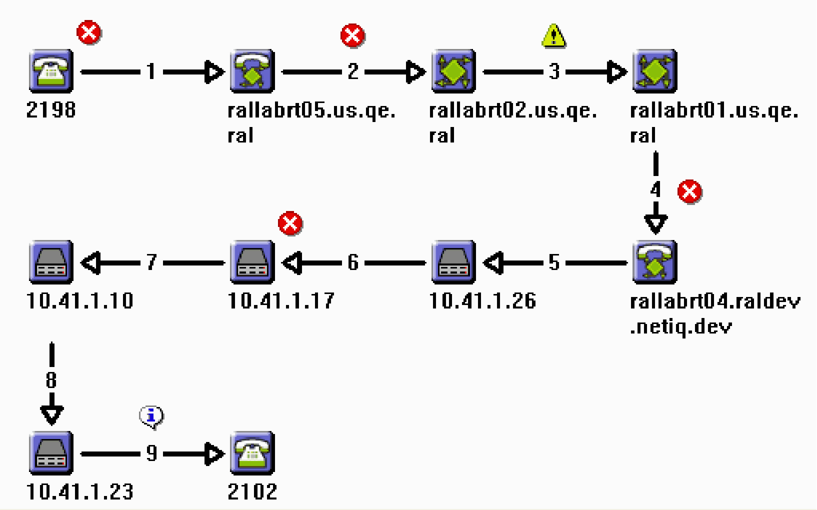
Phone 1: 2198   Phone 2: 2102

Time problem occurred: 30 minutes ago

In this sample Diagnosis, **Phone 1** was considered the source. It has an extension number of 2198. **Phone 2**, the destination, has an extension number of 2102. Therefore, Vivinet Diagnostics requested records pertaining to calls made from phone 2198 to phone 2102, as well as calls made in the other direction — from phone 2102 to phone 2198. Any records found between the source and destination phones are displayed in the Call Details tab of the Properties dialog box for Phone 1. Conversely, the Call Details tab of the Properties dialog box for Phone 2 displays records found between the destination and source phones.

7.3.3 Diagnose View

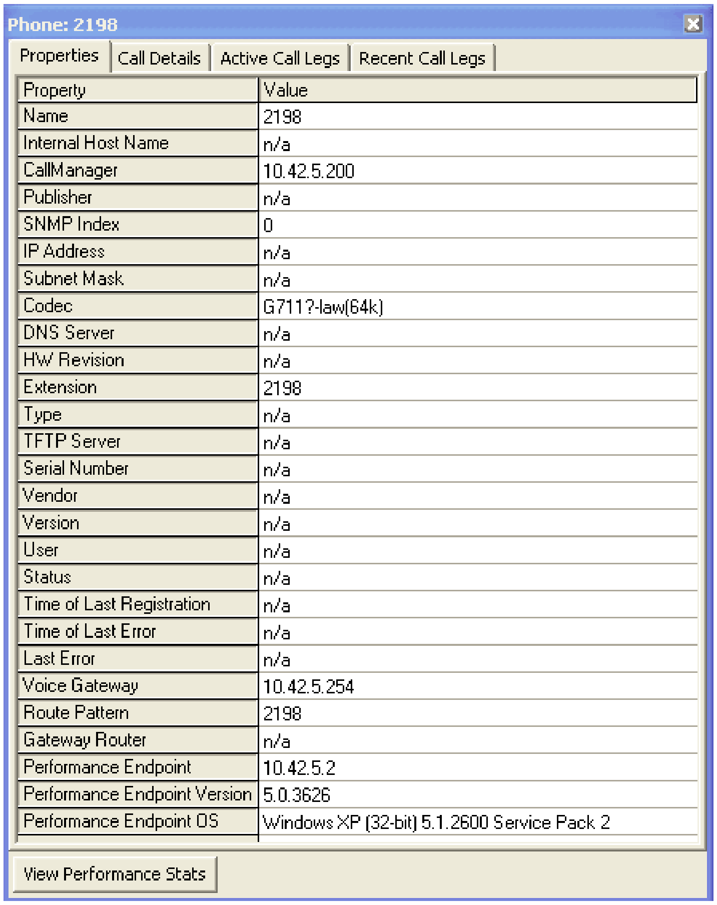
The outgoing Path Trace for the `VoIP2POTSSample1` Diagnosis depicts the following items:



The severity icons represent issues found between the source phone 2198 and the destination phone 2102. The red icons indicate issues severe enough to warrant a rating of Major Error. The following topics offer a closer look at some of the issues Vivinet Diagnostics flagged on the network.

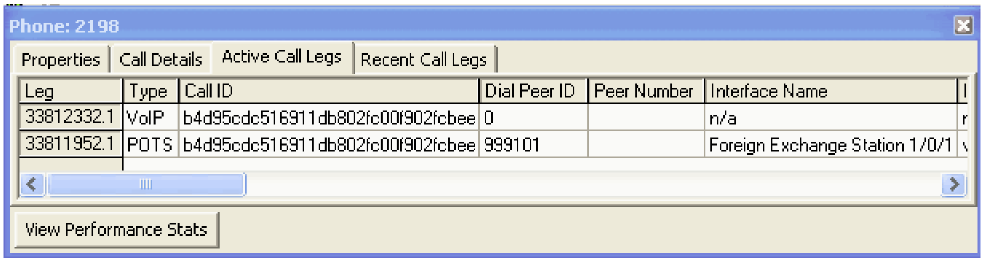
Phone and Call Details

Starting with the Path Trace showing the Outgoing direction, click the Target Device icon for phone 2198. The Phone dialog box contains general information about phone 2198, as well as specific information about the legs of active and recent calls, such as dial peer, interface type, call status, and duration. The **IP Address** field on the Properties tab shows a value of “n/a” and the **Voice Gateway** field contains an IP address. This information tells you phone 2198 is a POTS phone. If phone 2198 were an IP phone, the **IP Address** field would contain an IP address.



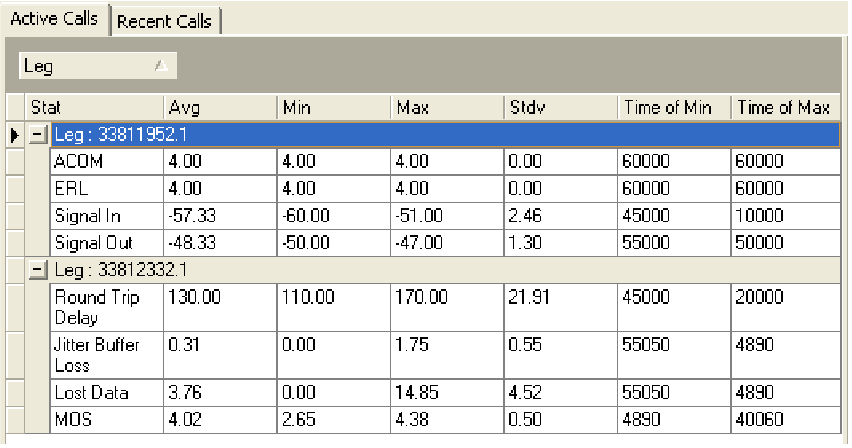
Property	Value
Name	2198
Internal Host Name	n/a
CallManager	10.42.5.200
Publisher	n/a
SNMP Index	0
IP Address	n/a
Subnet Mask	n/a
Codec	G711?-law(64k)
DNS Server	n/a
HW Revision	n/a
Extension	2198
Type	n/a
TFTP Server	n/a
Serial Number	n/a
Vendor	n/a
Version	n/a
User	n/a
Status	n/a
Time of Last Registration	n/a
Time of Last Error	n/a
Last Error	n/a
Voice Gateway	10.42.5.254
Route Pattern	2198
Gateway Router	n/a
Performance Endpoint	10.42.5.2
Performance Endpoint Version	5.0.3626
Performance Endpoint OS	Windows XP (32-bit) 5.1.2600 Service Pack 2

Click the Active Call Legs tab to see data for two call legs: 33812332.1 (the VoIP leg) and 33811952.1 (the POTS leg).



Leg	Type	Call ID	Dial Peer ID	Peer Number	Interface Name	I
33812332.1	VoIP	b4d95cdc516911db802fc00f902fcbee	0		n/a	r
33811952.1	POTS	b4d95cdc516911db802fc00f902fcbee	999101		Foreign Exchange Station 1/0/1	\

Remember, the VoIP leg was identified on the Report view as having severe data loss. Click **View Performance Stats** and review the data for leg 33812332.1.



Stat	Avg	Min	Max	Stdv	Time of Min	Time of Max
Leg : 33811952.1						
ACOM	4.00	4.00	4.00	0.00	60000	60000
ERL	4.00	4.00	4.00	0.00	60000	60000
Signal In	-57.33	-60.00	-51.00	2.46	45000	10000
Signal Out	-48.33	-50.00	-47.00	1.30	55000	50000
Leg : 33812332.1						
Round Trip Delay	130.00	110.00	170.00	21.91	45000	20000
Jitter Buffer Loss	0.31	0.00	1.75	0.55	55050	4890
Lost Data	3.76	0.00	14.85	4.52	55050	4890
MOS	4.02	2.65	4.38	0.50	4890	40060

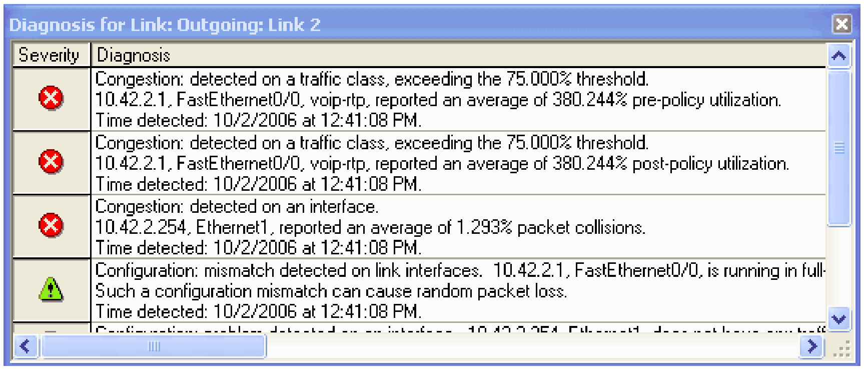
Notice average Lost Data registered as 3.76%. Remember, overall Lost Data for the call was 3.756% (as shown on the Report view). Therefore, the lost data that contributed to the marginal MOS score of 4.02 probably occurred at this end of the Path Trace. But you do not yet know the cause of the packet loss and so much delve further into the Path Trace to search for clues.

Severe Issue Details

The first severity icon in the Path Trace flags issues at phone 2198 with a severity level of **Error**. Click the icon to review a list of the same diagnoses summarized on the Report view. It is evident the packet loss between phones 2198 and 2102 is severe.

Note the frequency with which packet loss exceeded the threshold. And again, lost data for call leg 33812332.1 was measured at 3.756%, the overall Lost Data average for the call (as shown on the Report view).

Click the second severity icon, just above Link 2.



Diagnosis for Link: Outgoing: Link 2

Severity	Diagnosis
✖	Congestion: detected on a traffic class, exceeding the 75.000% threshold. 10.42.2.1, FastEthernet0/0, voip-rtp, reported an average of 380.244% pre-policy utilization. Time detected: 10/2/2006 at 12:41:08 PM.
✖	Congestion: detected on a traffic class, exceeding the 75.000% threshold. 10.42.2.1, FastEthernet0/0, voip-rtp, reported an average of 380.244% post-policy utilization. Time detected: 10/2/2006 at 12:41:08 PM.
✖	Congestion: detected on an interface. 10.42.2.254, Ethernet1, reported an average of 1.293% packet collisions. Time detected: 10/2/2006 at 12:41:08 PM.
⚠	Configuration: mismatch detected on link interfaces. 10.42.2.1, FastEthernet0/0, is running in full- Such a configuration mismatch can cause random packet loss. Time detected: 10/2/2006 at 12:41:08 PM.
	Configuration: problem detected on an interface. 10.42.2.254, Ethernet1, does not have any traff

Notice congestion was the Diagnosis for all three Error-severity issues. In fact, the congestion detected on interface 10.42.2.254 caused average packet collisions of 1.293%. Packet collisions usually lead to packet loss. So what is causing the packets to collide? More than likely, the cause is the mismatch in duplex configuration indicated by the green warning symbol:

```
“Configuration: mismatch detected on link interfaces. 10.42.2.1, FastEthernet0/0,
is running in full-duplex mode, while 10.42.2.254, Ethernet1,is running in half-
duplex mode.”
```

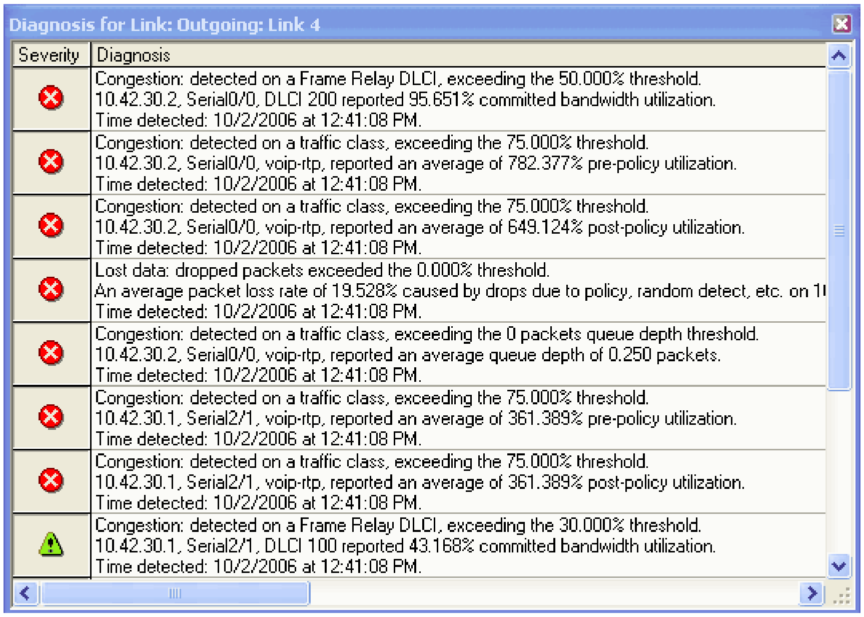
One interface is operating in half-duplex mode, which is inappropriate for VoIP traffic. Such a configuration mismatch can cause random packet loss. Full-duplex mode (sending and receiving simultaneously) is recommended for VoIP traffic.

In addition, it looks as though VoIP traffic is not being prioritized correctly on this link, as evidenced by the other congestion diagnoses:

```
"Congestion: detected on a traffic class, exceeding the 75.000% threshold.
10.42.2.1, FastEthernet0/0, voip-rtp, reported an average of 380.244% pre-policy
utilization."
```

When VoIP traffic is not given priority over data traffic, VoIP packets can become stuck in a queue behind data packets and subsequently lost or discarded.

Clicking the next Error icon (above Link 4) reveals not only oversubscribed priority classes, but dropped packets as well. Diagnoses of lost packets and 95.651% utilization may indicate bandwidth is too low for the VoIP traffic using this link.



Diagnosis for Link: Outgoing: Link 4

Severity	Diagnosis
✖	Congestion: detected on a Frame Relay DLCI, exceeding the 50.000% threshold. 10.42.30.2, Serial0/0, DLCI 200 reported 95.651% committed bandwidth utilization. Time detected: 10/2/2006 at 12:41:08 PM.
✖	Congestion: detected on a traffic class, exceeding the 75.000% threshold. 10.42.30.2, Serial0/0, voip-rtp, reported an average of 782.377% pre-policy utilization. Time detected: 10/2/2006 at 12:41:08 PM.
✖	Congestion: detected on a traffic class, exceeding the 75.000% threshold. 10.42.30.2, Serial0/0, voip-rtp, reported an average of 649.124% post-policy utilization. Time detected: 10/2/2006 at 12:41:08 PM.
✖	Lost data: dropped packets exceeded the 0.000% threshold. An average packet loss rate of 19.528% caused by drops due to policy, random detect, etc. on 1 Time detected: 10/2/2006 at 12:41:08 PM.
✖	Congestion: detected on a traffic class, exceeding the 0 packets queue depth threshold. 10.42.30.2, Serial0/0, voip-rtp, reported an average queue depth of 0.250 packets. Time detected: 10/2/2006 at 12:41:08 PM.
✖	Congestion: detected on a traffic class, exceeding the 75.000% threshold. 10.42.30.1, Serial2/1, voip-rtp, reported an average of 361.389% pre-policy utilization. Time detected: 10/2/2006 at 12:41:08 PM.
✖	Congestion: detected on a traffic class, exceeding the 75.000% threshold. 10.42.30.1, Serial2/1, voip-rtp, reported an average of 361.389% post-policy utilization. Time detected: 10/2/2006 at 12:41:08 PM.
⚠	Congestion: detected on a Frame Relay DLCI, exceeding the 30.000% threshold. 10.42.30.1, Serial2/1, DLCI 100 reported 43.168% committed bandwidth utilization. Time detected: 10/2/2006 at 12:41:08 PM.

7.3.4 Conclusions

These congested links are not configured properly for carrying VoIP traffic. However, because call quality is not terrible — the MOS value of 4.02 corresponds to “Marginal” call quality — correcting the duplex configuration problem and reallocating the priority class would very likely allow the network to carry a larger volume of VoIP calls. Better still, increasing the amount of available bandwidth should provide relief for users whose calls have been garbled due to lost packets.

8 Working with NetIQ AppManager

NetIQ AppManager provides Knowledge Scripts that monitor and detect problems with VoIP quality and call quality. These scripts raise informational events as a result of the detected problems. Vivinet Diagnostics can work with AppManager, providing the means to diagnose more precisely any problems with VoIP quality between phones, Performance Endpoints, or other target devices such as routers and gateways.

8.1 How the Integration Works

Using an existing methodology, launching an Action script based on an event, the integration of AppManager and Vivinet Diagnostics involves two Action scripts — *Action_DiagnoseVoIPQuality* and *Action_DiagnoseNortelIPT* — that trigger Vivinet Diagnostics to diagnose the problem for events raised by the following Knowledge Scripts.

When you run one of the applicable monitoring Knowledge Scripts, Vivinet Diagnostics can diagnose the problem when any VoIP or call quality metric exceeds or fails to meet its threshold. AppManager uses Action scripts to invoke Vivinet Diagnostics. For more information, see Section 8.3, “Knowledge Scripts that Trigger Diagnoses,” on page 131.

These Action scripts use an interface to Vivinet Diagnostics to define the parameters of the Diagnosis, run the Diagnosis, and then save the results. The parameters used to define the Diagnosis are taken from the Knowledge Script that raised the event. The thresholds in the scripts correspond to the Marginal/Poor threshold in Vivinet Diagnostics. Results are saved in Diagnosis files, which have a file extension of `.DGV`.

Upon completion of the Diagnosis, AppManager raises an event that contains the results of the Diagnosis. An event for an *unsuccessful* Diagnosis contains an error message explaining why the Diagnosis was unsuccessful. In an event for a *successful* Diagnosis, the Message tab contains either the full path to the location of the output file or a URL to an HTML report. An HTML report is created only if the AppManager Report agent is installed on the computer on which the Diagnosis ran. The HTML report contains hyperlinks to the Diagnosis file.

For more information about interpreting a Diagnosis file, see Chapter 5, "Understanding Results," on page 71.

NOTE

- If the AppManager Report agent is installed on the computer on which the Action scripts are run, you can use the Report agent settings to allow the Diagnosis results to be integrated with the AppManager Report Binder. For more information, see the *Control Center User Guide for AppManager*.
- When the Report agent is being used, you can see all completed diagnoses by launching the AppManager Report Binder, which you access from the Extensions menu of the Operator Console.
- When you open a Diagnosis from the Report Binder, Internet Explorer makes a copy of the file in your `\temp` folder. If you click **Save** in Vivinet Diagnostics, this copy is updated. If you modify the Diagnosis parameters or rerun the Diagnosis, use **Save as** to save the file in a different folder.

8.2 Deployment

This topic discusses the two ways in which you can deploy Vivinet Diagnostics to work with AppManager. In both cases, Vivinet Diagnostics must be installed on the computer on which you run the Action scripts.

8.2.1 Diagnostics and AppManager on One Computer

The most common configuration is one in which the AppManager server components are installed on a single computer: repository, management server, Web management server, consoles, and agent, including the Report agent. Vivinet Diagnostics is installed on this same computer.

Installing both applications on the same computer allows the Action scripts to run on the management server computer, which is the default location. In addition, by installing both applications on the same computer, you can configure the AppManager Report Binder and Web management server to view Diagnosis results.

8.2.2 Diagnostics and AppManager on Separate Computers

An alternative configuration is one in which Vivinet Diagnostics, the AppManager agent, the Report agent, and the AppManager consoles are installed on a computer that is remote from the computer on which the AppManager repository, management server, and Web management server are installed.

Install Vivinet Diagnostics on each computer on which you have installed an AppManager Operator Console. Having the Operator Console and Vivinet Diagnostics on the same computer allows you to rerun a Diagnosis if necessary.

In this configuration, you must configure Action_DiagnoseVoIPQuality and Action_DiagnoseNortelIPT to run on the remote, or proxy, computer.

To configure the Action scripts to run on a proxy computer:

1. In the AppManager Operator Console or Control Center, run one of the applicable Knowledge Scripts on a resource object. For more information, see Section 8.3, "Knowledge Scripts that Trigger Diagnoses," on page 131.

2 Click the **Actions** tab. Depending on the script, Action_DiagnoseVoIPQuality or Action_DiagnoseNortelIPT is selected.

3 In the **Location** field, select **Proxy**.

4 Select the computer on which Vivinet Diagnostics and the AppManager agent are installed, and then click **OK**.

5 If necessary, provide any required information on the other tabs. For more information, click **Help** in the Properties dialog box.

6 Click **OK** to start the monitoring job.

8.3 Knowledge Scripts that Trigger Diagnoses

Knowledge Scripts from several modules raise events for problems that Vivinet Diagnostics can diagnose.

8.3.1 AppManager for Avaya Communication Manager

Two Knowledge Scripts from this module raise events that Vivinet Diagnostics can diagnose.

- The **AvayaCM_CallQuality** Knowledge Script monitors RTCP packets in the Avaya CM supplemental database for calls that recorded poor call quality statistics. The script raises an event when call quality metrics exceed or fall below a threshold.
- The **AvayaCM_PhoneQuality** Knowledge Script collects real-time voice quality statistics for active calls on Avaya IP phones. This script raises an event if voice quality statistics exceed or fall below a threshold during the data collection interval.

Events from both scripts trigger **Action_DiagnoseVoIPQuality** to launch Vivinet Diagnostics, which generates a Diagnosis between the two phones in a call based on the following information from the scripts:

- The phone numbers of the phones involved in the call
- MOS threshold, as set in the *Average MOS* parameter, or R-Value, as set in the *Average R-Value* parameter. Vivinet Diagnostics does not diagnose R-value. Instead, when a Diagnosis with a R-Value threshold is triggered, Vivinet Diagnostics translates the threshold into an equivalent MOS value. MOS is computed only for calls that use one of the following codecs: G.711u, G.711a, or G.729.
- Jitter, measured in milliseconds, as set in the *Maximum interval jitter*

  parameter
- Latency, measured in milliseconds, as set in the *Maximum interval latency*

  parameter
- Packet loss, measured as a percentage, as set in the *Maximum interval packet loss* parameter

8.3.2 AppManager for Cisco CallManager

Two Knowledge Scripts from this module raise events that Vivinet Diagnostics can diagnose.

The **CiscoCallMgr_CallQuality** Knowledge Script monitors the Cisco Unified CallManager Call Management Record (CMR) database for calls that recorded poor VoIP quality metrics. This script runs periodically, looks at all calls generated since the last time the script ran, and raises an event if a call's quality falls into the "poor" category.

The event triggers **Action_DiagnoseVoIPQuality** to launch Vivinet Diagnostics, which generates a Diagnosis between the two phones in a call based on the following information from this script.

- The phone numbers of the telephones involved in the call. At least one telephone must be an IP phone. The other can be an IP telephone or a traditional (POTS) telephone on the PSTN.
- The time the problem occurred, based on the schedule of the CallQuality script
- Delay, measured in milliseconds, as set in the *Maximum acceptable latency* parameter
- Lost data, expressed as a percentage, as set in the *Maximum acceptable percentage lost data* parameter

The **CiscoCallMgr_CallFailures** Knowledge Script monitors the CDR and CMR databases, looking at the termination codes for all calls. This script runs periodically, looks at all calls terminated since the last time the script ran, and raises an event if the number of calls that terminated abnormally exceeds the threshold you set for the *Maximum failed calls* parameter.

The event triggers **Action_DiagnoseVoIPQuality** to launch Vivinet Diagnostics, which generates a Diagnosis between the two phones in a call based on the following information from this script:

- The phone numbers of the telephones involved in the call. At least one telephone must be an IP phone. The other can be an IP telephone or a traditional (POTS) telephone on the PSTN.
- The time the problem occurred, based on the schedule of the CallFailures script
- Call quality threshold. Because no call quality threshold is configured in the CallFailures script, Vivinet Diagnostics uses its default threshold settings. For more information, see Section 3.5.5, "Setting Thresholds," on page 37.

8.3.3 AppManager for Nortel Communication Server 1000

One Knowledge Script from this module raises events that Vivinet Diagnostics can diagnose.

The **NortelCS_Alarms** Knowledge Script monitors the Nortel CS1000 proxy computer for Nortel CS1000 alarms. Nortel CS1000 components send alarms to the proxy computer using SNMP traps. When one of the following alarms is detected, the Alarms script raises an event that triggers **Action_DiagnoseNortelIPT** to invoke Vivinet Diagnostics.

Alarm	What It Means
QOS0022	Packet loss has reached the warning level
QOS0024	Latency has reached the warning level
QOS0026	Jitter has reached the warning level
QOS0028	R-factor has reached the warning level
QOS0030	Packet loss has reached the unacceptable level
QOS0032	Latency has reached the warning level
QOS0034	Jitter has reached the warning level

Vivinet Diagnostics generates a Diagnosis between the two Nortel Phase 2 IP phones involved in the call for which an alarm was raised.

8.3.4 AppManager for Nortel Communication Server 2100

Two Knowledge Scripts from this module raise events that Vivinet Diagnostics can diagnose.

- The **NortelCS2x_CallQuality** Knowledge Script monitors the QoS Collector Application records that the Core & Billing Manager pushes to the QoS file collector service, as well as the QoS syslog records sent by the CICM Element Manager to the QoS syslog collector service. This script raises an event for end-of-call quality problems related to MOS, R-Value, jitter, latency, and packet loss.
- The **NortelCS2x_PhoneQuality** Knowledge Script monitors the mid-call QoS records for the Phase 2 IP phones on which you run the script and raises an event for call quality problems related to MOS, R-Value, jitter, latency, and packet loss. The QoS syslog collector service receives those records from the Call Server and pushes those records to the supplemental database.

The events for both scripts trigger **Action_DiagnoseVoIPQuality** to launch Vivinet Diagnostics, which generates a Diagnosis between the two phones in a call.

8.3.5 AppManager for Phone Quality

One Knowledge Script from this module raises events that Vivinet Diagnostics can diagnose.

The **PhoneQuality_CiscoPhoneQuality** Knowledge Script polls Web-enabled Cisco IP phones for call quality statistics on active calls. When an active call is detected, the script collects or calculates values for average and maximum jitter, percentage of packet loss, listening MOS, and listening R-Value.

If, while the script is polling an IP phone, a call quality metric falls below or exceeds the threshold you set, the script raises an event while the call is active. The event triggers **Action_DiagnoseVoIPQuality** to launch Vivinet Diagnostics, which generates a Diagnosis between the two IP phones in the call based on the following information from the script:

- The phone numbers of the Web-enabled IP telephones involved in the call
- The time the problem occurred, based on the schedule of the script CiscoPhoneQuality script

8.3.6 AppManager for VoIP Quality

One Knowledge Script from this module raises events that Vivinet Diagnostics can diagnose.

The **VoIPQuality_CallPerf** Knowledge Scripts monitor VoIP quality by periodically driving synthetic VoIP traffic between two NetIQ Performance Endpoints. These scripts raise an event when VoIP Quality metrics exceed the thresholds you set and if a VoIP test fails to run.

The event triggers **Action_DiagnoseVoIPQuality** to launch Vivinet Diagnostics, which generates a Diagnosis between two endpoints in a test based on the following information from a CallPerf script:

- The talker and caller endpoints, respectively, used in the VoIP test
- The type of codec applied to the test. The Knowledge Script name indicates the codec in use: G.711a, G.711u, G.723-1ACELP, G.723.1-MPMLQ, G.726, G.729, or G.729A.
- Whether packet loss concealment was enabled
- Whether silence suppression was enabled
- The amount of delay set to occur between voice datagrams
- Whether Service Quality (DiffServ) was enabled, and which type
- The size of the jitter buffer

- Whether additional fixed delay was set, and how much
- The destination port number
- The voice activity rate, which, although you specify in the Knowledge Script, cannot be set in Vivinet Diagnostics. Vivinet Diagnostics uses a default voice activity rate of 50% when generating a Diagnosis.
- MOS threshold, as set in the *Minimum MOS* parameter, or R-Value, as set in the *Minimum R-Value* parameter. Vivinet Diagnostics does not diagnose R-value. Instead, when a Diagnosis with a R-Value threshold is triggered, Vivinet Diagnostics translates the threshold into an equivalent MOS value. MOS is computed only for calls that use one of the following codecs: G.711u, G.711a, or G.729.
- Delay, measured in milliseconds, as set in the *Maximum delay*

  parameter
- Lost data, measured as a percentage, as set in the *Maximum lost data*

  parameter
- Loss due to jitter buffer, measured in percentage, set to the *Maximum jitter buffer* loss parameter

8.4 Deleting Expired Diagnoses

A new Diagnosis results file is generated for each Diagnosis triggered by the Diagnose Action scripts. These files can build up over time, so consider deleting these files occasionally.

If you use the Report agent settings when generating the Diagnosis results, use the AMAdmin_DeleteExpiredReports Knowledge Script to automatically delete old reports. Reports generated as a result of the Diagnose Action scripts expire by default after 60 days.

8.5 Sharing Configuration for SNMP Version 3

Vivinet Diagnostics can diagnose devices running SNMP v3 by using the SNMP v3 permissions you may have already configured for AppManager. AppManager and Vivinet Diagnostics do not need to be installed on the same computer. For more information, see "Configuration for Version 3" on page 33.

8.6 Troubleshooting

The following topics should help you troubleshoot some of the more common problems you may encounter when using Vivinet Diagnostics together with AppManager.

An error message indicates Action_DiagnoseVoIPQuality will not run.

Ensure Vivinet Diagnostics version 1.1 or later is installed on the computer on which the Action script is running. That same computer requires Microsoft XML Parser version 3 or Internet Explorer 5.5 Service Pack 2 or later.

In addition, ensure you have registered your version of Vivinet Diagnostics.

You ran the Diagnosis, but cannot view the Diagnostic report from a different computer.

Ensure Vivinet Diagnostics version 1.1 or later is installed on the computer from which you are trying to view the Diagnostics report. If you have several AppManager Operator Consoles installed on remote computers, install Vivinet Diagnostics on these computers as well. By installing both the Operator Console and Vivinet Diagnostics on the same computer, you can view the Diagnostic report as well as rerun the Diagnosis.

Errors in the Diagnosis results indicate Vivinet Diagnostics cannot resolve the phone or query SNMP information.

If Vivinet Diagnostics cannot resolve phone or SNMP information, the Log Viewer is displayed when you attempt to open the Diagnosis file (`.dgv`). The Log Viewer displays all relevant error messages. In addition, if an error exists, Vivinet Diagnostics will not display results when you click the **Report** view tab in the Console.

Ensure you have configured Vivinet Diagnostics with the names and passwords of your Cisco Unified CallManagers, as well as the SNMP permissions required for querying SNMP information from routers. For more information, see Section 3.5.4, “Configuring CallManager User IDs and Passwords,” on page 36 and Section 3.5.1, “Configuring SNMP Permissions,” on page 32.

If you had not configured this information before you ran the Diagnosis, do so now, and then rerun the Diagnosis. You need only configure the CallManager and SNMP information once. Vivinet Diagnostics will use the information for all subsequent diagnoses.

AppManager raised several call quality events, but Vivinet Diagnostics generated only one Diagnosis.

To enable the Diagnose Action scripts to trigger Vivinet Diagnostics to run diagnoses as often as a problem occurs, disable or modify the “event collapsing” feature on the applicable Knowledge Scripts. Event collapsing allows AppManager to suppress, or collapse, what it considers to be duplicate events. However, you probably want Vivinet Diagnostics to diagnose a problem each time one occurs, even if it occurs between the same two targets. Vivinet Diagnostics cannot do that if AppManager has collapsed all call quality events between the same targets into one event. Use the **Advanced** tab of the applicable Knowledge Script to disable event collapsing, or at least to shorten the 20-minute collapsing interval.

For more information, see Section 8.3, “Knowledge Scripts that Trigger Diagnoses,” on page 131.

To disable or modify event collapsing:

1. In the Properties dialog box for the applicable script, click the **Advanced** tab.
2. *To disable event collapsing*, deselect **Collapse duplicate events into a single event**.
3. *To shorten the collapsing interval*, select a smaller number in the **Time interval for event collapsing** field.
4. Stop and then restart the Knowledge Script job so your changes are activated.

You receive a 404 error message when attempting to open a .DGV file on a Windows Server 2003 computer.

Tightened security of IIS in Windows Server 2003 prohibits the opening of unrecognized MIME types. Configure Windows Server 2003 to recognize the `.DGV` extension.

To configure Windows Server 2003:

1. Stop and then restart the Knowledge Script job so your changes are activated.
2. On the Windows Server 2003 computer, right-click **My Computer** and select **Manage**.
3. Expand **Services and Applications**, double-click **Internet Information Service**, and then double-click **Web Sites**.
4. Right-click the Web site in question (you may have several) and select **Properties**.

5. On the HTTP Headers tab, click **MIME Types**, and then click **New**.
6. In the **Extension** field, type `.DGV`.
7. In the **MIME type** field, type `application/octet-stream`.
8. Click **OK** three times to complete the change.

NOTE: You may need to stop and restart the Web site before the change takes effect.

A Cisco Unified CallManager Termination Codes

The table below explains all the return codes you might see in the Call Detail Records (CDRs) from Cisco Unified CallManager. For more information, see "Phone Call Details Tab" on page 78.

Termination Code	Description	Explanation
0	No error	No error.
1	Unallocated (unassigned) number	Indicates the called party cannot be reached because although the called party number is in a valid format, it is not currently allocated (assigned).
2	No route to specified transit network (national use)	Indicates one of the following: The equipment sending this code has received a request to route the call through a particular transit network it does not recognize. The equipment does not recognize the transit network either because the transit network does not exist or because the transit network exists but does not serve the equipment sending the code. The prefix 0 is invalid for the entered number.
3	No route to destination	Indicates one of the following: The called party cannot be reached because the network through which the call has been routed does not service the desired destination. This cause is supported on a network-dependent basis. A 1 was dialed when not required. Redial without the 1.
4	Send special information tone	Indicates one of the following: The prefix 1 is not required for this number. The called party cannot be reached for reasons of a long-term nature. The special information tone should be returned to the calling party.
5	Misdialed trunk prefix (national use)	Indicates the erroneous inclusion of a trunk prefix in the called party number.
6	Channel unacceptable	Indicates a called user cannot negotiate for a B-channel other than that specified in the SETUP message.
7	Call awarded and being delivered in an established channel	Indicates the user has been awarded the incoming call and the call is being connected to a channel (such as packet mode or X.25 virtual calls) already established to that user for similar calls.

Termination Code	Description	Explanation
8	Preemption	Indicates a call has been preempted.
9	Preemption - circuit reserved for reuse	Indicates a call has been preempted because the circuit is reserved for reuse.
16	Normal call clearing	Indicates normal call clearing has occurred.
17	User busy	Indicates the called party is unable to accept another call because the user busy condition has been encountered. Code 17 may be generated by the called user or by the network. In the case of user-determined user busy, it is noted that the user equipment is compatible with the call.
18	No user responding	Indicates a called party does not respond to a call establishment message with either an alerting or connect indication within the allotted prescribed period of time (before timer T303 or T310 has expired).
19	No answer from user (user alerted)	Indicates the called user has provided an alerting indication, but not a connect indication within a prescribed period of time (before timer T301 has expired).
20	Subscriber absent	Indicates one of the following:· A mobile station has logged off. Radio contact is not obtained with a mobile station. A personal telecommunications user is temporarily not addressable at any user-network interface.
21	Call rejected	Indicates one of the following: The equipment sending this cause does not wish to accept the call, although it could have accepted the call because it is neither busy nor incompatible. May be generated by the network, indicates the call was cleared due to a supplementary service constraint.
22	Number changed	Indicates the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this cause, cause #1 shall be used.
26	Non-selected user clearing	Indicates the user has not been awarded the incoming call.

Termination Code	Description	Explanation
27	Destination out of order	Indicates the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates a signal message was unable to be delivered to the remote party, as in the following examples: Physical layer or data link layer failure at the remote party User equipment off-line
28	Invalid number format (address incomplete)	Indicates one of the following: The called party cannot be reached because the called party number is not in a valid format or is not complete. The user should be returned a Special Intercept Announcement.
29	Facility rejected	Indicates one of the following: The network cannot provide the requested facility. A user in a special business group, such as a Centrex, dialed an undefined code.
30	Response to STATUS ENQUIRY	Indicates one of the following: This cause is included in the Status Message when the reason for sending the Status Message was the previous receipt of a Status Enquiry message. A user from outside a basic business group, such as a Centrex, has violated an access restriction feature.
31	Normal, unspecified	Used to report a normal event only when no other cause in the normal class applies.
34	No circuit/channel available	Indicates no appropriate circuit or channel is available to handle the call.
38	Network out of order	Indicates the network is not functioning correctly and the condition is likely to last a relatively long time. Immediately re-attempting the call is not likely to be successful.
39	Permanent frame mode connection out of service	Indicates a permanent connection was terminated, probably due to equipment failure.
40	Permanent frame mode connection operational	Indicates a permanent connection is operational again. The connection was previously terminated, probably due to equipment failure.
41	Temporary failure	Indicates the network is not functioning correctly and the condition is not likely to last a long time. The user may wish to attempt another call almost immediately. May also indicate a data link layer malfunction locally or at the remote network interface, or a call was cleared due to protocol errors at the remote network interface.

Termination Code	Description	Explanation
42	Switching equipment congestion	Indicates the switching equipment generating this cause is experiencing a period of high traffic.
43	Access information discarded	Indicates the network is unable to deliver user information (such as user-to-user information, low-level compatibility, or sub-address) to the remote users as requested.
44	Requested circuit/channel not available	Indicates the other side of the interface cannot provide the circuit or channel indicated by the requesting entity.
46	Precedence call blocked	Indicates the called remote device is busy.
47	Resource unavailable, unspecified	Indicates one of the following: No other cause in the resource unavailable class applies. The original destination is unavailable. Invoke redirection to a new destination.
49	Quality of Service not available	Indicates the network cannot provide the requested Quality of Service. May be a subscription problem.
50	Requested facility not subscribed	Indicates this facility is unavailable because the user has not subscribed to it.
53	Service operation violated	Indicates the user has violated the service operation.
54	Incoming calls barred	Indicates the user will not accept the call delivered in the SETUP message.
55	Incoming calls barred within CUG (Closed User Group)	Indicates the network does not allow the user to receiver calls.
57	Bearer capability not authorized	Indicates the user has requested a bearer capability implemented by the equipment that generated this cause, however the user is not authorized to use it. This common problem is caused by incorrect Telco provisioning of the line at the time of installation.
58	Bearer capability not presently available	Indicates the user has requested a bearer capability implemented by the equipment that generated this cause, however the bearer capability is unavailable at the present time. This problem may be due to a temporary network problem or a subscription problem.
62	Inconsistency in designated outgoing access information and subscriber class	Indicates an inconsistency in the designated outgoing access information and subscriber class.
63	Service or option not available, unspecified	Indicates a service or option is not available. Used only when no other cause in this class applies.
65	Bearer capability not implemented	Indicates the equipment sending this cause does not support the requested bearer capability.
66	Channel type not implemented	Indicates the called party has reached an unsupported channel type.

Termination Code	Description	Explanation
69	Requested facility not implemented	Indicates the network (or node) does not support the requested bearer capability and therefore cannot be accessed at this time.
70	Only restricted digital information bearer capability is available (national use)	Indicates the calling party has requested an unrestricted bearer service, however the equipment sending this cause only supports the restricted version of the requested bearer capability.
79	Service or option not implemented, unspecified	Indicates a service or option was not implemented. Used only when no other cause in this class applies.
81	Invalid call reference value	Indicates the equipment sending this cause has received a message with a call reference not currently in use on the user-network interface. This value applies only if the call reference values 1 or 2 octets long and is not the global call reference.
82	Identified channel does not exist	Indicates the equipment sending this cause has received a request to use a channel not active on the interface for a call.
83	A suspended call exists, but this call identity does not	Indicates a suspended call exists but the call's identity does not.
84	Call identity in use	Indicates a call identity is in use.
85	No call suspended.	Indicates no call is suspended.
86	Call having the requested call identity has been cleared	Indicates the call having the requested call identity has cleared.
87	User not member of CUG (Closed User Group)	Indicates the call was not completed, probably due to one of the following reasons: The dialed number is incorrect The user is not authorized to use (or has not subscribed to) the requested service User is using a service the remote device is not authorized to use
88	Incompatible destination	Indicates the equipment sending this cause has received a request to establish a call that has low layer compatibility, high layer compatibility, or other compatibility attributes (such as data rate or DN subaddress), which cannot be accommodated. This call can be returned by a switch to a CPE when trying to route a call to an incompatible facility, or one without a data rate.
90	Destination number missing and DC not subscribed Nonexistent CUG (Closed User Group)	Indicates the call was not completed, probably due to one of the following reasons: The dialed number is incorrect The user is not authorized to use (or has not subscribed to) the requested service User is using a service the remote device is not authorized to use

Termination Code	Description	Explanation
91	Invalid transit network selection (national use)	Indicates an invalid transit network selection has been requested.
95	Invalid message, unspecified	Indicates the entity sending this cause has received an invalid message. Used when no other cause in this class applies.
96	Mandatory information element is missing	Indicates the equipment sending this cause has received a message missing an information element that must be present in the message before the message can be processed.
97	Message type non-existent or not implemented	Indicates one of the following: The equipment sending this cause has received with a message type it does not recognize. Either the message is not defined, or it is defined and not implemented by the equipment sending this cause. A problem with the remote configuration or with the local D-channel.
98	Message is not compatible with the call state, or the message type is non-existent or not implemented	Indicates one of the following: Message received is not compatible with the call state Message type is non-existent or not implemented
99	An information element or parameter does not exist or is not implemented	Indicates the equipment sending this cause has received a message that includes information elements not recognized because either the information element identifier is not defined, or it is defined but not implemented by the equipment sending the cause. However, the information element is not required for the equipment sending the cause to process the message.
100	Invalid information element contents	Indicates the equipment sending this cause has received an information element it has implemented. However, one or more fields of the information elements are coded in such a way (such as truncated, invalid extension bit, invalid field values) that the information element has not been implemented by the equipment sending this cause.
101	The message is not compatible with the call state	Indicates one of the following: The equipment sending this cause has received a message the procedures indicate is not a permissible message to receive at this time. The switch sending this cause is clearing the call because a threshold has been exceeded for multiple protocol errors during an active call.
102	The call was terminated when a timer expired and a recovery routine was executed to recover from the error	Indicates a procedure has been initiated by the expiration of a timer in associated with error-handling procedures.

Termination Code	Description	Explanation
103	Parameter non-existent or not implemented - passed on (national use)	Indicates the equipment sending this cause has received a message that includes parameters not recognized because the parameters are defined but not implemented by the equipment sending the cause. The parameters were ignored. In addition, if the equipment sending this cause is an intermediate point, this cause indicates the parameters were passed on unchanged.
110	Message with unrecognized parameter discarded	Indicates the equipment sending this cause has discarded a received message that includes a parameter that is not recognized.
111	Protocol error, unspecified	Reports a protocol error event only when no other cause in this class applies.This cause may be displayed if the user failed to dial a 9 or an 8 for an outside line. In addition, this cause may be returned in the event of certain types of restrictions as to number of calls.
126	Call split	A Cisco-specific code. Indicates a call was terminated during a transfer operation because it was split off and terminated (not part of the final transferred call). This code can help determine which calls were terminated as part of a transfer operation.
127	Internetworking, unspecified	Indicates an internetworking call (usually a call to SW56 service) has ended. May also be seen in the event of a non-specific rejection by a long distance carrier.

B Statistics Used in Diagnoses

Statistics are presented as “stat objects” in the Raw Data file. They are owned by the device objects from which they were collected.

For each statistic, a series of parameters applies, including the device type from which it was collected, how many samples were used in deriving the values, and calculations, such as averages and standard deviations where applicable. For more information, see “Field Definitions for the Raw Data File” on page 51 and Section 5.2.1, “Interpreting the Results Table,” on page 88.

The names of many statistics are abbreviated in the Raw Data file. Their abbreviations are shown in the table below:

Abbreviation	Statistic	Definition
ACOM	ACombined	Equal to ERL (Echo Return Loss) + ERLE (Echo Return Loss Enhancement). ERLE is the amount of echo provided by an echo canceller.
Bandwidth	Bandwidth utilization	Bandwidth utilization as a percentage found during SNMP polling
Broadcasts	Broadcast packets	Broadcast packets expressed as a percentage of all packets processed on the device since it came online
ChannelUtil	Channel utilization	Percentage of bearer channels in use for a T1 or E1 circuit
CollRate	Collision rate	Percentage of all packets processed on the device since it came online
CPU1min CPU5min	CPU utilization 1 min; 5 min	CPU utilization measured during one-minute or five-minute polling interval
CPU5sec	CPU utilization 5 seconds	CPU utilization measured during five-second polling interval
Delay	Delay	End-to-end delay in a single direction between Target Devices
Discards	Discards	Number of packets discarded by the device since it came online
DroppedPacketsPct	Dropped packets percentage	Percentage of packets for this traffic class dropped as a result of all features that can cause drops, such as policy and random detect
ECNS	Congestion notification	Number of frame-relay frames that experienced congestion during SNMP polling
ERL	Echo return loss	Ratio of the power level of the transmitted voice signal to the power level of the echo signal generated by the VoIP gateway
Errors	Errors	Errors detected from the cyclical redundancy checks (CRSs) in the packets

Abbreviation	Statistic	Definition
Frames	Frames	Frame-relay frames sent and received during SNMP polling
InSignal	Signal in	Active input signal level (in decibels) from the telephony interface used by a call leg
JitterBufferLoss	Jitter buffer loss	Percentage of all datagrams lost due to jitter buffer overruns or underruns since the device came online
LossRate	Loss rate	Rate at which packets were lost, as a percentage of all packets sent and received since the device came online
LostData	Lost data	Number of datagrams lost between the Target Devices, expressed as a percentage of all data sent.
MediaRate	Media rate	Percentage of all packets that experienced media errors on the device since it came online
MemFast	Fast memory	Percentage of the memory pool being utilized
MemI/O	I/O memory	Percentage of the memory pool being utilized
MemProcessor	Processor memory	Percentage of the memory pool being utilized
MOS	Mean Opinion Score	Numerical representation of the quality of a VoIP transmission. A MOS of 5 is considered excellent. A MOS of 1 is unacceptably bad.
MultRate	Multiple collision ratio	Percentage of all packets processed that experienced multiple collisions since the device came online
NoBufPacketsPct	Dropped packets percentage	Percentage of packets for this traffic class dropped due to a lack of SRAM buffers during output processing on an interface
Octets	Octets	Bytes sent and received since the device came online
OutSignal	Signal out	Active output signal level (in decibels) from the telephony interface used by a call leg
Packets	Packets	Packets sent and received since the device came online
Ping	Ping test	Results from the Ping test used to collect statistics
PostUtil	Post-policy traffic class utilization	Bandwidth utilization for this traffic class after execution of any QoS policies by the device
PreUtil	Pre-policy traffic class utilization	Bandwidth utilization for this traffic class before execution of any QoS policies by the device
Protos	Unknown protocols	Number of packets discarded with unknown protocols, as a percentage of all packets sent and received since the device came online
QLen	Queue length	For an interface: the length of a router or switch queue, as a number of packets For a traffic class object: the queue depth for a particular traffic class
Reach	Traceroute	Traceroute test used to collect statistics
SignalErrors	Signal errors	Accumulated number of signaling protocol errors detected in the interface since the interface came online

C Supported Devices

Vivinet Diagnostics cannot monitor every conceivable router or switch on a given network. The following sections summarize the supported devices.

Devices from Cisco and Nortel

Vivinet Diagnostics supports the following Cisco and Nortel devices.

Vendor	Device
Switches	
Cisco	All known switches are supported
Nortel	◆ Baystack 460 Series and later ◆ 550 Series ◆ Passport Series 1600, 8100, 8300 **NOTE**: Vivinet Diagnostics cannot collect CPU utilization metrics from switches that run Baystack OS version 3.1 or from Passport 1600 switches.
Routers	
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 **Notes** ◆ BayRS version 14.x and 15.x. Other OS versions are also supported, but not all metrics can be collected. ◆ CPU and memory utilization metrics are gathered from Rapid City-based Passport routers. If SONMP is enabled, ingress and egress interface data is also collected.

Switches from Other Vendors

For the Layer 2 trace, Vivinet Diagnostics does not automatically discover the routers and switches of vendors other than Cisco and Nortel. However, the devices of other vendors can be discovered if you manually configure the device addresses in Vivinet Diagnostics and if the devices support SNMP traceroute standards. For more information, see Section 4.4, "Understanding Layer 2 Trace," on page 65 and Section 4.4.2, "Device Configuration," on page 68.

However, even after device configuration, Vivinet Diagnostics can only determine VLAN (virtual LAN) information for Cisco and Nortel switches.

Routers from Other Vendors

Vivinet Diagnostics provides partial support for routers from vendors other than Cisco and Nortel:

- All routers in the Layer 3 trace are discovered using standard traceroute methods
- Device and interface details are retrieved from standard System, Interfaces, and `dot3StatsTable` MIB tables
- CPU utilization statistics are collected from Alcatel and Xylan routers
- Memory utilization statistics are gathered from Alcatel and Xylan routers

Devices Running LLDP

NetIQ Corporation has tested Vivinet Diagnostics on the following Nortel LLDP (Link Layer Discovery Protocol) implementations. For more information, see Section 1.6, "Link Layer Discovery Protocol," on page 13.

- ERS83xx (version 3.0 and later)
- ES325 (version 3.6)
- ES325 (version 3.6)

Devices Running VRRP

NetIQ has tested Vivinet Diagnostics on the following VRRP (Virtual Router Redundancy Protocol) implementations. For more information, see Section 3.5.8, "Configuring VRRP IP Addresses," on page 42.

- Nortel ERS86xx
- Wellfleet Series 7 routers (tested on OS Versions 14.20 and 15.4.2.0)