Nortel Unified Communications Campus Solution

Troubleshooting

Release: 1.0
Document Revision: 01.01

www.nortel.com

NN49000-700

Nortel Unified Communications Campus Solution
Release: 1.0
Publication: NN49000-700
Document release date: 29 May 2009

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

All other trademarks are the property of their respective owners.

Contents

New in this release

This is the first issue of this document, Nortel Unified Communications Campus Troubleshooting (NN49000-700) . Because this is the first issue, all features described in this document are new.

Introduction

Nortel professional services

Nortel Global Services offers solutions that combine comprehensive network expertise, world class partners and global reach. For the UC Campus Solution, Nortel Global Services provides a complete range of services for the products described in the rest of this document. For further details on services to complement the design, deployment and support of a UC Campus Solution, please refer to Nortel Unified Communications Campus Solution Fundamentals, NN49000-100.

Navigation

- "Solution-level Troubleshooting" (page 11)
- "Tools and Procedures" (page 21)
- "Information resources by service" (page 71)

Solution-level Troubleshooting

The UC Campus Solution concurrently supports many end user services. When operational problems occasionally occur within a deployed UC Campus network, they may present marginal, intermittent, or solid indications of the problem source.

This chapter describes a troubleshooting workflow, key information to gather and analyze against symptoms, followed by repair or remediation of services to a known baseline. The following topics describe the workflow or phases of solution-level troubleshooting described herein.

Planning for the troubleshooting process

There are some things you can do to minimize the need for troubleshooting and to plan for doing it as effectively as possible.

- Familiarize yourself with the UC Campus Solution documentation suite so you know where to get information when you need it. To access solution-level documentation, go to Nortel Technical Support Portal, at: http://support.nortel.com and navigate to Unified Communications Campus by choosing the successive pages: Solutions > Unified Communications Campus.
- Complete the associated Support Specialist certifications for UC Campus. For information, go to on this and other UC training go to Technical Support at: http://support.nortel.com and navigate to Unified Communications Campus by choosing the successive pages: Solutions > Unified Communications Campus. Alternatively, after you get to the Certification site (http://app97.nortelnetworks.com/cgi-bin/teds/cs/maintc.jsp?level=0&category=12&subcategory=), you can select "All Certifications" in the left margin to get the list that includes UC training and certification.
- Make sure the Solution is properly installed and maintained so that it operates as expected.
- Keep the acceptance testing results in an accessible location if allowed within site security mandates. These results provide a performance baseline against which you can compare current performance of UC Campus services.
- If allowed within site security mandates, have access to the current site topology map, logical connections, device configuration information, and other data that you may require if you have to troubleshoot.
  - Know how your devices are connected logically and physically with virtual local area networks (VLANs).
  - If allowed within site security mandates, maintain online and paper copies of your device configuration information. Ensure that all online data is stored with your site's regular data backup for your site. If your site has no backup system, copy the information onto a backup medium and store the backup offsite.
  - Store passwords in a safe place. It is a good practice to keep records of your previous passwords in case you must restore a device to a previous software version. You need to use the old password that was valid for that version.
  - Maintain a device inventory, which list all devices and relevant information for your network. If you have administrative access to the UC Campus devices, you could use a show config command

via the CLI or management GUI. Use this inventory to easily see the device types, attached devices, and if allowed within site security mandates, see IP addresses, port numbers, MAC addresses, VLAN IDs, and so on.

— Keep a list of the MAC addresses that correlate to the ports on your hubs and switches.

— Maintain a change-control system for all critical systems. Permanently store change-control records in a secure location.

— Store the details of all key contacts, such as support contacts, support numbers, engineer details, and telephone and fax numbers. Having this information available during troubleshooting saves you time.

- Understand the normal network behavior so you can be more effective at troubleshooting problems.

  — Monitor or generate service- and device-specific reports over a period of time sufficient to allow you to obtain statistics and data to see patterns in the traffic flow, such as which devices are typically accessed or when peak usage times occur.

  — Note the frequency, duration, and time during which any access or performance problems occur.

  — Use a baseline analysis as an important indicator of overall network health. A baseline view of network traffic as it typically is during normal operation is a reference that you can compare to network traffic data that you capture during troubleshooting.

Capturing symptoms

An effective troubleshooting methodology focuses first on key or critical health indicators associated with each UC Campus service and its supporting components:

- User complaints: User complaints are typically support calls or cases raised at the customer site, Nortel partner site, or at Nortel to report problems with a specific service or set of services. Upon receiving the call or case, support personnel collect and analyze available information to solve the problem.

  In addition to the information gathered when the problem occurred, the history of cases logged for a specific customer site may be useful. For cases escalated to Nortel, this kind of information may be found at kanisa Support Center: http://qtcfh0mb.ca.nortel.com:8080/KanisaSupportCenter/

- Alarms: To indicate a problem, a component raises an alarm, then reports or sends that alarm to a management workstation.
- Alerts: To notify of a significant event, components send alerts to a management workstation.
- Traps: To notify of a significant event, components send SNMP traps to a management workstation.
- Logs: Management workstations retrieve and analyze log files, which contain a time-stamped record of both normal and abnormal events, which in turn may be helpful information for problem identification.
- Syslog event messages: To notify of a significant event, components send Syslog messages to a management workstation.
- Statistics: Statistics captured using CLI show commands, management worstations (for example, statistical reports and graphs), or component MIB tables, upon analysis, provide information on the overall health of a component or system. If there is a problem, the analysis can also indicate trends or discrepancies that help with diagnosing and fixing the problem.
- Diagnostics: A variety of Solution-specific and industry-standard tools and utilities run diagnostics to help discover additional clues about the relative health of the Solution, its services, and components.
- Reports: Reports provide real-time snapshots and time-interval views of a Solution, service, or component. This provides information about Solution, service, or component status, behaviors, and performance.

Obtaining key reference information

After capturing information about the symptoms of a problem, you can attempt to collect as much reference information as possible about the normal and abnormal conditions and diagnosis of the problem. For example:

Site-specific design plans

Site-specific design plans provide an overview of how UC Campus is put together, as well as the relationship of individual components. You can request site-specific plans from the network administrator.

Solution customer acceptance test data

After the initial setup or modification, a solution is tested to be sure that performance falls within an acceptable range. The results of this testing provides a baseline against which you can compare and determine the current Solution health. You can request this information from the network administrator.

Customer support case histories

Customer support case histories provide a view from which a possible cause or pattern may become apparent. For example, use the Nortel kanisa Support Center to view histories at: http:qtcfh0mb.ca.nortel.com:8080KanisaSupportCenter. The Solution customer may also have their own support database to track technical problems and outcomes.

Recovery Trees

Recovery Trees (RT) provide a quick reference for troubleshooting without procedural detail. Starting with the initial event, they provide a flow meant to guide you through symptoms to identify the problem and provide a solution.

Nortel Business Partners can go to http://navigate.us.nortel.com/imds?pg=/ss/cs/30msr/process/recovery, click Recovery Tree Repository, and then scan the list of RT folders and open the one that applies to the service or component they are trying to troubleshoot.

You can also find Recovery Trees for Solution components on the Nortel Technical Support Portal (http://support.nortel.com). For this approach, you must:

- Log on to the Portal with your Nortel-registered username and password.
- Enter "recovery tree" in the search field in the upper-right area of the Portal Welcome <username> page.
- Press the Enter key.

This procedure triggers a search for all Recovery Trees. You can serially browse the list of Recovery Trees on each numbered search page, or you can attempt to narrow your results through more advanced search techniques.

Message flow diagrams

Message flows are diagrams associated with setup and teardown of the many different call scenarios supported by the UC Campus Solution are helpful for troubleshooting from a normal-operation baseline, knowing which components should send and receive specific messages at each stage of call progress. These diagrams are available on request through Nortel Global Services.

Service and component experts

Nortel Global Services offer Network Support Services Solutions that combine comprehensive network expertise, world class partners and global reach. For information on Network Support Services Solution, see the Global Services web page at: http://products.nortel.com/go/service_index.jsp For more information on Global Services, see “Nortel professional services” (page 9).

Solution-level and product-level customer documentation and training

Nortel provides Solution- and component-level documentation, technical bulletins, training and some certification paths for UC Campus and its components. (See “Information resources by service” (page 71).)

To access additional resources of this kind, go to Nortel Technical Support Portal, at: http://support.nortel.com.

Analyzing symptoms

Analyze symptoms to determine the scope and identity of the problem. This can be done using the following resources:

- Recovery Trees (RT) provide a quick reference for troubleshooting without procedural detail. For more information, see “Recovery Trees” (page 15).
- If available, Use Cases provide the symptoms of common problems and what to do about them.

  Use cases can also indicate what is normal operation -- a comparison baseline for a very specific call scenario or similar operation.

  “Message flow diagrams” (page 16) often depict normal use-case scenarios that are useful for troubleshooting
- For extended/escalated symptom analysis and support for a deployed UC Campus network, contact Nortel Network Support Services at: http://products.nortel.com/go/service_index.jsp and click on NETWORK SUPPORT SERVICES.

Identifying out-of-bounds services and components

The troubleshooting methodology should include a Solution-level prioritized approach to fault identification, isolation, and resolution, down to the component level. This chapter describes what considerations determine the character and priority of a problem.

Character and severity of the problem

The character and severity of the problem depends on the area in which it exists. For example, the problem may exist in any of these areas:

- Authentication and access services
- Voice services and applications
- Unified messaging services and applications
- Ethernet Infrastructure services

Location and span of effects on Solution users

The severity of the problem is measured in part by the span of effects on Solution users. For instance, does the problem impact:

- All solution users
- A specific group of users
- A single user

For example, a user authentication and access problem might affect all, some, or only one of the Solution users. However, it is also true that a single user experiencing a problem with Solution services could indirectly affect all Solution users, or an important group of Solution users.

Identifying and isolating the fault, and what to do next

Once you have analyzed all symptoms and relevant reference information, and you have identified the root cause of a problem with a UC Campus service, you must then determine the appropriate action(s) to resolve the problem. This may vary from simple remediation procedures to replacement of hardware, restoral of an earlier backed-up database, or component upgrades.

Remediating or repairing service-component operations

The remediation or repair effort required for problems with Solution operations varies. For example, the resolving action to boost performance levels, QoS, or QoE within a specific service may require completion of a simple reconfiguration task. A more severe problem could involve module or whole component replacements, re-installation and commissioning, or configuration of additional components to upwardly scale Solution capabilities and performance levels.

In general, the levels of redundancy and resiliency designed into the UC Campus Solution enable you to perform remediation or repairs during scheduled or unscheduled maintenance intervals.

Nortel has established the Nortel 30MSR, a company-wide program launched to improve our customers' experience by seeking to eliminate long duration outages.

Nortel 30MSR

The goal of this initiative is to preempt or eliminate any outage condition lasting longer than 30 minutes, from outage start to service fully restored. 30MSR has been integrated across all business units and Nortel functions - from the development cycle through everyday interactions with customers. The 30MSR web portal (http://navigate.us.nortel.com/imds?pg=/ss/cs/30msr) is an information resource for communities across all Nortel product and business teams.

Verifying services restored to a known baseline

The same service-specific tests performed during Solution customer acceptance can be performed again to verify service restoration to a known baseline. To this end, you can use the original UC Campus Customer Acceptance Test documentation (if available) to match the problem you resolved to an applicable test in the Acceptance document. See your network administrator for this information.

Depending on the nature and business impacts of the problem you resolved, additional testing and sustained monitoring may be warranted for customer confidence and satisfaction.

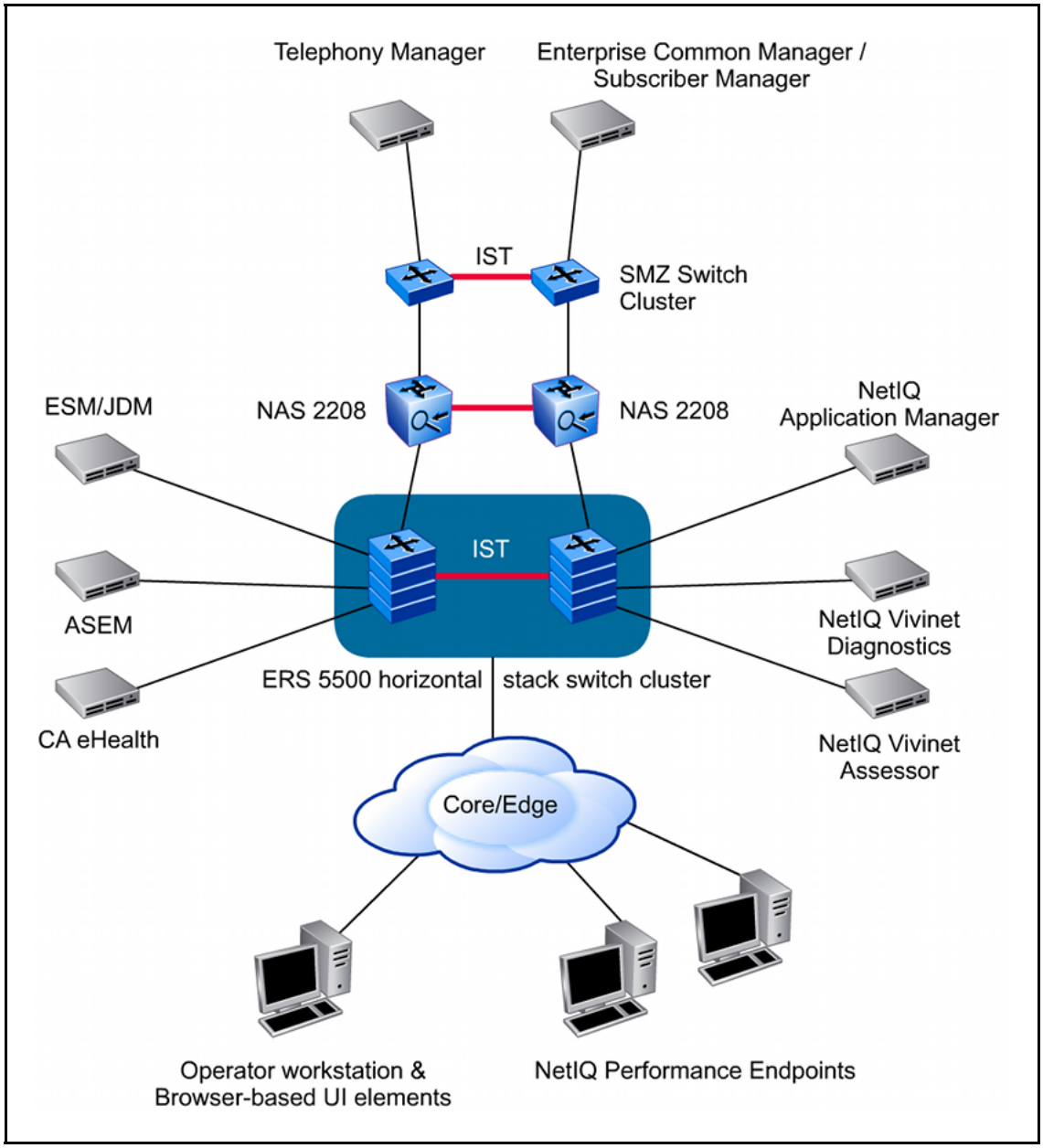
Tools and Procedures

The UC Campus Solution consists of many components from Nortel, Microsoft, and other third parties. This solution integrates your desktop applications with telephony, presence, and other multimedia applications. To maintain the reliability of your voice, data, and unified communications network, Nortel supports the following troubleshooting tools:

- CA eHealth—This tool constantly monitors your network for variances that exceed user-defined thresholds and may indicate a troubleshooting issue.
- PVQM—This tool quickly identifies the faulty device and where it is in the network.

After identifying a faulty device, UC Campus supports a comprehensive set of network management tools that you can use to troubleshoot the configuration of each element in the network. Each Element Manager provides real time performance and event monitoring. They also enable you to check configurations and, if necessary, modify them to correct a performance problem. The following figure shows the troubleshooting tools in the UC Campus Solution.

Figure 1
Troubleshooting tools

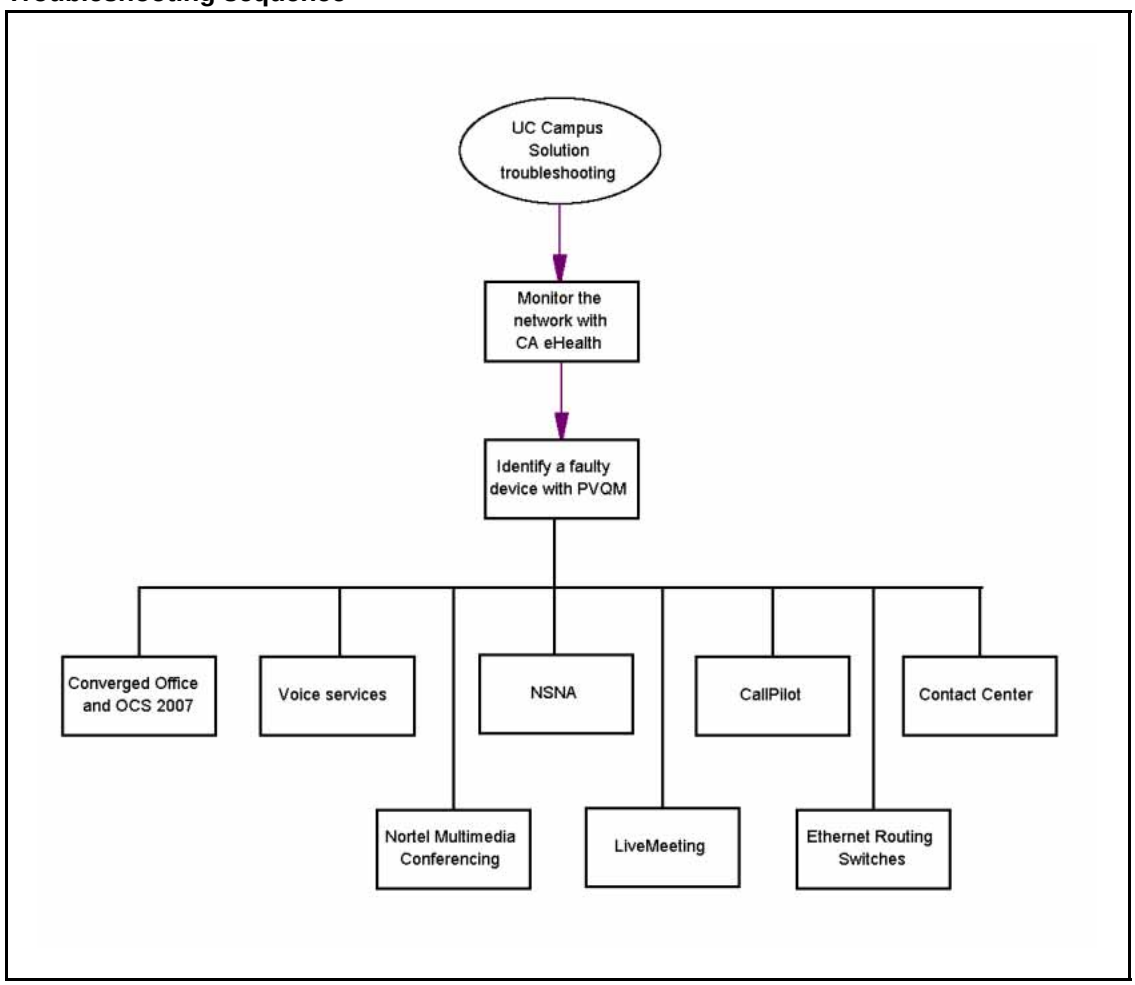


This chapter describes the troubleshooting tools, explains their function, and indicates what sequence to use them. It also describes solution-level troubleshooting tasks. It is not the intention of this chapter to repeat the step-by-step troubleshooting procedures already documented in component-level documents. However, most sections provide the names and part numbers of relevant documentation.

Troubleshooting tasks

This task flow shows the sequence of when to use the troubleshooting tools. To link to any procedure, go to “Navigation” (page 23).

Figure 2
Troubleshooting sequence



Navigation

Monitor the network with CA eHealth

CA eHealth is an optional component in UC Campus. Although it is not required, Nortel recommends CA eHealth because it serves as an early warning system for potential problems in the network. After you get your UC Campus Solution up and running, CA eHealth uses historical data to establish a baseline performance metric bound by an upper and lower threshold. Then CA eHealth polls the network every five minutes and provides reports that illustrate network trends and threshold exceptions.

CA eHealth helps you to manage the end-to-end performance and availability of your UC Campus infrastructure. It keeps track of every component in the network and monitors the performance of the network. You can use eHealth to determine if the current network bandwidth is sufficient and whether network traffic is increasing over time. This enables you to detect issues before they become problems.

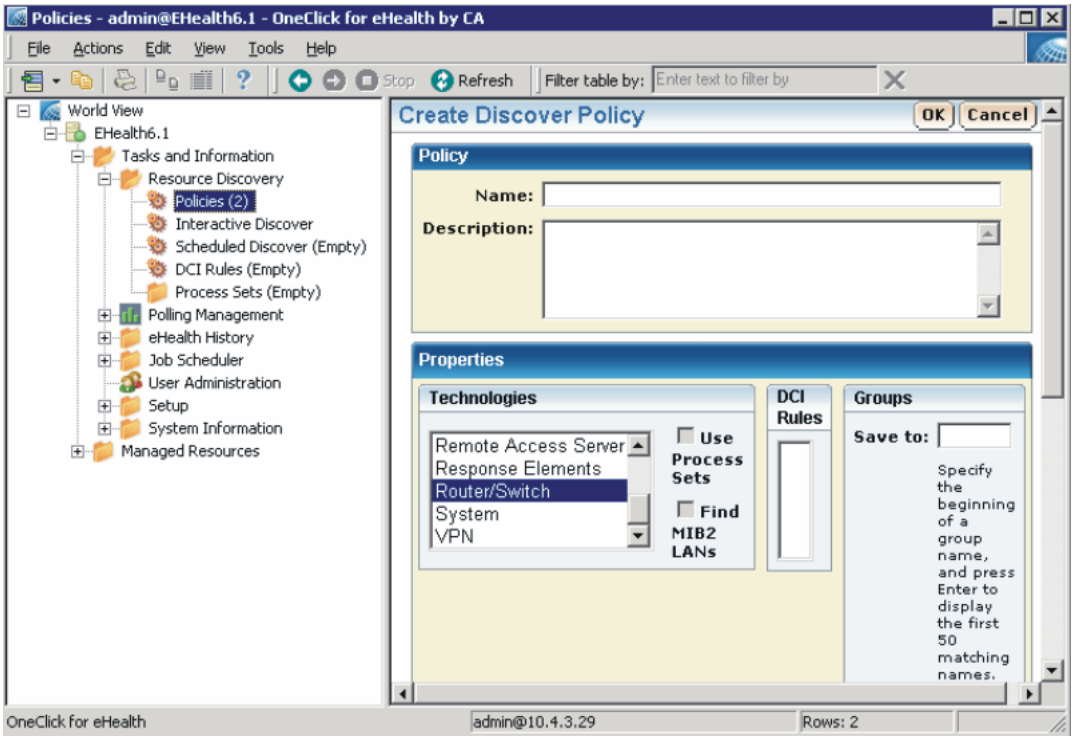
For online technical assistance and a complete set of eHealth documentation, contact Technical Support at www.ca.com/support.

eHealth policies

CA eHealth uses two policies to create reports: Router/Switch policy and LAN/WAN policy. The Router/Switch policy provides reports on the switch chassis and their network interfaces. The LAN/WAN policy provides reports on all the Ethernet interfaces.

To create the two policies, open OneClick for ehealth and logon as the eHealth admin and use the default password, **`ehealth`**. Under Tasks and Information, click **Resource Discovery, Policies**. The following figure shows the eHealth Discover dialog box.

Figure 3
eHealth Discover Policy



eHealth report types

eHealth collects data from your network infrastructure and generates the following types of reports:

- At-a-Glance
- Health
- Service Level
- Top N
- Trend
- What-if

At-a-Glance report

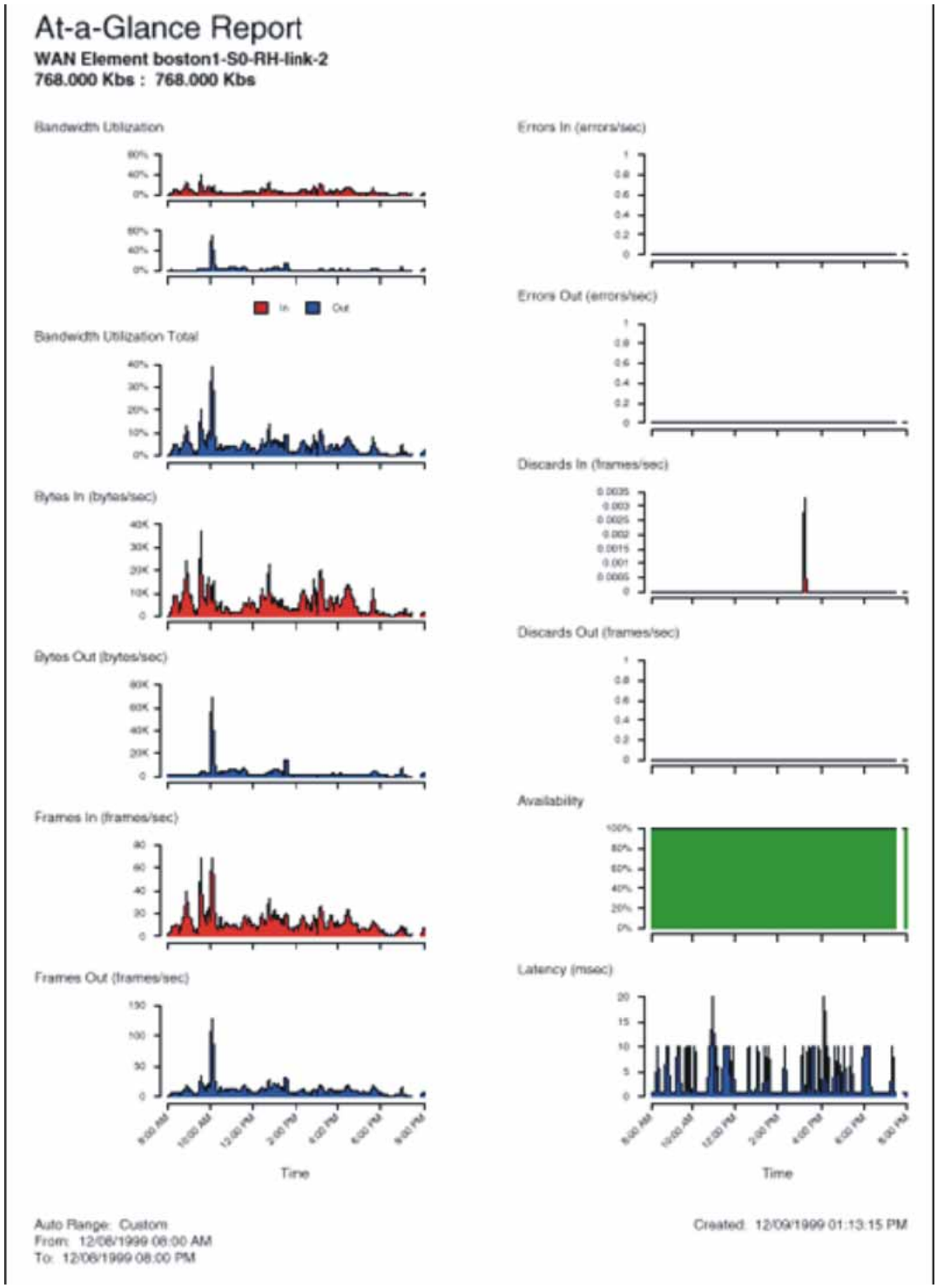
At-a-Glance reports consist of a series of charts that show the performance of critical variables. You can use the reports to show the following trends:

- CPU utilization
- Buffer management

- Traffic activity by protocol
- Total throughput

You can run At-a-Glance reports for a specific element to obtain immediate, detailed information on the critical performance parameters. The charts that appear in an At-a-Glance report vary depending on the element type that the report represents. The following figure shows an example of an At-a-Glance report.

Figure 4
At-a-Glance report



Health report

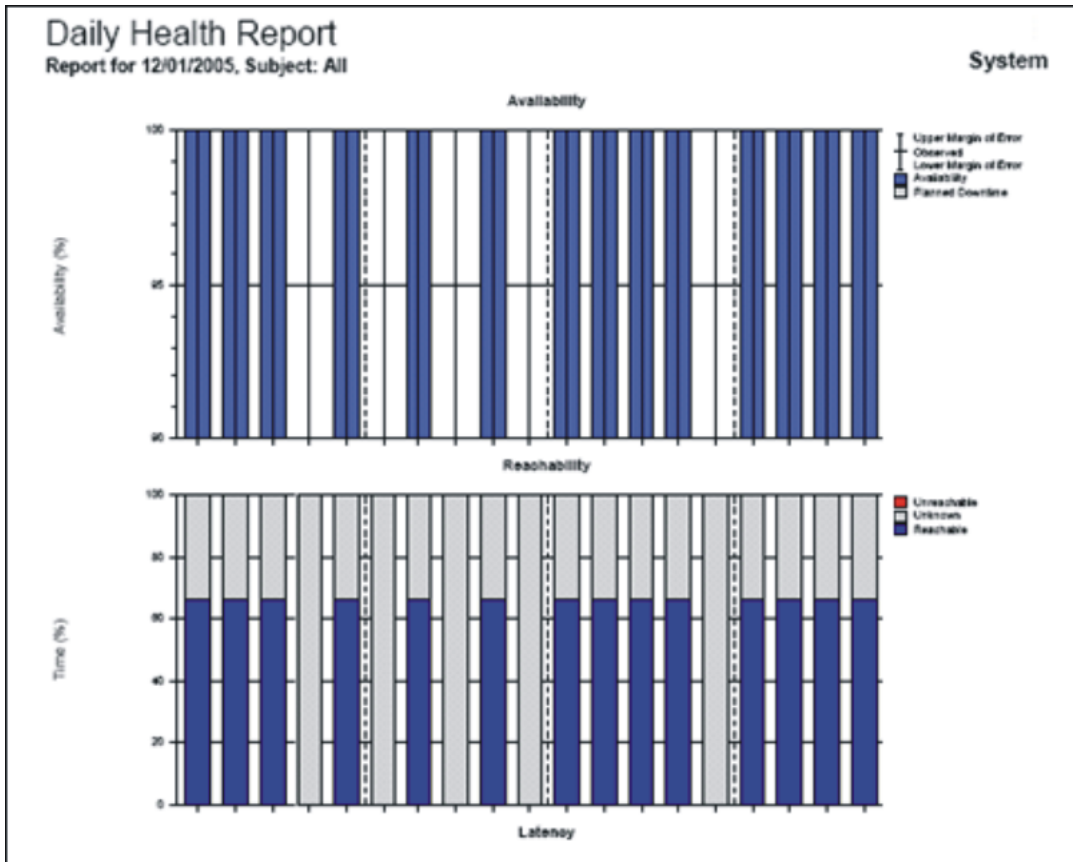
Health reports evaluate the health of a group of elements by comparing current performance to historical performance. CA eHealth polls the elements and then stores the information as historical data. Using the historical data from the baseline period, it constructs a trend line that it uses to predict the value for each variable over the course of a day, week, or month.

The baseline period is one of three rolling periods that projects backward in time from the day the report is run:

- For a daily Health report, the baseline is 6 weeks (42 days) by default.
- For a weekly Health report, the baseline is 13 weeks by default.
- For a monthly Health report, the baseline is 12 months by default.

The following figure shows an example of a Health report.

Figure 5
Health report



Service Level report

Service Level reports summarize the performance of the resources in an enterprise, department, or business unit based on analysis ranges and thresholds defined in a service profile.

The following table describes the types of Service Level reports that are available. Each type of report can provide details about individual technologies. For example, you can run a LAN/WAN Executive report or a Response Service Customer report. These reports provide the most value when you run them for a month.

Table 1
Service Level reports

Type of Service Level Report	Description
Business Unit	Summarizes the service level for the network resources that belong to a department or organization.
Executive	Determines how workloads, availability, and latency vary with time across the enterprise.
IT Manager	Summarizes service levels by specific groups in a group list and provides details on elements.
Service Customer	Provides information about the service level performance of the elements in a group and determines quality of service.
Response	Determines the relative performance of an application for a location or functional group.
VoIP	Monitors the quality of voice services across groups within the enterprise.

Top N report

Top N reports list the top elements in a group that exceed or fall below the performance values that you specify. You can use these reports to troubleshoot the infrastructure and identify elements that may be potential problems.

When you run a Top N report, you can specify up to six variables on which to report and then use the reports to compare the performance of specified elements. For example, the following figure compares elements that have a CPU utilization above a certain percentage.

Figure 6
Top N report

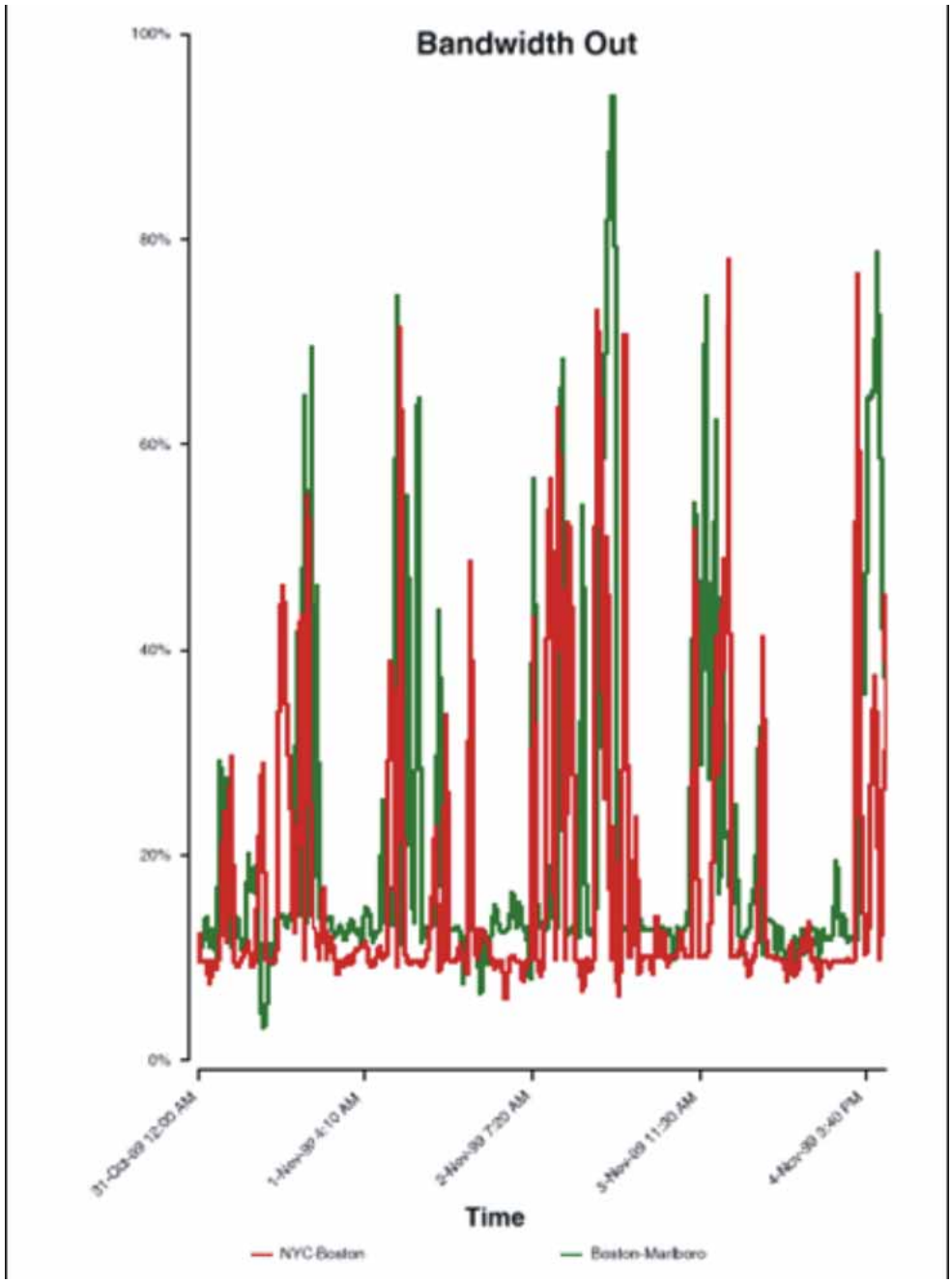
	CPU Utilization	
Element	**Above 80**	**Goal 50**
Colorado-SH-Cpu	98.69	48.69
NewYork-SH-Cpu	94.34	44.34
Detroit-SH-Cpu-1	87.57	37.57
Boston-SH-Cpu-1	87.40	37.40
Atlanta-SH-Cpu	84.90	34.90
Houston-SH-Cpu-1	82.18	32.18
SanDiego-SH-Cpu-1	80.24	30.24

Trend report

Trend reports show the performance of an element or a group of elements over a specified period of time. You can use Trend reports to observe traffic patterns over time, relationships among elements (or groups), and relationships among variables. The relationship between two variables may indicate a cause and effect. For example, if the Trend report shows a strong correlation between bandwidth utilization and collision rate, then the high bandwidth utilization on that Ethernet segment is probably causing the high rate of collisions.

The following figure shows an example of a Trend report run on one variable (bandwidth utilization) for two WAN elements. The color-code enables you to compare the performance of the two elements throughout the report period.

Figure 7
Trend report

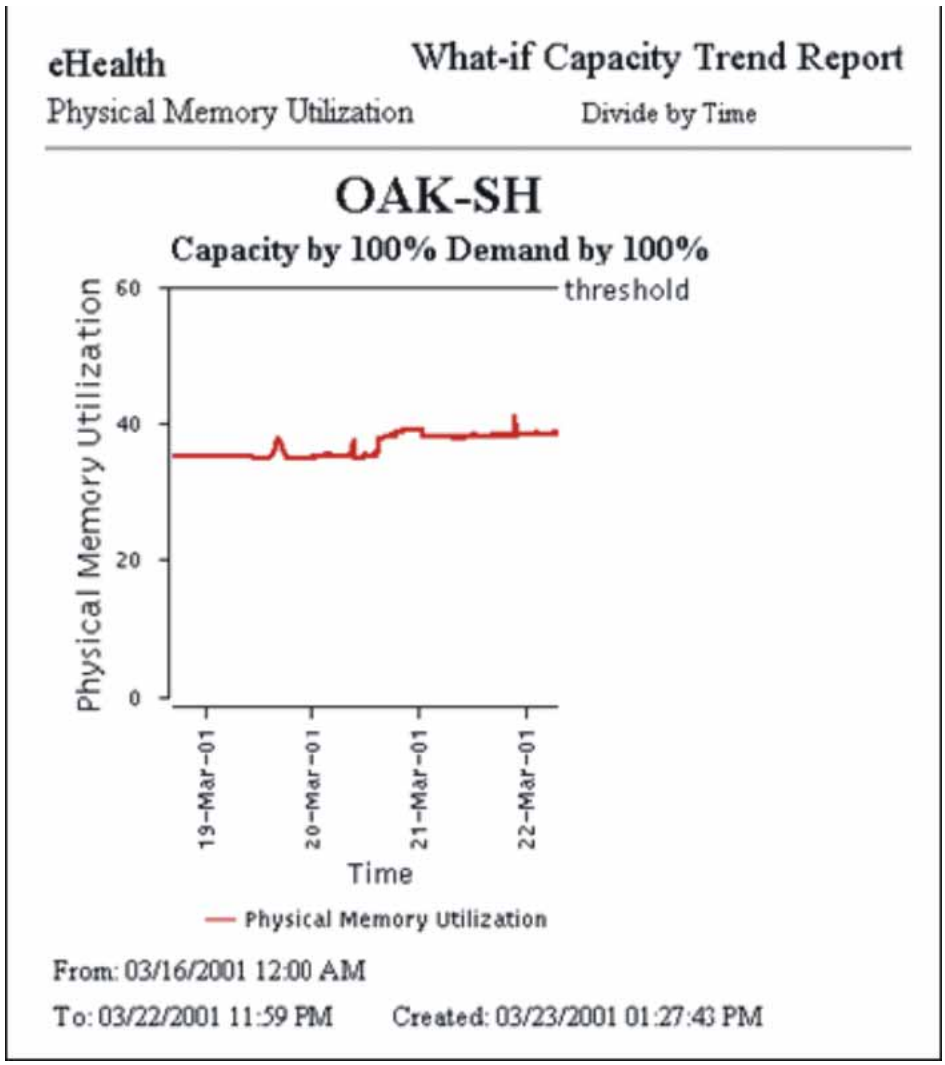


What-if report

What-if reports model changes in capacity and demand. This enables you to evaluate the current trends in resource usage and plan for growth and changes before problems occur. For example, you can change the amount of traffic, volume, or usage that a resource supports to observe what happens if you increase or decrease the usage for the resource.

You can use What-if reports to visualize different scenarios and devise potential solutions. The following figure shows an example of a What-if report. The red line represents a user-defined goal that you can use to measure changes in data with respect to a specific threshold.

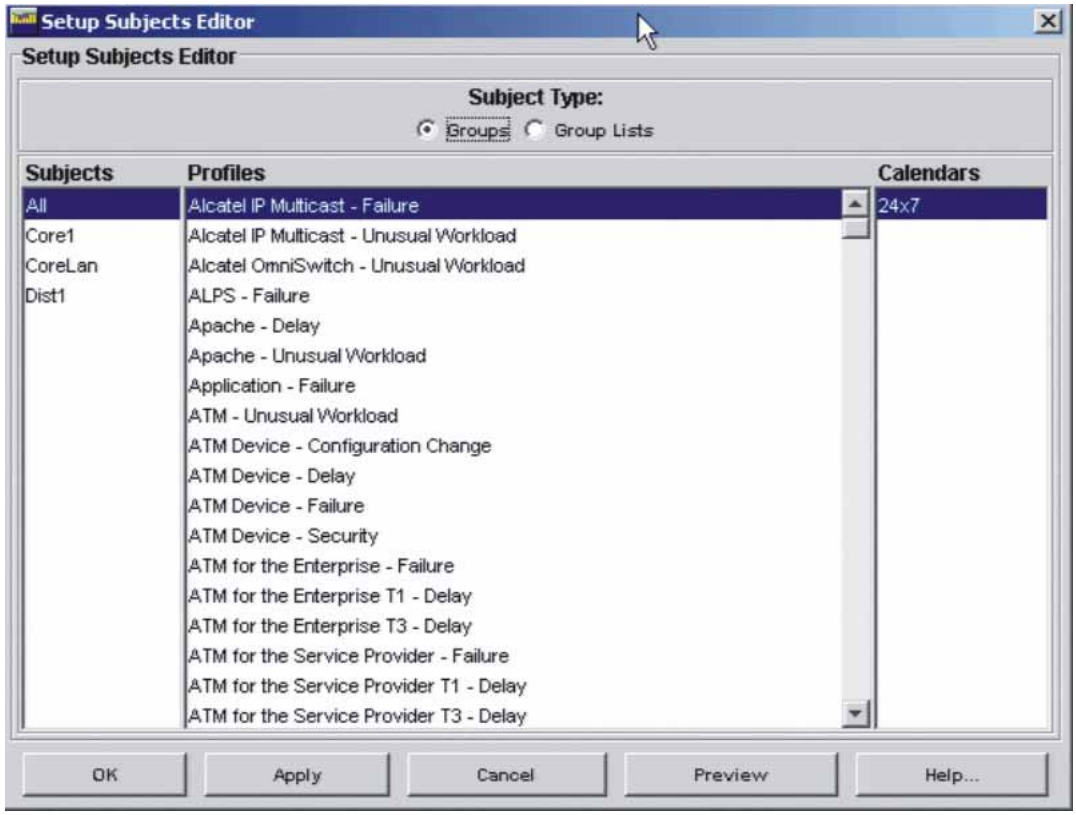
Figure 8
What-if report



eHealth Alerts

CA eHealth uses Live Exceptions to generate Alerts when the threshold value increases above the limit configured in a selected profile. To configure Live Exception Alerts, click on **Setup, Subject to monitor, new**. Then select the subject to monitor and a profile. Use the default profiles or create a new profile, if required. The following figure shows a sample dialog box with the available subjects and profiles.

Figure 9
eHealth Live Exception Alerts



Identify a faulty device with PVQM

Proactive Voice Quality Management (PVQM) is a network management and troubleshooting tool that Nortel codeveloped with NetIQ. PVQM ensures the overall quality of UC Campus voice services by continuously and passively measuring the user quality of experience (QoE) for all IP Telephony communications. If PVQM detects any performance degradation or fault condition, it immediately notifies you of the problem and provides troubleshooting information while a call is ongoing, without end-user involvement or awareness.

Voice problems are immediately apparent to end users so they must be resolved as quickly as possible. PVQM isolates the problem to a specific device wherever it occurs in the network. This includes detecting Layer 2 and Layer 3 switch failures, card failures, memory utilization, CPU utilization, power supply status, temperature status, fan status, QoS parameters, and IP phone port status.

The following are key components of PVQM:

- Application Manager—This tool monitors end-to-end call quality, provides call quality metrics for Nortel Call Servers with information about the availability and health of network devices, and reports on overall network performance for voice traffic. AppManager also highlights the underlying conditions that caused the service quality degradation. This allows operators to map VoIP service quality back to the underlying network infrastructure.
- Vivinet Diagnostics—This tool automatically troubleshoots the network to pinpoint VoIP call quality problems and explains why you are experiencing reduced call quality. Vivinet Diagnostics reduces the time you need to resolve voice quality issues and lessens the skills required for VoIP troubleshooting. Vivinet Diagnostics is automatically invoked when a real-time R-value (Quality of Experience) trap is received from a Communication Server 1000 or you can manually invoke it using synthetic VoIP Quality Endpoint clients.

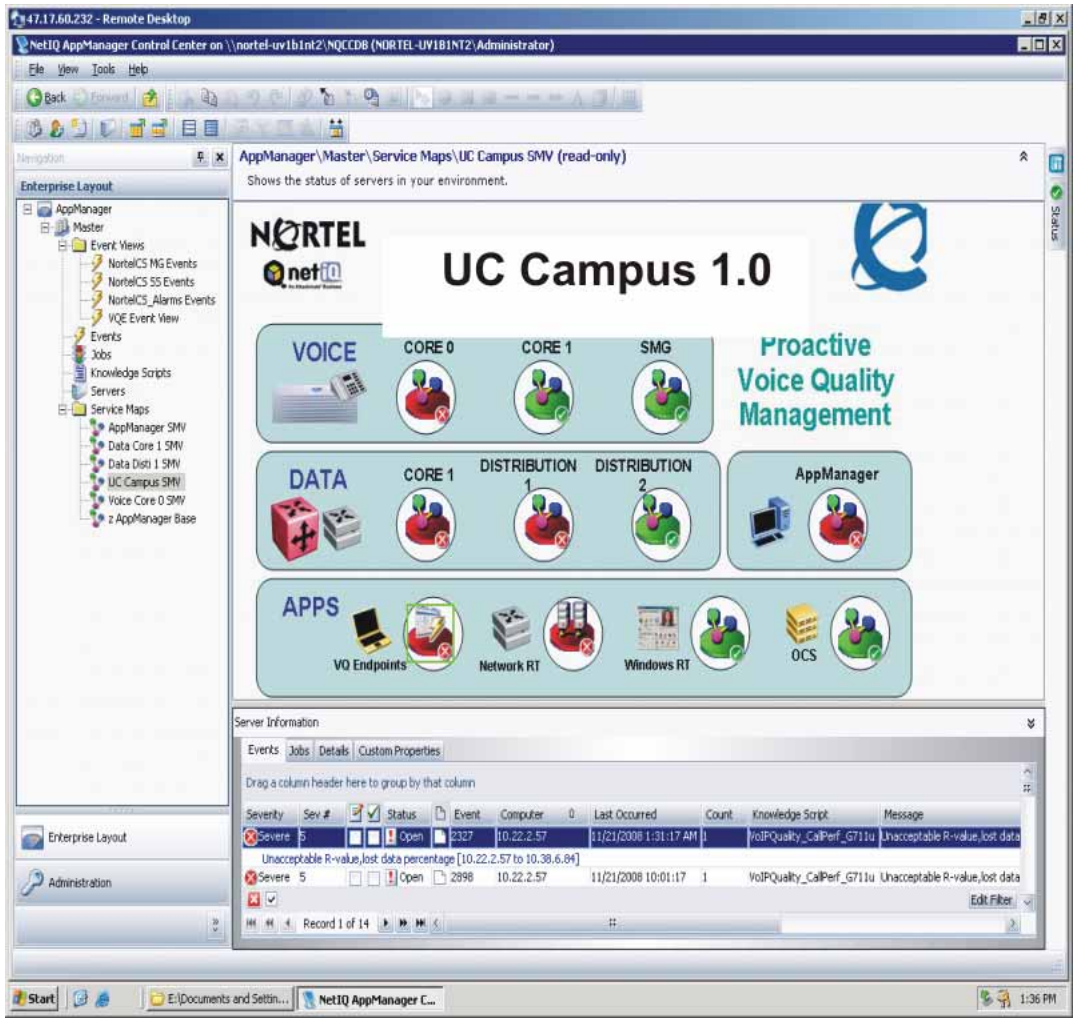
For technical assistance and support for NetIQ applications, see www.netiq.com/support/.

Views of the UC Campus network

PVQM uses graphics to provide different views of the network so you can visualize where the faulty device is in the network. You can also use these views to develop and measure different simulated flows using NetIQ Vivinet Assessor and the Performance Endpoints tools.

The following figure shows a top-level view of UC Campus.

Figure 10
Top-level view of the UC Campus network

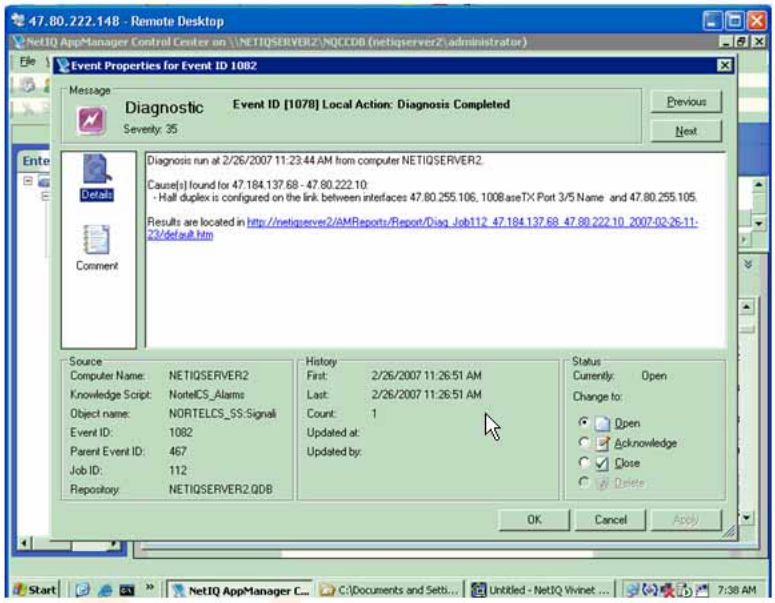


Using NetIQ AppManager

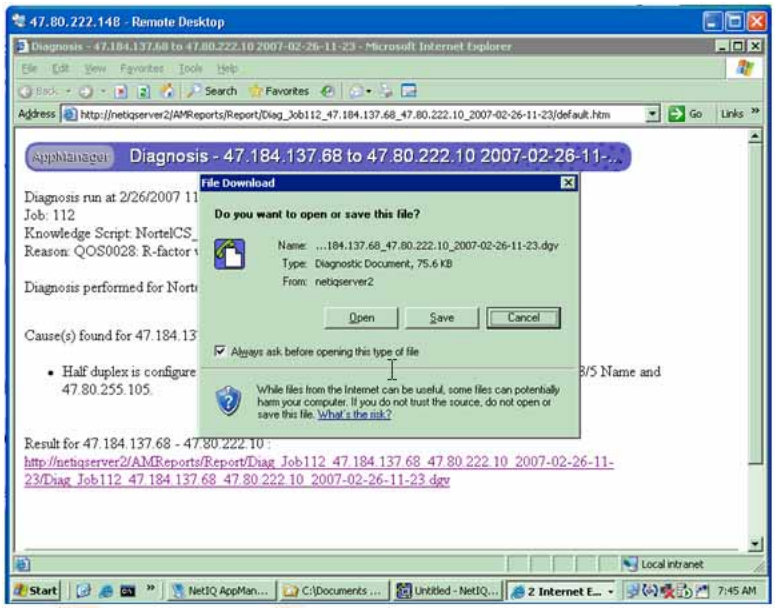
Perform this procedure to configure NetIQ AppManager to automatically monitor end-to-end user quality of experience (QoE) and report the underlying conditions for any service quality degradation. AppManager also provides a historical list of forensics that identify circumstances that interfere with VoIP quality. This constant monitoring and reporting enables you to detect and gather statistics on transient problems that sometimes affect networks.

Procedure steps

Step	Action
1	Log on to AppManager.
2	Click Server View.
3	Double-click the diagnostic that you want to see. The Event Properties window appears to show the Event ID and some of the potential causes found.



4	Click the URL in the Diagnostic message to see detailed diagnostic information. The Web page on the server appears where the link to the forensics is stored for accessibility.
5	To download the diagnostic file, click the URL on the bottom of the screen.
6	Click Save to save and retain all of the forensics in this single file for later use or reference, or click **Open** to open it directly without saving the file.



--End--

Using NetIQ Vivinet Diagnostics

Perform this procedure to configure NetIQ Diagnostics to automatically capture statistics and to see the path trace between the phones where there was a quality issue.

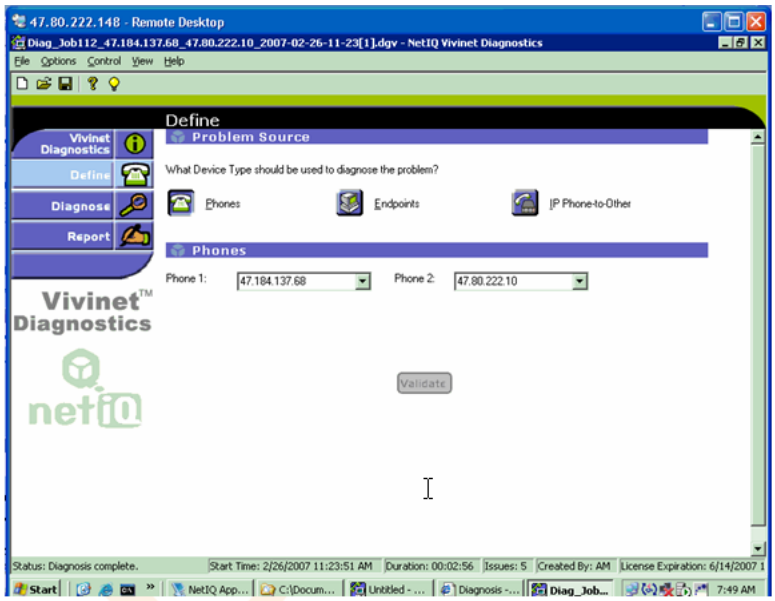
If there is a problem with a phone, you can click on the icon for that phone to see detailed statistics including the Terminal Number (TN) and Directory Number (DN). The DN shows exactly whose extension is having the problem, which saves time and effort. This information also tells you if the problem is with a critical phone that requires immediate corrective action.

NetIQ Diagnostics also provides detailed Real-Time Control Protocol (RTCP) statistics during the time when there was a problem with a phone. The statistics show the Local Listening R-Value for the phone, which indicates the toll quality satisfaction rating from an end user perspective.

Procedure steps

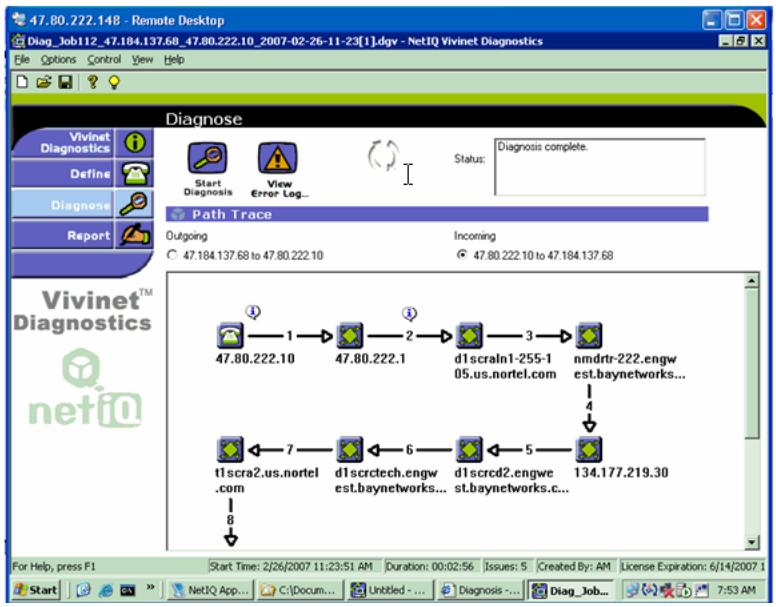
Step	Action
1	Log on to the Diagnostics Viewer, or launch it directly from AppManager.

2 Click **Define** to change the perspective of the diagnostics depending upon the Phone1/Phone2 (Source/Destination) perspective that you are interested in.

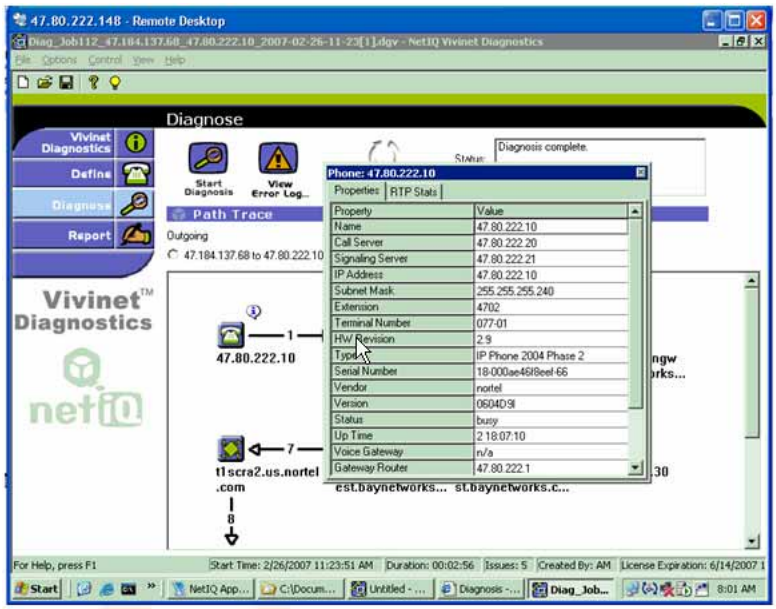


3 Click **Validate**.

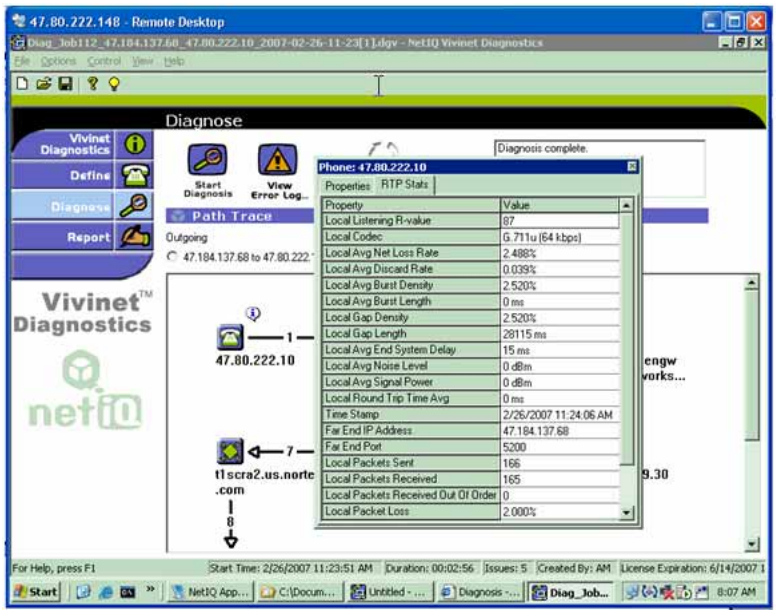
The path trace between the phones where there was a quality issue appears.



4 Click the icon of a phone to see detailed statistics about that phone including the Terminal Number (TN) and Directory Number (DN).

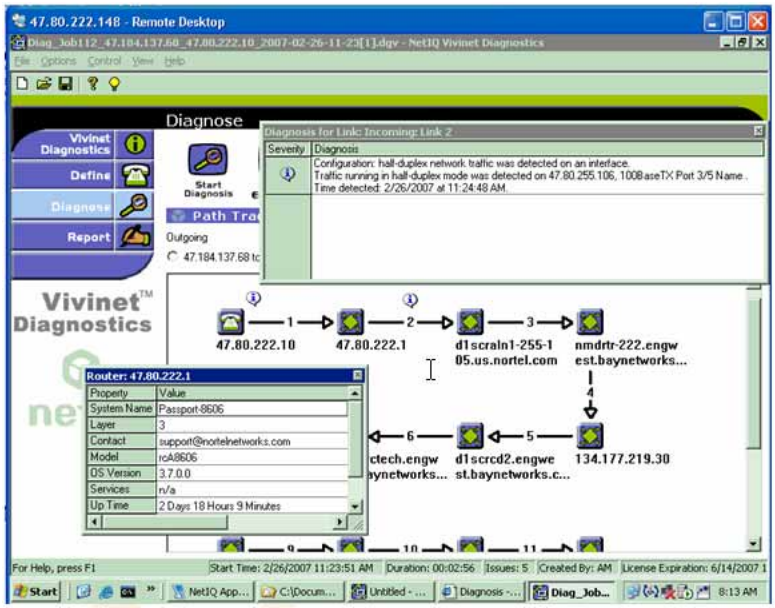


5 Click **RTP Stats** to see detailed RTCP statistics during the time when there was a problem.



6 Click on an information icon (i) above a hop to display diagnostics about that link. In the following figure, a Link Speed Duplex mismatch was detected on a 100MB Fast Ethernet port.

7 Click on the Router icon to see more details about the router itself. In the example shown in the following figure, it shows that it's an Ethernet Routing Switch 8600 running 3.7.0.0 code. It also shows the uptime of the router so you can see if perhaps the device rebooted recently, which affected voice traffic over that router.



--End--

Converged Office and OCS 2007 troubleshooting issues

If you experience a problem with Converged Office and OCS 2007 or if PVQM isolates a problem to them, you can use the tools and tips in this section to further troubleshoot the issue. If possible, try to determine if the problem is Communication Server 1000 related or OCS 2007 related and then refer to one of the following sections.

Converged Office troubleshooting issues

For Converged Office troubleshooting issues, check the following table to see if any of the symptoms describe the problem you are experiencing and try the possible solutions. To modify your Communication Server 1000, you can use the following tools:

- Telephony Manager (TM)—TM allows you to configure, control, and analyze your telephony network, either through a Windows GUI or a Web browser interface. You can also integrate TM with other Nortel management products to provide a complete management view of an entire converged network infrastructure.
- Enterprise Common Manager (ECM)—ECM provides a common interface for managing Communication Server 1000 elements, Telephony Manager WebUI, and Subscriber Manager. ECM provides framework-level security that simplifies security control for managed elements and system management applications. With this single unified framework, you only need to log on once to access all the network system management elements. This eliminates the need to reauthenticate when you launch each system management application.

ATTENTION
Improper configuration of Host Authorization and Certificates for Office Communications Servers and Pool are the primary reason Converged Office does not function properly in the Enterprise Edition configuration.

Table 2
Converged Office configuration issues

Symptom	Possible Causes	Possible Solutions
Signaling server does not boot	• Invalid CDROM or boot floppy are in drives • BIOS boot order is incorrect • Software has not been installed • Configuration is incorrect	• Remove CDROM or boot floppy from drives. • Reset BIOS defaults. • Re-install the software. • Verify Signaling Server's IP telephony configuration.

Symptom	Possible Causes	Possible Solutions
Cannot ping ELAN	• Signaling Server has not booted successfully • Data network configuration/routing problem	• Verify Signaling Server has booted successfully. • Verify Signaling Server data network configuration and connectivity.
Cannot ping TLAN	• Signaling Server has not booted successfully • Data network configuration or routing problem • Application configuration or routing problem	• Verify Signaling Server has booted successfully. • Verify Signaling Server data network configuration and connectivity. • Verify Signaling Server's IP telephony configuration.
Phones do not register	• Signaling Server unavailable • Incorrect IP telephony parameters (node ID and IP) • Incorrect system configuration	• Verify that Signaling Server has booted successfully. • Verify data network connectivity between telephones and Signaling Server. • Verify that Signaling Server is running TPS. • Verify IP telephony configuration of telephones. • Verify system TN configuration (LD 11).
Cannot make outgoing trunk calls	• Virtual trunk and/or GK configuration is corrupt	• Verify configuration in Element Manager. • Retransfer node files from Element Manager.
Cannot log in to CLI	• Incorrect login or password	• Try using the system PWD2. • Try using the default administrator login and password. • Reset the administrator login and password using the Install Tool.
Cannot access Element Manager web pages	• Signaling Server unavailable • Web server has not loaded • No route between Signaling Server and browser PC • Web server security flag is enabled and browser PC is not on ELAN	• Verify that Signaling Server has booted successfully. • Verify data network configuration and connectivity. • Verify browser PC and Signaling Server configuration. • Disable Web server security flag, or move browser PC to ELAN subnet.

Symptom	Possible Causes	Possible Solutions
Cannot log in to Element Manager	• Incorrect login or password or Call Server IP • Option Login Names is disabled • Call Server is unavailable • Login is already in use • Logins are blocked due to too many incorrect logins • Incorrect browser used	• Verify login, password, Call Server IP. • Enable login names (LD 17). • Verify Call Server is available. • Log out exist user, or wait for user to time out automatically. • Wait for logins to unblock automatically, or reboot the Call Server. • Disable browser caching (set to **reload pages every time**). • Use only Microsoft IE 5.5 or higher.
Unable to log on to the Signaling Server through Element Manager after SIP CTI services are activated. When rebootin g, some HTTP tasks are not up.	• Insufficient memory on the Signaling Server	• Check the memory and upgrade the memory to 1 GB, if required. The Signaling Server (running Converged Office) requires 1 GB of memory.
Telephony Gateway configuration issues	• Converged Office not functioning properly	• Check all CS 1000 resources (packages, licenses, and CS 1000 patches). • Check the DN, telephone TNA, and PCA configuration. • Check the DNS on the Signaling Server. • Verify the Signaling Server SIP and MCM endpoint registration on the NRS. • Ensure the MCM is registered to the NRS. • Verify the Host Authorization and Certificates for Office Communications Servers and Pool.

Symptom	Possible Causes	Possible Solutions
Remote Call Control configuration issues	• Remote Call Control not functioning properly	• Check all CS 1000 resources (packages, licenses, and CS 1000 patches). • Check the DN, telephone TNA, and PCA configuration. • Verify AST, IAPG, and CLS (CDMR/TR87A) are configured properly (SIP CTI only). • Verify ALM Link status is up. Ensure ELAN ID ≥ 32 (SIP CTI only). • Check the SIP CTI status (on the Signaling Server under PDT; command SIPCTIShow). Ensure SIP CTI status is Application status: Active (SIP CTI only). • Check the DNS on the Signaling Server. • Verify the Signaling Server SIP and MCM endpoint registration on the NRS. • Ensure MCM is registered to the NRS. • Verify the MCM configuration for the Called Phone Context. Check it against the Signaling Server configuration for the SIP URI map and Private/CDP domain name parameter (SIP CTI only). • Verify Routing, Host Authorization, and Certificates inside OCS servers and Pool.
When logged into Office Communicator, the phone icon does not display.	• The Server URI or the Line URI is incorrect.	• Use Microsoft tool nslookup to verify the DNS configuration on the Signaling Server, and the Host Name resolution for each IP address. • Check configuration parameters in AD for this user. • Confirm FQDN and IP address are correct.

Symptom	Possible Causes	Possible Solutions
New users were configured in AD, but the MCM did not download them to its AD cache during synchronization, and cannot find them.	• The change to the users in AD was not replicated to the Global Catalog (GC) server that the MCM uses. • MCM Service credentials are not sufficient to view msRTCSIP properties. • Field AD is not enabled for propagation to the GC.	• Check the GC content. Confer with the Network Administrator about schedule of replications between the domain controllers (DC). • Access permissions for the AD object properties. • Enable propagation of the AD to the GC. (Specify a DC LDAP server to reduce search scope to only one domain.)
OC Client(s) Unable to Register	For a Single Client	• Verify all clients are registered. • Look in the client options for AD for a mistake in SIP URI or Line URI. • For an RCC-enabled user, verify T87A class of service is configured for this client, and a session is established. • Remove RCC to see if VoIP functionality exists.
OC Client(s) Unable to Register	For Multiple Clients	• Ensure all component configuration information is correct on the Front End Server, Mediation Server, MCM, Signaling Server, SPS, Call Server, DNS.
When an Office Communicator user receives a call, the called telephone rings, but no pop-up appears for the user to click to answer the call.	• The Phone Context may not be correct. Address Book Service may not be set up properly. Phone integration is not activated.	• Ensure user's name is in the AD, the MCM, and the Signaling Server (L1 parameter) have the correct Phone Context. • Ensure Address Book Service is set up properly for an OC client. • Ensure PBX integration is marked for an OC client in the AD. Server URI Line must have valid information. • Ensure user has activated phone integration on OC client. • Ensure PCA is configured properly for the called user.

Symptom	Possible Causes	Possible Solutions
OC client users observe a delay at the beginning of a call.	• Missing OC client patch.	• Ensure that the OC client patch is current.
Customers using smart phones or Mobile Com munications cannot take control of the phone after having been disconnected abruptly at least 3 times.	• This disconnection could be due to the customer's network (for example, GPRS or WLAN). • SIP CTI link is disconnected abnormally, and the Association is out of service for 30 minutes (1800) seconds. This timer is hard coded by the OC client and cannot be changed.	• Increase field Maximum Associations per DN on the Signaling Server through Element Manager. The default setting is 3. Increase this parameter to allow more network disconnections.
When logged into the OC client, the phone is not controlled. The con in Undefined Resource displays.	• The Tel URI or Remote Call Control SIP URI is incorrect.	• Use Microsoft tool nslookup to verify DNS configuration of the Signaling Server and the Host Name resolution into each IP address. • Check the parameters configured in AD for this user. • Confirm that the FQDN (case sensitive) and the IP address are correct.

OCS 2007 troubleshooting issues

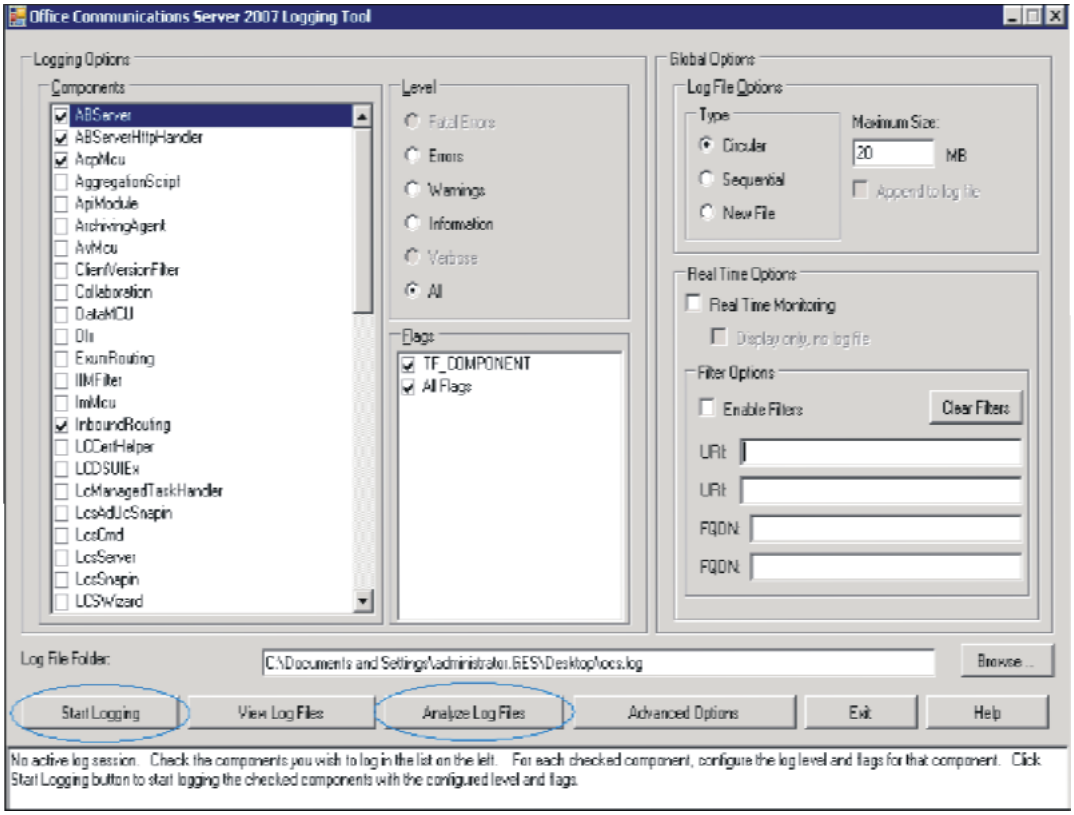
For OCS 2007 troubleshooting issues, you can use WireShark and any of the following tools:

- Logging Tool (accessible from FE pool and from a Mediation Server in the Microsoft Office Communications 2007 console)
- Event Viewer on OCS servers
- Windows Event logging for Communicator (requires a PC running Microsoft Office Communicator client)
- Logging in Communicator (requires a PC running Microsoft Office Communicator client)

Logging Tool

Access the Logging Tool from either the **FE pools** or **Mediation Servers** menu picks in the OCS 2007 console. From the Logging Tool dialog box, select **Start Logging**. Then make a call, stop logging, and analyze the log files. The following figure shows a sample of the Logging Tool dialog box.

Figure 11
Logging Tool

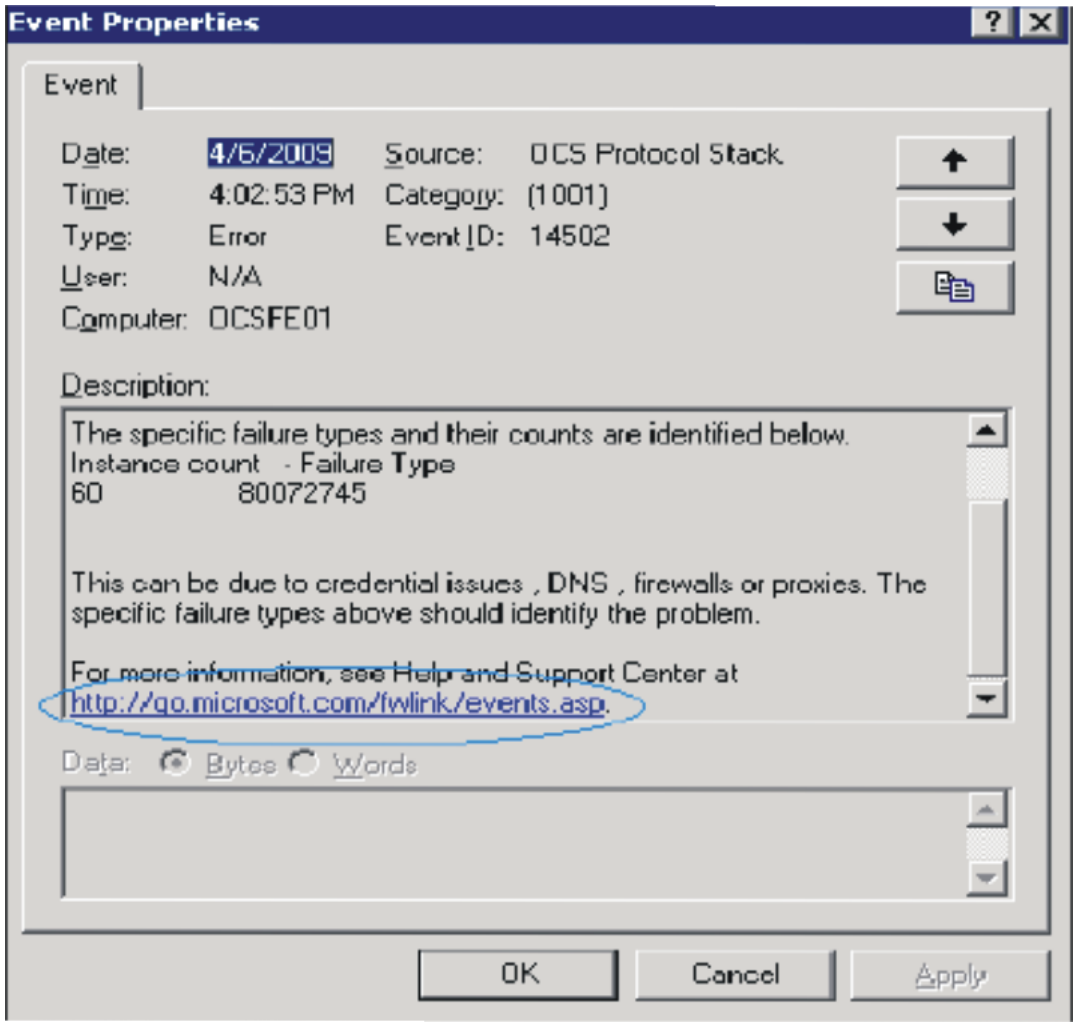


Event Viewer

The Event Viewer displays monitoring and troubleshooting messages. To access the Event Viewer, select it from the OCS server Administrative Tools menu.

For information about a specific event, click on Event Properties. This provides the date, time, and type of event along with a description of the event. It also includes a link to Microsoft's Help and Support Center for additional information. The following figure shows a sample of Event Properties.

Figure 12
Event Properties



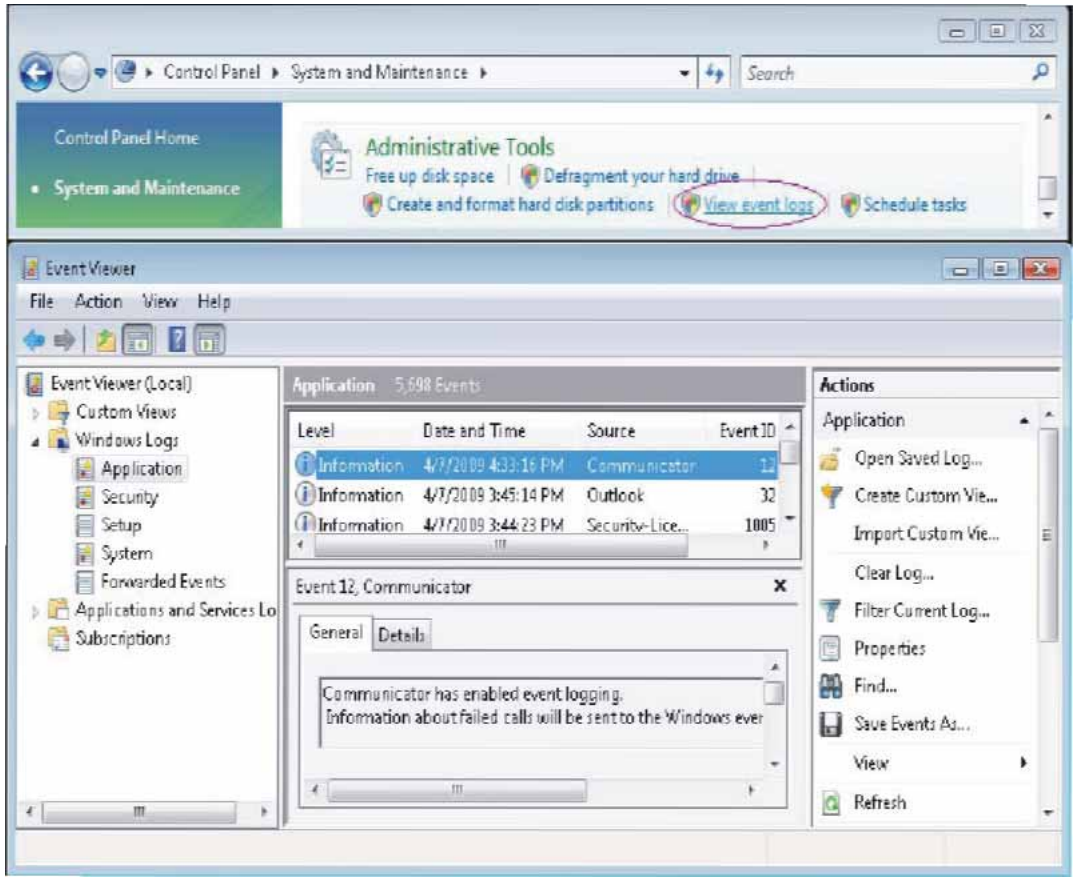
Windows Event logging for Communicator

Use the following steps to view the logs for Communicator.

ATTENTION
If you are not in the Performance Log Users group, the following message appears: **`Only the administrator of the computer and users in the 'Performance Log Users' group can control logging. Please try again after adding your account to 'Performance Log Users' and logging off and back onto your computer.`**

The following figure shows a sample Event logging for Communicator dialog box.

Figure 13
Windows Event logging for Communicator



Logging in Communicator

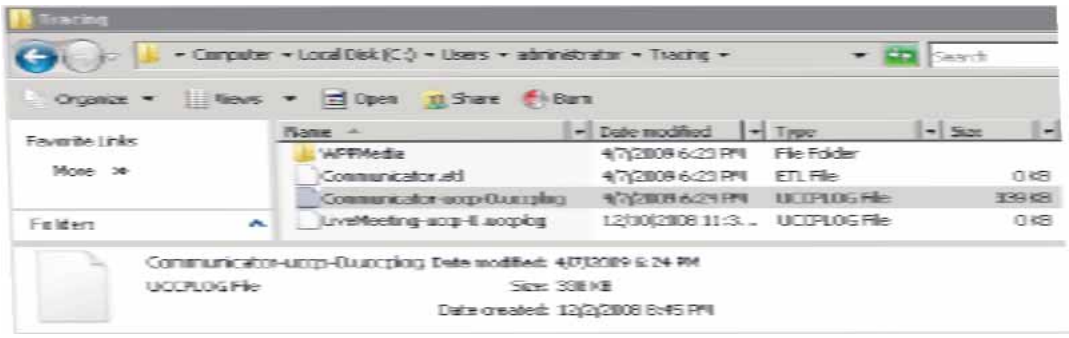
Use the following steps to access Logging in Communicator.

Step	Action
1	Log on to your PC with **administrator** credentials.
2	Navigate to the Office Communicator, Tools, Option, General tab.
3	Launch the OC client and sign in as an OCS user.
4	Check **`Turn on logging in Communicator`**.

--End--

The following figure shows a sample event log for Communicator.

Figure 14
Logging in Communicator



Voice services troubleshooting issues

If you experience a problem with a voice service or if PVQM isolates a voice problem, you can use the tips in this section to further troubleshoot the issue. For many issues with voice services, start your troubleshooting by checking the Customer Data Block configuration (LD 15 Options) and the Phone configuration (LD 20 Prt TNB). For more information, see *Nortel Communication Server 1000 Software Input Output Reference — Administration* (NN43001-611) and *Communication Server 1000 Troubleshooting Guide for Distributors* (NN43001-730.)

The rest of this section describes troubleshooting tips for the following specific issues:

Sets not getting Locate911 updates

Use the following steps to ensure that sets get location updates.

Step	Action
1	Use the following command to make sure the set appears in NU=1 state with ERL=0: `isetLocNeedUpdateShow`
2	Check the Search option using IP in the Locate911 menu.
3	Give Locate911 some time to search by waiting until the NU=18. NU=18 means that Locate911 conducted 18 search iterations.
4	If the set is not located, check the following: • Make sure the MAC ID is valid. • Make sure the IP Address is valid. • Check the Edge switch to make sure the MAC ID is visible against the port that this phone or PC is connected to.
5	When the set is located, wait until Locate911 updates the Call Server.

Locate911 shows two MAC IDs for each data port on a data switch with connections to phones and PCs connected to a phone.

--End--

Duplicate Locate911 entries for single set

Locate911 sometimes shows duplicate phone table entries for a single set. Where there should be one MAC ID for a single IP, the set shows multiple MAC IDs that are in a **`needs-update`** state. This issue affects soft phones only. When a soft phone changes location, its MAC and IP addresses also change. This causes Locate911 to create multiple entries in the phone table, and it does not delete the old entries.

A typical example of when duplicate entries appear is when a user is out of the office and registers a 2050 softphone. Locate911 creates an entry in the phone table. However, because the phone is not on the network that Locate911 is monitoring, Locate911 cannot locate the phone so the entry appears in the **`needs-update`** state. When the same user goes into the office and connects to the network, Locate911 creates a new entry, but does not delete the old entry.

To delete phone table entries that are no longer in use, reseed the phone table from the **Control Panel, Manage Nortel Settings, Seed Phones Database**.

Watchdog reset

The Telephony Proxy Server (TPS) sends watchdog reset messages to every softphone. This message causes the softphone to send an acknowledgement. If the softphone does not send a response, the RUDP transport resends the message up to 10 times. If there is still no response, the TPS marks the phone as offline and notifies the Call Server.

A softphone may not acknowledge a watchdog reset message for the following reasons:

- The softphone never received the watchdog timer reset message. In this case, the watchdog timer times out and the softphone reboots and begins the registration process.
- A network failure or high traffic through a router causes the message to be lost or delayed. This can happen when the softphone is on a different subnet than the TPS TLAN and one of the network routers drops packets. The RUDP polling message is a plain UDP message

and is thus a candidate for being dropped before higher priority packet data.

- The softphone is unplugged and left unplugged during the time the TPS card polls it.

To troubleshoot this issue, use the following commands to set levels in vxshell to view traces:

```
syslogLevelSet tSET, x
syslogLevelSet tVTM, x
syslogLevelSet tCSV, x
syslogLevelSet tRUDPSS, x
syslogLevelSet tTPS, x
```

Then use **syslogShow** to confirm the settings.

IP peer calls fail

If the Endpoints register successfully and you cannot successfully make a call to an IP peer, try the following steps.

ATTENTION
If you are using **cslogin** to communicate with the Call Server, make sure all of your PTYs have SCH, MTC & BUG enabled.

Step	Action

1	Use the following command to verify that the call is being pushed out the virtual route through a Virtual DCH trace in LD 96.
	`STAT DCH <dch#>`
	The following display appears:
	`DCH 063: OPER EST ACTV AUTO`
	`ENL MSGI DCH 63 (incoming messages)`
	`ENL MSGO DCH 63 (outgoing messages)`

2	Place a call that fails and observe the messages.
3	Verify that the call is being received on the virtual DCH on the far end.
4	If the call is not received on the far end, verify that the numbering plan in the Gatekeeper is defined correctly for the far end.
5	Use the following command to perform a debug trace of the Gatekeeper lookup at the Signaling Server: `gwCallTrace all`

Use **gwTraceOff** to turn off the trace.

--End--

NSNA troubleshooting issues

If you experience a problem with NSNA or if PVQM isolates a problem to NSNA, you can use the steps in this section to further troubleshoot the issue. For many issues with NSNA, start your troubleshooting with the trace utility.

```
Maintenance# starttrace
```

For more troubleshooting information, see *Nortel Secure Network Access Switch Troubleshooting* (NN47230-700.)

Step	Action
1	Use the **netstat** command to check the ancillary service devices such as the DHCP, TFTP, and DNS servers:
2	Use the **netstat –an** command to check to see which network sockets are operating. The following shows some sample output from this command.

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:53	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
.			
.			

Step	Action
3	Use the **netstat –ab** command to see which processes are operating.
4	Use the **tasklist** command to see the processes and executables running on the platform. The following shows some sample output from this command.

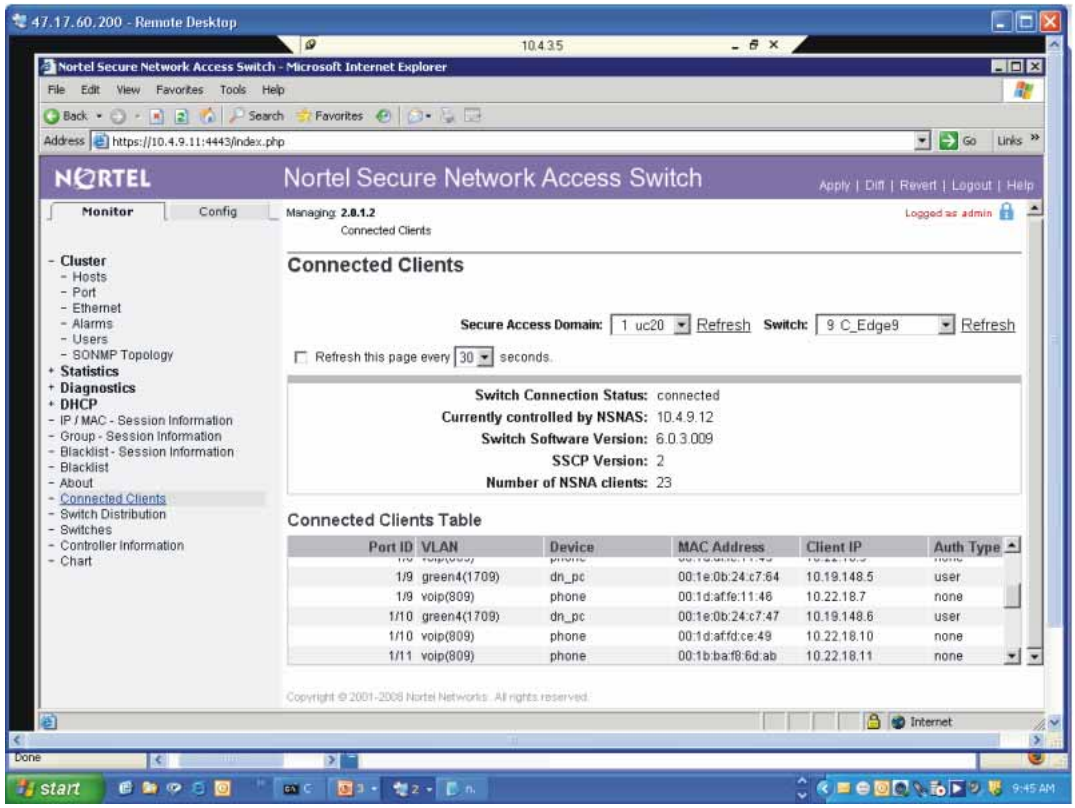
Image Name	PID	Session Name	Session #	Mem Usage
System Idle Process	0	RDP-Tcp#59	0	16 K
System	4	RDP-Tcp#59	0	224 K
smss.exe	280	RDP-Tcp#59	0	452 K
.				
.				

5 Match the PID from the **`netstat`** output with the PID of **`tasklist`** to identify the executable.

6 From **NSNA, Monitor, Connected Clients**, check the network to confirm that the accessing client is in the correct physical LAN and IP subnet.

The following figure shows the devices connected to edge switch 9 along with the following information:

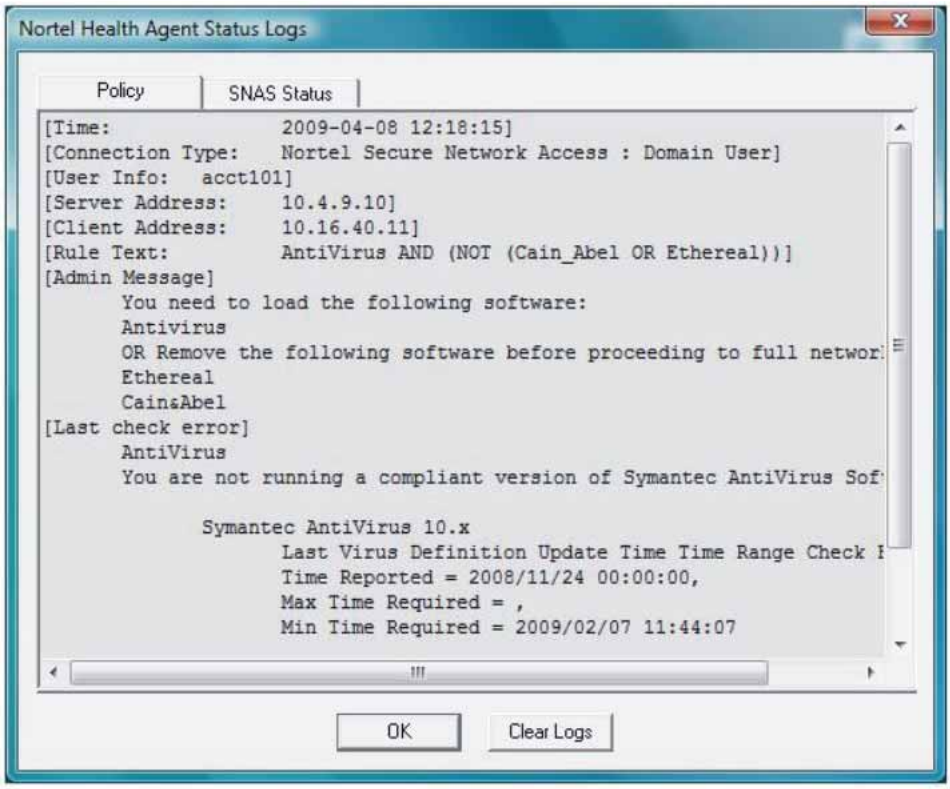
- A phone is connected to port 9.
- A PC is connected to the phone's Ethernet switch port.
- The physical port, 1/9, has a PC and a phone based upon MAC info and device type.
- There are VLANs called green4 (1709) and voip (809).
- The IP address for the PC is 10.19.148.6, and the IP address for the phone is 10.22.18.7.



7 Confirm that the Connected Clients information aligns with the design intent. If it does not align, then check to make sure the applications are functioning.

8 Check the Nortel Health Agent (NHA) client.

The following figure shows an example of an NHA log. This particular log indicates that there is an issue with the software loaded on the PC.



9 Check the logs to make sure the system components are functioning correctly.

10 Check the actual server providing the required service such as the OCS server or the Communication Server 1000 to confirm that the service is functioning.

--End--

CallPilot troubleshooting issues

If you experience a problem with CallPilot or if PVQM isolates a problem to CallPilot, you can use the tips in this section to further troubleshoot the issue. Be sure to check the CallPilot High Availability (HA) installation. HA requires specific installation and maintenance procedures that differ from the standard procedures. Failure to follow these procedures could render a system unusable. For more information, see*CallPilot High Availability Installation and Maintenance* (NN44200-311.)

Dead air

If you call someone and the phone rings, but there's no answer (dead air), try the following:

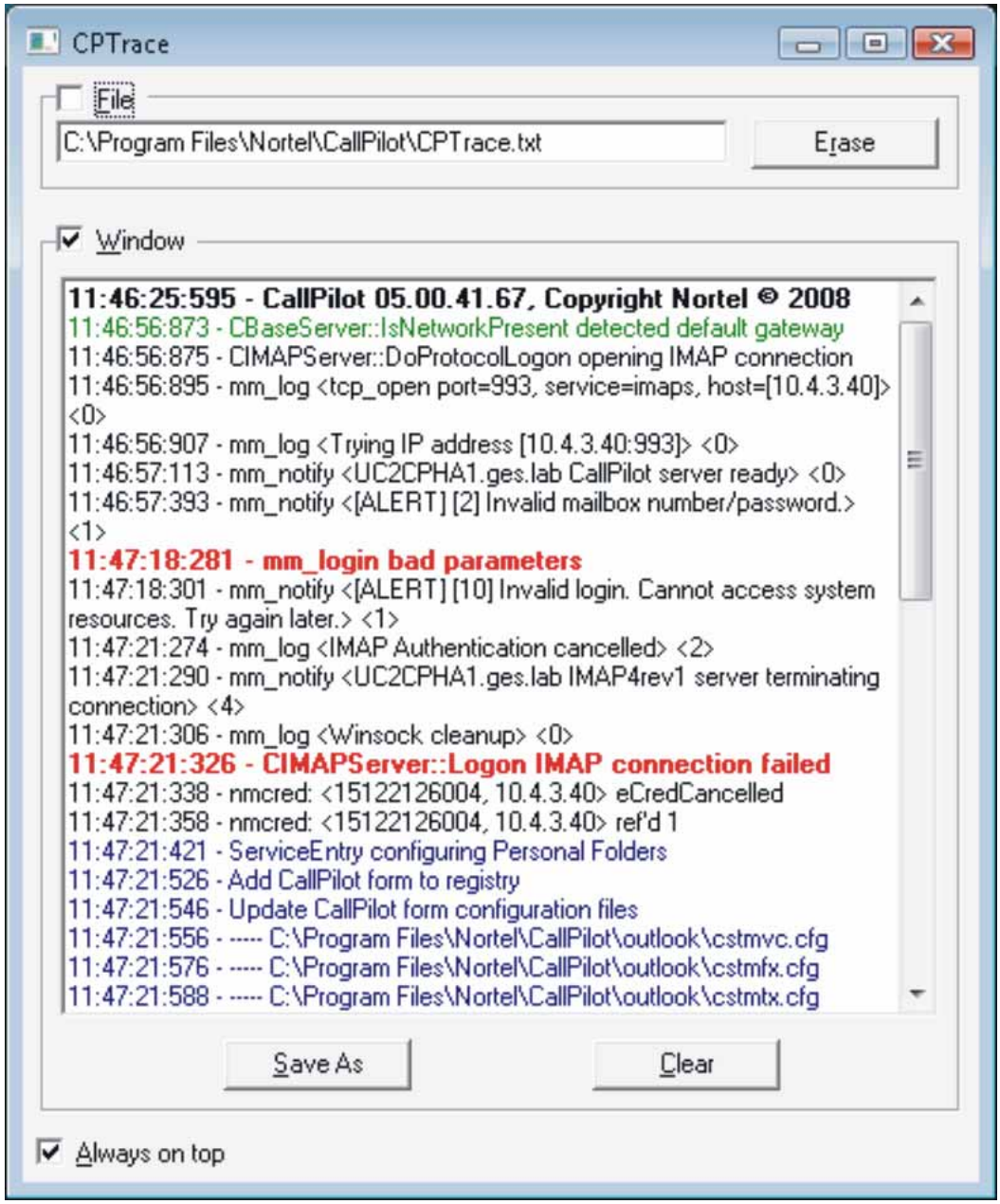
- Use CPMgr to check that all channels are up.
- Check cabling from MPB to MGates on active server.
- From the CallPilot server, ping the Communication Server 1000 ELAN to check connectivity.
- Start ELAN in ld 48 to ensure that it is running.
- Use EMC Autostart to check that the CallPilot resource group is online.

Client connection issues

If you experience Client connection issues with Desktop, Appbuilder, Reporter, or MyCallPilot, try the following:

- Verify that the Client is configured to connect to the managed CLAN host name and IP address.
- Run CPTrace from desktop clients to trace the connection and login. (The following figure shows a sample CPTrace.
- Run CPTrace from the MyCallPilot server to trace the connection and login.

Figure 15
CallPilot Trace



Event logs

Use the Event logs to troubleshoot issues.

- To determine why failovers occurred, view the Event logs from the Autostart Console.
- To view general CallPilot events, view the Event logs from the Windows Event logs and CPMgr event monitor.

Autostart notification

You can closely monitor CallPilot with the Autostart notification feature. When enabled, this feature sends you an e-mail notification when there is a change in CallPilot such as a resource group status change or when a failover occurs.

Contact Center troubleshooting issues

If you experience a problem with Contact Center or if PVQM isolates a problem to it, use the tips in this section to further troubleshoot the issue. You can also use the following tools:

- Shutdown—This tool stops all Contact Center Manager Server (CCMS) services. You can use this tool during manual failovers and when you want to stop services to help you isolate a problem. Access Shutdown from **Start, Programs, Nortel Contact Center, Manager Server, Shutdown**.
- System Monitor—This tool shows the current state of all CCMS services. Access System Monitor from **Start, Programs, Nortel Contact Center, Manager Server, System Monitor**.

CCMA and CCMS issues

This section describes some general Contact Center Manager Administration (CCMA) and CCMS troubleshooting issues.

- **CCMA license error**—If CCMA shows that your license expired, it may be a problem with the NIC card configuration. Contact Center (CC) licensing is tied to NIC cards so, if there are multiple NICs, make sure CC is using the correct one. You can swap NICs if you configured the wrong one, but then you have to delete and re-add the server definition to CCMA.
- **Adding a CCMS server**—You can add a CCMS server only if it is online. If this is a secondary server, you can add it only after the active server failed over to the secondary.
- **CCMS configuration tool error**—You may see configuration errors if there are multiple NICs on the server and CCMS is using only one. To correct this error, disable the unused NICs.
- **MIRAN audio files**—To import audio files to Meridian Integrated Recorded Announcements (MIRAN), they must be in a specific format. For more information, see *Integrated Recorded Announcer — Service Implementation Guide* (553-3001-112.)
- **CCMS replication synchronization**—If replication gets out of sync, try the following steps:
  - — Remove the warm standby configuration from the replication server.
  - — If successful, recreate the warm standby.
  - — If you cannot remove the warm standby configuration

- run **D:\nortel\iccm\bin\wsstoprep.exe** on both CCMS servers to remove replication configuration from the servers.
- Uninstall the replication server.
- Reinstall the replication server.
- Recreate the warm standby configuration.

Agent Desktop Display

The Agent Desktop Display (ADD) requires a multicast-enabled network between the CCMS and CCMA server and between the CCMA server and the desktop clients. Then the agents must be logged in before you can see Agent Desktop Displays. If there is a troubleshooting issue with ADD, try the following steps:

- Make sure the RTD/RSM configuration parameters are correct.
- Use **mrcv.exe** to verify that data is being transmitted from CCMS.
- Use **icertdtrace -r IPReceive <Multicast_IP_Receiving_Address> -t statistic** to trace incoming data from CCMS. This enables you to verify that data is being received at CCMA.
- Use **icertdtrace -r IPSend <Multicast_IP_Sending_Address> -t statistic** to trace outgoing data from CCMA. This enables you to verify that CCMA is transmitting data.

Contact Recorder

You can configure Contact Recorder in either of the following configurations:

- Master and Slave—In this configuration, the Slave records all calls. The Master records only when the Slave is unavailable.
- Master and Standby—In this configuration, the Master records all calls. The Standby takes over when the Master is down.

In either configuration, you can create log files to help you troubleshoot issues. For detailed logs, change the log level by entering in **http://recorderservername:8080/log?level=DEBUG** in your browser. To turn logging back to normal level, enter **http://recorderservername:8080/log?level=INFO** If you see a socket error in the log file every minute, you probably have quality monitoring enabled in keycode and an address specified in the configuration. Clear this error by removing the address from the configuration.

To access the Contact Recorder Playback feature, you need a sound card on the machine where you launch the browser. Nortel recommends a USB sound card. Playback is available only on the server that actually recorded the call. If the Standby server recorded the call, you cannot play back the recording on the Master server. You can also only play back recordings based on your user settings in Contact Recording.

Nortel Multimedia Conferencing troubleshooting issues

If you experience a problem with Nortel Multimedia Conferencing (NMC) or if PVQM isolates a problem to NMC, you can use the tips in this section to further troubleshoot the issue. Check your configuration to make sure it adheres to the Nortel Best Practices listed in *Nortel Unified Communications Campus Solution Configuration — Voice Services* (NN49000-313.) For more information, see *Nortel Multimedia Conferencing Logs* (NN44460-700.)

NMC runs on the Media Application Server (MAS) platform so you can use the MAS Reporter to troubleshoot NMC. Reporter is a performance management tool that generates reports. For detailed information about MAS performance management, see *Nortel Media Application Server Performance Management* (NN44450-701.)

Step	Action
1	In the MAS Console, select **Configuration, Reporter**.
2	In the Reporter window, locate the type of report that you want to generate.
3	Double-click the report name.
4	In the report Properties window, select **Enable** to enable the selected report or **Disable** to disable the report in the Value list.
5	Click **OK**.
6	If you want to generate multiple reports, repeat step 2 to step 5 for each type of report that you want to generate.
7	Restart the MAS platform for the changes to take effect.

--End--

LiveMeeting troubleshooting issues

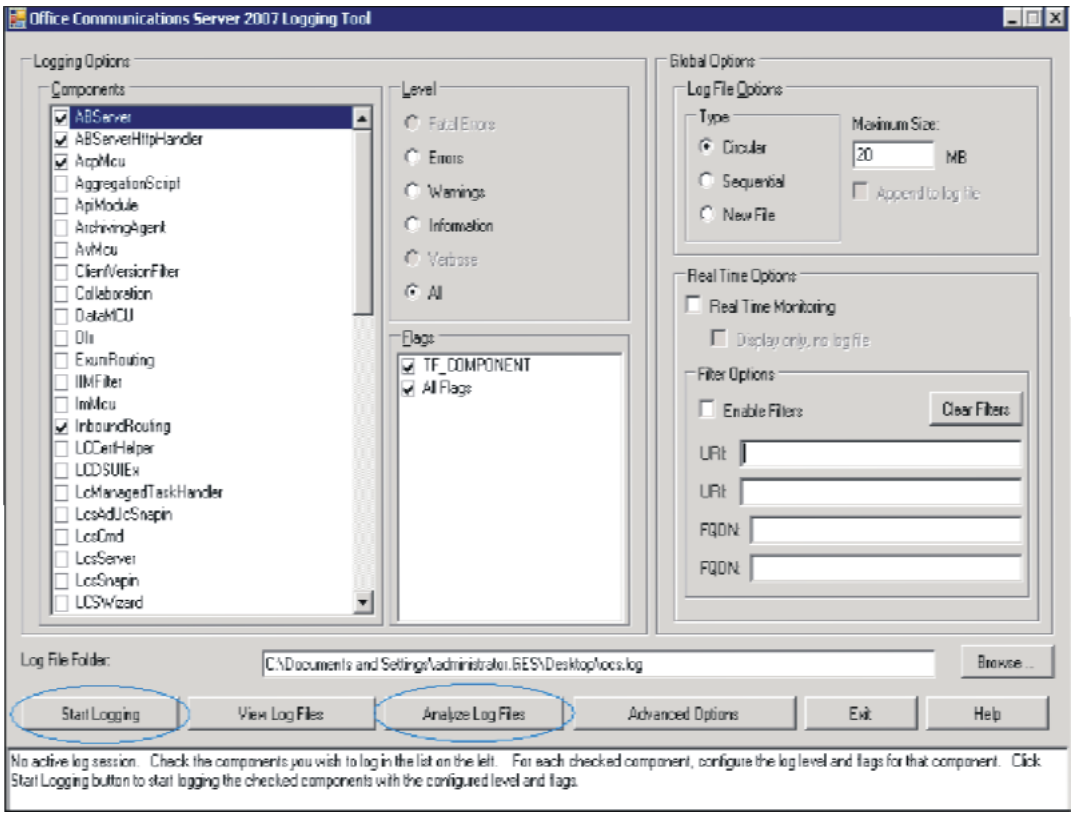
For LiveMeeting troubleshooting issues, you can use WireShark and any of the following tools:

- Logging Tool (accessible from FE pool in the Microsoft Office Communications 2007 console)
- Event Viewer on OCS servers
- Logcapture in the NMC server running Audio Conferencing Provider (ACP)

Logging Tool

Access the Logging Tool from the **FE pool** menu pick in the OCS 2007 console. From the Logging Tool dialog box, select **Start Logging**. Then make a call, stop logging, and analyze the log files. The following figure shows a sample of the Logging Tool dialog box.

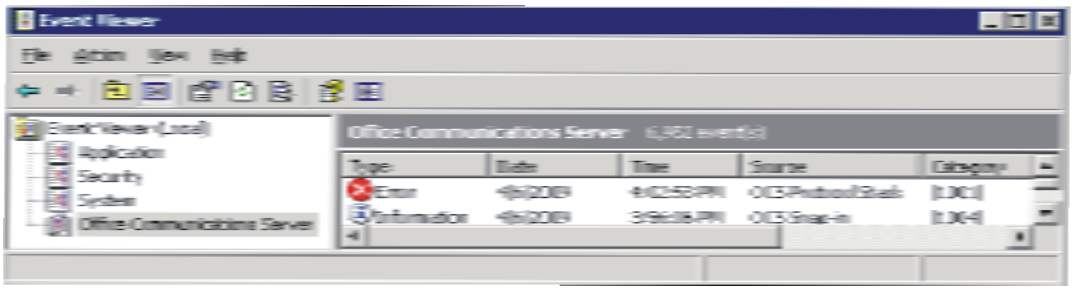
Figure 16
Logging Tool



Event Viewer

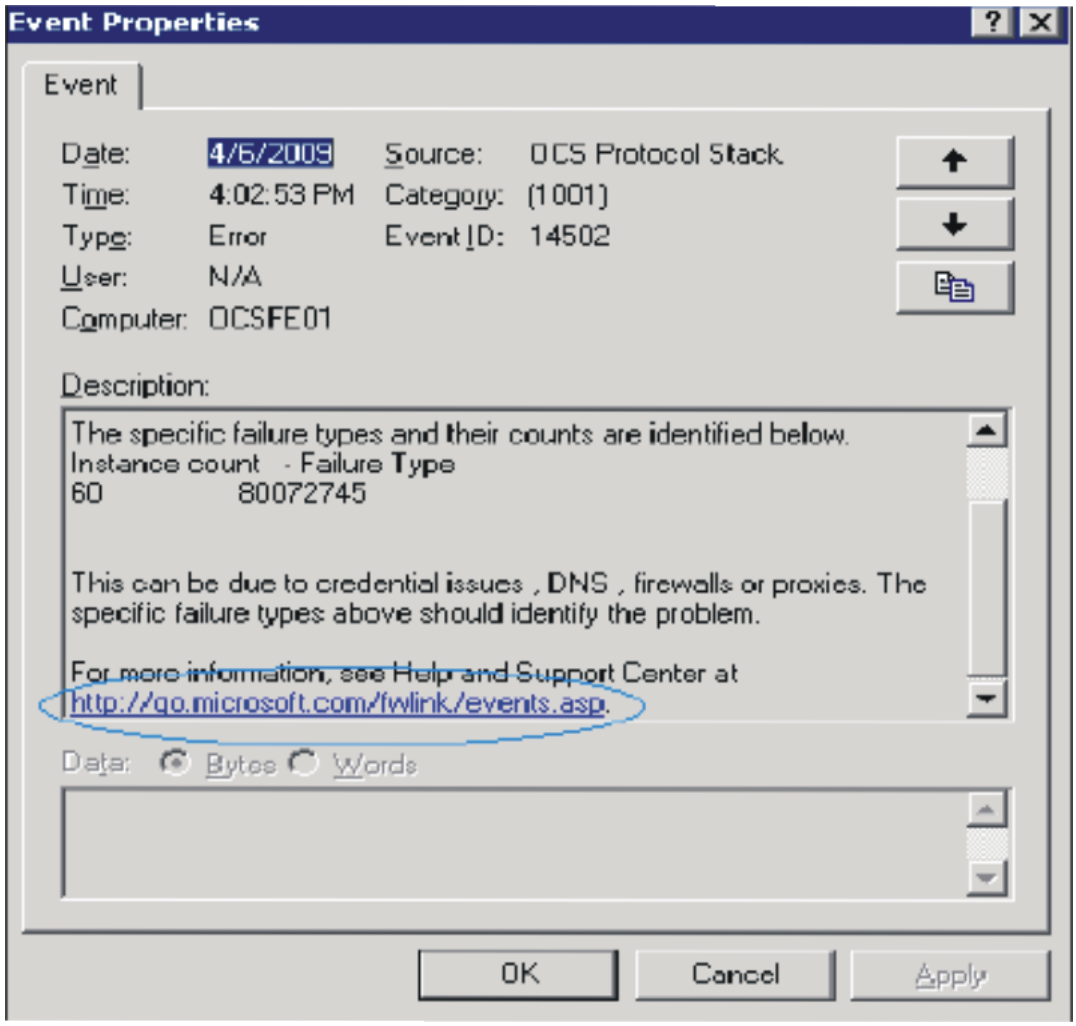
Access the Event Viewer from the OCS server Administrative Tools menu. The Event Viewer displays monitoring and troubleshooting messages. The following figure shows a sample Event Viewer dialog box.

Figure 17
Event Viewer



For more information about an event, click on Event Properties. This provides the date, time, and type of event along with a description of the event. It also includes a link to Microsoft's Help and Support Center for additional information. The following figure shows a sample of Event Properties.

Figure 18
Event Properties



Logcapture

Access the Logcapture tool by logging on to the NMC server running ACP with administrator credentials. Then launch the command window and enter **`logcapture -t`**.

Logcapture creates a **log.zip** file in the directory where you entered the **`logcapture`** command. All of the files in the log.zip file are important for troubleshooting, especially **acpserver.txt** and **sipmcDebug.txt**

Ethernet Routing Switch troubleshooting issues

If you experience a problem with Ethernet Routing Switches or if PVQM isolates a problem to them, determine if the faulty switch is in the Core or the Edge. Then check your configuration to make sure it adheres to the Nortel Best Practices listed in *Nortel Unified Communications Campus Solution Configuration — Ethernet Infrastructure, Security, and Network Management* (NN49000-312.)

If you continue to experience problems, the Ethernet Routing Switches support a wide range of diagnostic tools that you can use to monitor and analyze traffic; capture and analyze data packets; trace data flows; view statistics; and manage event messages. Some of the available tools are: Port Mirroring, Remote Monitoring, Ping, Ping Snoop, Trace, Traceroute, and Packet Capture (PCAP).

For more troubleshooting information: see one of the following:

- For the ERS 8600, see *Nortel Ethernet Routing Switch 8600 Troubleshooting* (NN46205-703.)
- For the ERS 5500, see *Nortel Ethernet Routing Switch 5500 Series Troubleshooting* (NN47200-700.)
- For the ERS 4500, see *Nortel Ethernet Routing Switch 4500 Series Troubleshooting* (NN47205-700.)

Information resources by service

This chapter describes information resources available for troubleshooting a UC Campus deployed Solution, service by service.

Data infrastructure

Troubleshooting the Unified Communications data infrastructure requires the use of management tools as discussed in the prior chapter, "Troubleshooting: Tools and Procedures", as well as tools residing locally on infrastructure components. Areas of focus for troubleshooting the UC data infrastructure are, for example:

- Layers 1 and 2 -- Ethernet switching (ERS 8600, 5500, 4500), Inter-Switch Trunking (IST), Single Link Trunking (SLT), and Split Multiple Link Trunking (SMLT), Physical and Data Link connectivity within the UC data infrastructure
- Layer 3 -- Unicast and multicast IPv4 routing and Routed Split Multiple Link Trunking (RSMLT) running on Nortel ERS components within the UC data infrastructure
- Other IP-based protocols (SNMP, DHCP, IGMP, ICMP) running on Nortel ERS components within the UC data infrastructure.

A dedicated component-level Troubleshooting publication exists for each of the model 8600, 5500, and 4500-series Ethernet Routing Switches, providing many aids to Layer 1 to 3 troubleshooting. Other ERS component publications (for example, relating to performance management) contain additional information and procedures that are helpful during the fault isolation process. After isolating a problem down to a specific component, refer to the appropriate component-level publications as detailed in:

- “ERS 4500” (page 72)
- “ERS 5520/5530” (page 74)
- “ERS 8600” (page 75)

ERS 4500

Nortel provides documentation resources to troubleshoot the ERS 4500 as follows:

The publication, *Nortel Ethernet Routing Switch 4500 Troubleshooting*, NN47205-700, provides reference and procedural information on the following topics:

- Troubleshooting tools
  - *Port mirroring:* Monitoring and analyzing network traffic.
  - *Port statistics:* Displaying the number of packets received and transmitted at ERS ports.

- — *Stack loopback testing:* Determining if the switch has a bad stack cable or a damaged stack port.
- — *Stack health check:* Confirming stack operation and stack continuity.
- — *Stack forced mode:* Maintaining operation and IP reachability of a stand-alone stackable switch, where another switch in the stack pair has failed.
- — *System logs:* Analyzing SYSLOG messages sent to a management station.
- — *Backup configuration file:* Automatically checking at boot time the primary switch configuration file against the backup configuration file, resulting in a success/fail message sent to the system log. If the check fails, the system resets all configuration settings to their default values.
- — *ASCII download log enhancement:* Checking customer-accessible log messages describing any failures detected during an ASCII Configuration File download.
- — *CPU and memory utilization:* Analyzing switch CPU and/or memory utilization levels.

- Emergency Recovery Trees (ERTs)
- Troubleshooting hardware
- Troubleshooting Automatic Detection and Configuration (ADAC)
- Troubleshooting authentication
- Troubleshooting SNAS
- Troubleshooting XFP/SFP
- Troubleshooting IGMP
- Troubleshooting SNMP traps
- Troubleshooting DHCP/BootP relay

Additional documentation available for troubleshooting the ERS 4500:

- *Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and Multi-Link Trunking* (NN47205-501).

  This document provides information you need to configure VLANs, Spanning Tree, and Multi-Link Trunking for the ERS 4500 Series. This document also lists which VLACP failures and errors result in error logs.

- *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502)

This document describes system diagnostics tools including Syslog, Remote Monitoring, port mirroring, and displaying port and chassis statistics.

ERS 5520/5530

Nortel offers documentation and training resources to troubleshoot the ERS 5520 and 5530. See:

- “ERS 5520/5530 documentation” (page 74)
- “ERS 5520/5530 training” (page 75)

ERS 5520/5530 documentation

The publication, *Nortel Ethernet Routing Switch 5500 Troubleshooting*, NN47200-700, provides reference and procedural information on the following topics:

- Troubleshooting tools
  - *Port mirroring:* Monitoring and analyzing network traffic.
  - *Port statistics:* Displaying the number of packets received and transmitted at ERS ports.
  - *Stack loopback testing:* Determining if the switch has a bad stack cable or a damaged stack port.
  - *System logs:* Analyzing SYSLOG messages sent to a management station.
  - Auto Unit Replacement (AUR): Replacing a failed unit in a stack with a new unit, while retaining the configuration of the previous unit.
- Emergency Recovery Trees (ERTs)
- Troubleshooting hardware
- Troubleshooting authentication
- Troubleshooting the Nortel SNAS
- Troubleshooting Layers 2 and 3
  - VLANs
  - Virtual Routers (VRs)
  - ARP
  - OSPF
  - VRRP
- Troubleshooting XFP/SFP

- Troubleshooting IGMP
- Troubleshooting SNMP traps
- Troubleshooting DHCP/BootP relay

Additional documentation used to troubleshoot the ERS 5520 or 5530:

- *Nortel Ethernet Routing Switch 5000 Series Configuration — System* (NN47200-500)

  This document provides information and procedures required to configure the software for the ERS 5000 Series. This document also describes the error messages that may be displayed by a port that supports PoE.

- *Nortel Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and Link Aggregation* (NN47200-502)

  This document provides information you need to configure VLANs, Spanning Tree and Link Aggregation for the ERS 5000 Series. This document also describes VLACP feature error logs and information on troubleshooting IST problems.

- *VLACP time-out issue between stackable platforms and ERS 8300/8600* (2008009238)

  This bulletin describes and gives recommendations for the VLACP time-out issue between stackable platforms and ERS 8300/8600.

- *Ethernet Routing Switches: SysUpTime approaching 497 days can cause the switch or stack to behave in some unexpected way.*

  This bulletin addresses the issue of unexpected switch or stack behavior that occurs when SysUpTime approaches 497 days.

ERS 5520/5530 training

The following video provides ERS troubleshooting information.

- *ERS 5510, 5520, 5530, ES470 and BPS Recovery Training Video*

  This RTV provides customer support personnel recovery methods used by Nortel's Emergency Recovery team in resolving network outages.

ERS 8600

Nortel offers documentation and training resources to troubleshoot the ERS 8600. See:

- "ERS 8600 documentation" (page 76)
- "ERS 8600 training " (page 77)

ERS 8600 documentation

The publication, *Nortel Ethernet Routing Switch 8600 Troubleshooting*, NN46205-703, provides reference and procedural information on the following topics:

- Troubleshooting tools
  - *Port mirroring:* Monitoring and analyzing network traffic.
  - *Remote mirroring:* Steering mirrored traffic through a switch cloud to a network analysis probe located on a remote switch.
  - *Ping Snoop:* Displaying the route that IP traffic takes over an MLT or SMLT path. Console displays the port used for each IP traffic flow from source to destination.
  - *Packet Capture (PCAP)*: Capturing ingress and egress packets associated with different traffic flows on selected I/O ports. You can subsequently analyze captured packets offline for anomalies.
  - *Traceroute*: Using the traceroute command to record the IP route to a specific destination IP address, revealing the address of the computer at each hop of the route, as well as the amount of time for a packet to traverse each hop.
  - *Ping:* Determining reachability of a specified IP destination.
  - *Log and trap configuration*: Configuring the ERS 8600 to send system log and trap messages to a management workstation
- Troubleshooting hardware
- Troubleshooting software
- Troubleshooting licensing issues
- Troubleshooting Layer 1 (optical fiber links)
- Troubleshooting Layer 2 (IST links)
- Troubleshooting Layer 3 (OSPF and Multicast IP routing)
- Troubleshooting IP utilities (SNMP and DHCP)
- SNMP traps reference

Other documents used to troubleshoot the ERS 8600 are:

- *Ethernet Routing Switch 8600 Logs Reference* (NN46205-701)

  This guide describes the log messages generated by the ERS 8600 System Messaging Platform (SMP).

- *Ethernet Routing Switch 8600 - Fault Management* (NN46205-705)

  This document provides information about Remote Monitoring (RMON), traps and logs, controlling link state changes (port flapping), viewing RMON statistics, and RMON alarm variables.

- *Ethernet Routing Switch 8600 - Traps Reference* (NN46205-706)

  The document describes the proprietary and standard traps available for the ERS 8600.

- *Ethernet Routing Switch 8600 Firewall and Intrusion Sensor Fundamentals* (NN46205-100)

  This document includes initial setup, configuration, maintenance and troubleshooting procedures for the ERS 8600 Firewall and Intrusion Sensor components and features of the Service Delivery Module Firewall 1 (SDM FW1), FW2, and FW4 system.

- *Nortel Ethernet Routing Switch 8600 User Interface Fundamentals* (NN46205-308)

  This document describes how to use Device Manager, the command line interface (CLI), or the Nortel command line interface (NNCLI).

- *Nortel Ethernet Routing Switch 8600 Configuration — IGAP* (NN46205-512)

  This document describes how the Internet Group Management Protocol (IGMP) for Internet Group Membership Authentication Protocol (IGAP) is implemented in the ERS 8600, as well as how to configure an IGAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.

  This document also describes how to troubleshoot IGAP network connectivity.

- *Nortel Ethernet Routing Switch 8600 Configuration — IP VPN* (NN46205-520)

  This document describes how to configure logs and traps for fault management operations and use to provide diagnostic information in troubleshooting procedures.

- *ERS 8600: Software System Monitor May be Disabled* (2009009386)

  This Bulletin describes the Software Lockup Detection feature and how to tell if it is enabled on the system.

- *Nortel Response to OpenSSL 'EVP_VerifyFinal' Function Signature Verification Vulnerability* (2009009350)

  This bulletin provides a response for Nortel products which are potentially affected by the OpenSSL "EVP_VerifyFinal()" function signature verification vulnerability.

ERS 8600 training

The following course and video address troubleshooting the ERS 8600:

- *ERS 8600 Troubleshooting* (6728C)

This course covers basic and advanced troubleshooting skills for different problem scenarios on the ERS 8600.

- *Enterprise Ethernet Routing Switch 8300 and 8600 Saving Configuration files Recovery Training Video*

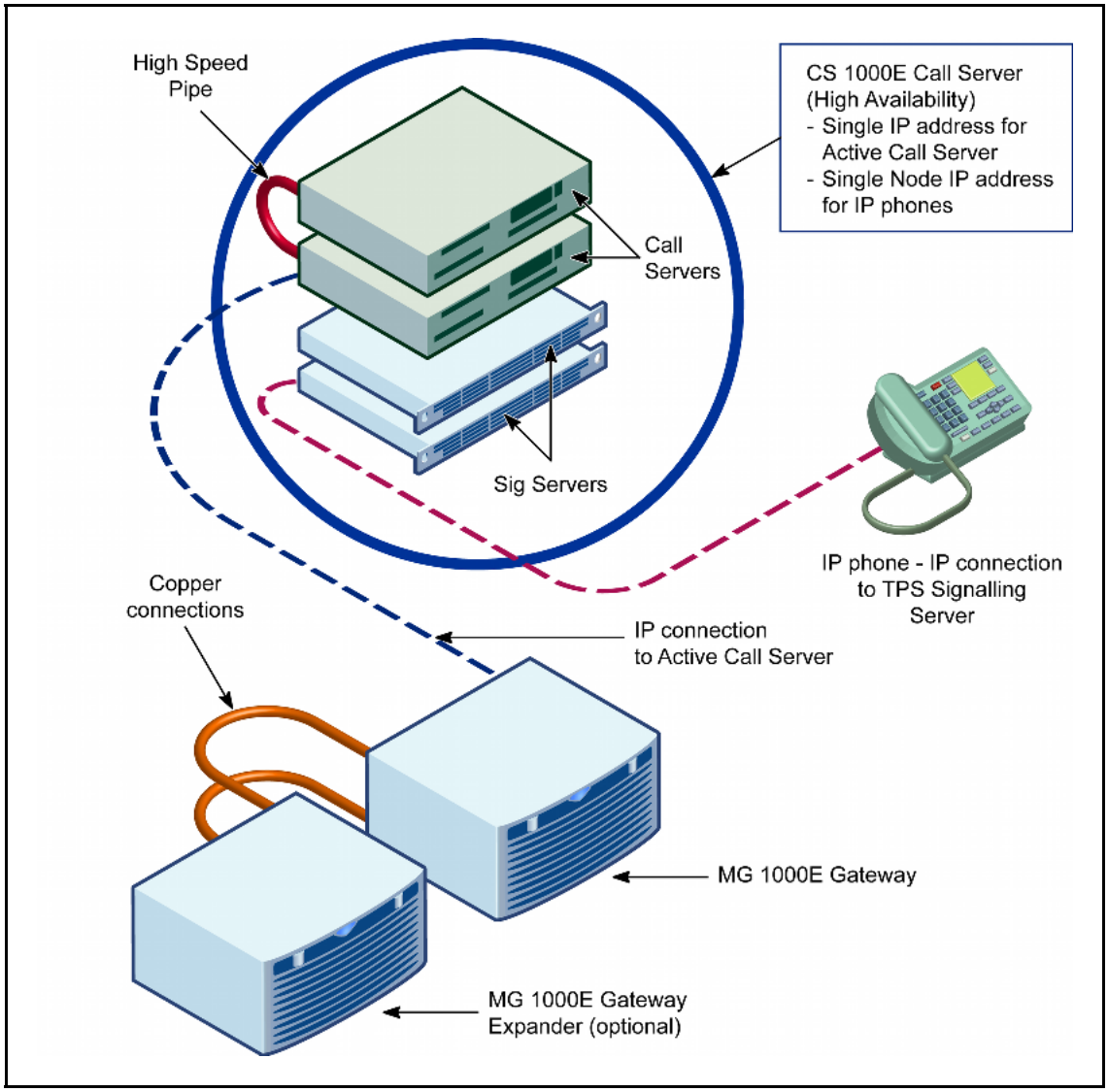
  This video provides describe recovery methods used by Nortel's Emergency Recovery team to resolve network outages.

CS 1000 voice services

The CS 1000 supports business-critical applications, including unified messaging, customer contact center, and IP phones. This section describes:

- “Survivable Media Gateway (SMG)” (page 83)
- “CS 1000 training” (page 82)
- “eTelemetry Locate911” (page 84)

From a troubleshooting point of view, the CS 1000E high availability (HA) configuration includes multiple call servers, signaling servers, media gateways, and PRI gateways, as shown in the following figure:



Message flow diagrams associated with setup and teardown of the many different call scenarios supported by the CS 1000 are helpful for troubleshooting from a normal-operation baseline, knowing which components should send and receive specific messages at each stage of call progress. These diagrams are available on request through Nortel Global Services.

For more information about Nortel troubleshooting resources, see:

- “CS 1000 documentation” (page 81)
- “CS 1000 training” (page 82)

CS 1000 documentation

The following documents provide information on troubleshooting CS 1000E health and performance.

- *Communication Server 1000 Release 5.x Troubleshooting Guide for Distributors* (NN43001-730)

  This document describes commands and techniques you can use to troubleshoot problems with CS 1000 and VoIP components.

- *Nortel Communication Server 1000 Communication Server 1000E Maintenance* (NN43041-700)

  This document describes system maintenance for the CS 1000E system. It also describes error messages and how to troubleshoot MG 1000T faults.

- *Communication Server 1000 Software Input Output Reference - System Messages* (NN43001-712)

  This document outlines the system messages sent by the CS 1000 components and provides information on interpreting and responding to these messages.

- *Nortel Communication Server 1000 Branch Office Installation and Commissioning* (NN43001-314)

  This document describes the Branch Office feature and contains information on planning, installation, configuration, maintenance, and troubleshooting.

- *Enterprise: Common Solution Integration Guide for Communication Server 1000 Release 5.0/Microsoft Office Communications* (NN49000-309)

  This document describes the planning, configuration, and troubleshooting of the integration of the CS 1000 system with Microsoft Office Communications Server 2007 (OCS 2007) Enterprise Edition services. It also describes how to collect system logs for troubleshooting purposes.

- *Nortel Communication Server 1000 Nortel Converged Office Fundamentals — Microsoft Office Communications Server 2007* (NN43001-121)

  This document describes the elements and processes necessary to integrate the CS 1000 with the OCS 2007 in the Nortel Converged Office. It also describes troubleshooting general Converged Office problems.

- *Enterprise Voice Audio Quality* (NN43001-705)

  This document provides an overview of common problems encountered when using Enterprise Voice, provides tools and techniques to resolve audio quality issues, and introduces common troubleshooting terminology used.

For access to all troubleshooting documentation related to the CS 1000E platform, proceed as follows:

Step	Action
1	Go to the Nortel Technical Support Portal at http://support.nortel.com/go/main.jsp
2	Under "Documentation, Software, and Bulletins", select "Voice, Multimedia, and Unified Communications".
3	Scroll down and select "Communications Server 1000E".
4	Under "Documentation" > Fault and Performance Management", select "Troubleshooting". *You should see a list of all CS 1000E troubleshooting resources (publications, videos, and so on).*

--End--

CS 1000 training

The following course and videos provide information about how to troubleshoot various aspects of CS 1000E operation.

- *Nortel Communication Server 1000 5.5 Troubleshooting and Maintenance* (0701C)

  This course describes how to troubleshoot CS 1000 systems through demonstration, class discussions, and hands-on labs.

- RTVs describe recovery methods used by Nortel's Emergency Recovery team to resolve network outages. The following RTVs are available for CS 1000E:

  — *CS1K Outage Data Collection Recovery Training Video*

  — *CS1K Understanding Traffic Measurement System Recovery Training Video*

  — *CS1K Large System Back Up Recovery Training Video*

  — *CS1K Small Systems Back Up Recovery Training Video*

  — *Enterprise CS1K MGC Loadware Recovery Training Video*

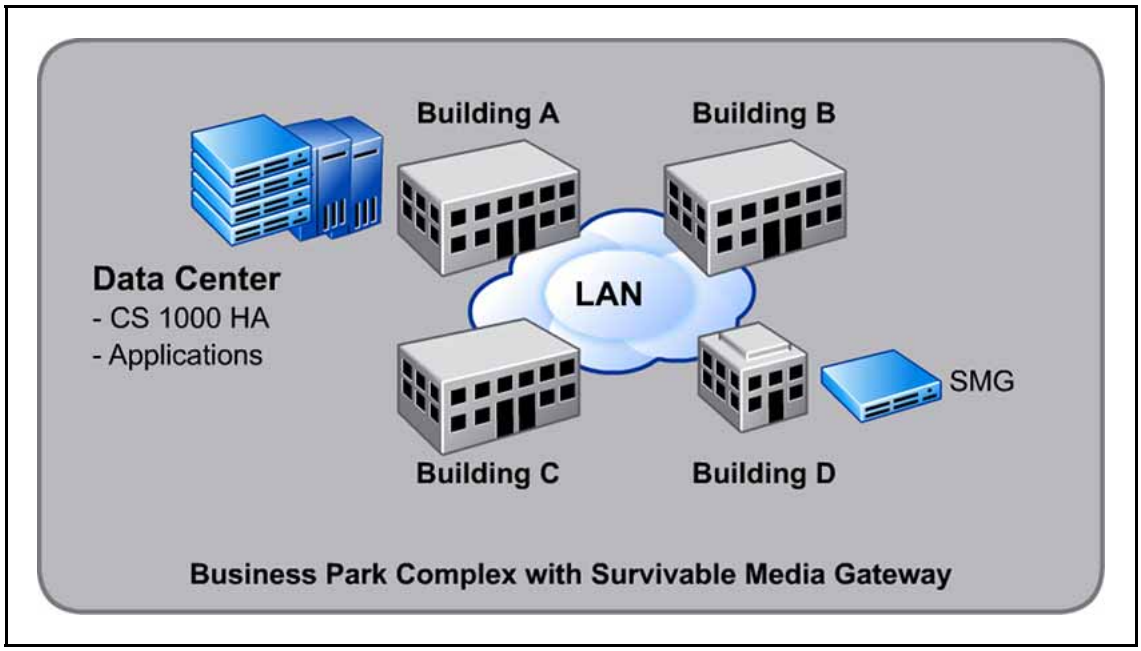
  — *CS1K - How to shut down system gracefully Recovery Training Video*

  — *Call Reception Information Recovery Training Video*

  — *Enterprise How to use Recovery Trees Training Video*

Survivable Media Gateway (SMG)

The Survivable Media Gateway (SMG) provides continuity of certain voice services in the event of a loss of connectivity with a CS 1000E communications server in the UC Campus Data Center. Within a UC Campus environment, the SMG may be deployed in any building where maintaining the continuity of voice services is especially important, such as shown in the following figure:



For troubleshooting purposes, the SMG is basically a Nortel CS 1000E configured to serve as a media gateway. The SMG at a building site must include:

- a CPPM-based call server
- a CPPM-based terminal proxy server (TPS)
- other resources (for example, media gateway cards, PRI trunks, and so on), according to site-specific UC design requirements

To establish a troubleshooting baseline for comparison to a normally operating SMG, the operational model for the SMG is for IP telephones to register with the SMG in the same building, and then to be redirected to the CS 1000E HA for normal services. Upon detecting a loss of connectivity between the local SMG and a CS 1000E, IP telephones attempt to re-register with their local SMG, thereby maintaining access to key or critical voice services at that local site. For example, even with a loss of connectivity to the CS 1000E at Building A in the preceding figure,

users in Building D can still make calls within their building and external to their building by means of PSTN access. (This example assumes that the Campus design included provisions for external trunks to be available at Building D.)

When connectivity to the CS 1000E (HA) has been restored, IP telephones registered with their local SMG now re-register with the Data Center CS 1000 to reestablish access to full voice services.

At least one ERS 5200 or ERS 5300 is required to complete the SMG connection to the main Data Center infrastructure. The choice of using a standalone switch, cluster, or stack depends on what the customer required in the original site design for ports and/or resiliency at the SMG site.

eTelemetry Locate911

For an overview of the eTelemetry Locate911 service within the UC Campus environment, see the publication, *Nortel Unified Communications Campus Fundamentals*, NN49000-100.

For information about how to troubleshoot the eTelemetry Locate911 software and hardware, contact the eTelemetry business partner support organization, at http://www.etelemetry.com/partners/ .

If you need to escalate your e911 problem for resolution, you can also open a "trouble ticket" with the eTelemetry support organization, at: http://www.etelemetry.com/support.aspx.

Security

UC Campus security may occasionally require troubleshooting in these areas:

Endpoint security

Endpoint security -- The Nortel Secure Network Access Switch interoperates with UC campus edge switches to provide end-station authentication, end-node compliance enforcement, and network access controls to any switch port within the UC campus infrastructure. These components allow users access to the UC Campus network, and to PC and VoIP services. Troubleshoot endpoint security when users are unable to access the UC Campus network or one or more of the services they have authorization to use. Problems may exist with the Secure Network Access Switch or UC Campus edge switches, in any of the following areas:

- Interoperation between a Secure Network Access Switch and UC Campus edge switches.
- Configuration of Red/Yellow/Green VLANs (for PC data filtering only)
- Configuration of VoIP data filtering

For more information on how to troubleshoot the SNAS, see *Nortel Secure Network Access Switch Troubleshooting* (NN47230-700).

Voice and application security

Voice and applications security -- UC Campus uses the Nortel Application Switch (NAS) to protect the Secure Media Zone (SMZ) and the following voice components and applications that are in the SMZ:

- Communication Server 1000E
- CallPilot (excluding MyCallPilot webserver)
- Locate 911
- Contact Center
- Contact Recording and Quality Monitoring

Troubleshooting may be required if the functionality or access to any of the above components or applications appears compromised.

For example:

- Misconfigured NAS white-list filters. The filters should identify and allow into the SMZ only traffic associated with voice and related applications signaling, management, server access, and telephony network infrastructure.
- Misconfigured or compromised Denial of Service (DoS) protection provided by the NAS.

  For information on how to troubleshoot NAS operation, see *Nortel Application Switch Operating System Troubleshooting Guide* (NN47220-700). This document describes the diagnostic tools available for the Nortel Application Switch Operating System including the Application Switch Element Manager (ASEM) and the Command Line Interface (CLI).document
- The Locate911 service fails to connect a user to emergency services or fails periodic usage testing, pointing to interoperation or access problems with any of the following: the CS 1000E call server, the Locate911 component or its configuration, the LDAP subscriber server/database, DHCP for discovery of IP phone addresses, or an IP phone.

  For information about troubleshooting E911, contact Etlemetry. Contact information can be found on the ETelemetry webpage at: http://www.etelemetry.com/contact.aspx

After After using CA eHealth (optionally) and NetIQ to identify a problem related to UC Campus endpoint or voice/applications security, use the following additional UC management tools for extended component-level troubleshooting:

- Nortel Enterprise Common Manager (ECM) -- Common Management interface for the CS 1000 Element Manager, Telephony Manager WebUI, and Enterprise Subscriber Management
- Nortel Telephony Manager (TM) -- Management suite for configuration, control, and analysis of the Communication Server 1000.
- Nortel Subscriber Manager (SM) -- Provides a centralized location for managing subscribers and their accounts (phone services) within a network.
- Nortel Application Switch Element Manager (ASEM) -- Software wizards used to configure Application Switching

Unified Messaging

The Unified Communications Campus Solution provides two options for Unified Messaging:

- Nortel CallPilot
- Microsoft Exchange Unified Messaging

Use the following management tools for extended component-level troubleshooting of CS 1000 device configuration and performance issues related to either of the Unified Messaging options:

- Nortel Enterprise Common Manager (ECM) -- Common Management interface for the CS 1000 Element Manager, Telephony Manager WebUI, and Enterprise Subscriber Management
- Nortel Telephony Manager (TM) -- Management suite for configuration, control, and analysis of the Communication Server 1000.
- Nortel Subscriber Manager (SM) -- Provides a centralized location for managing subscribers and their accounts (phone services) within a network.
- Nortel Application Switch Element Manager (ASEM) -- Software wizards used to configure Application Switching

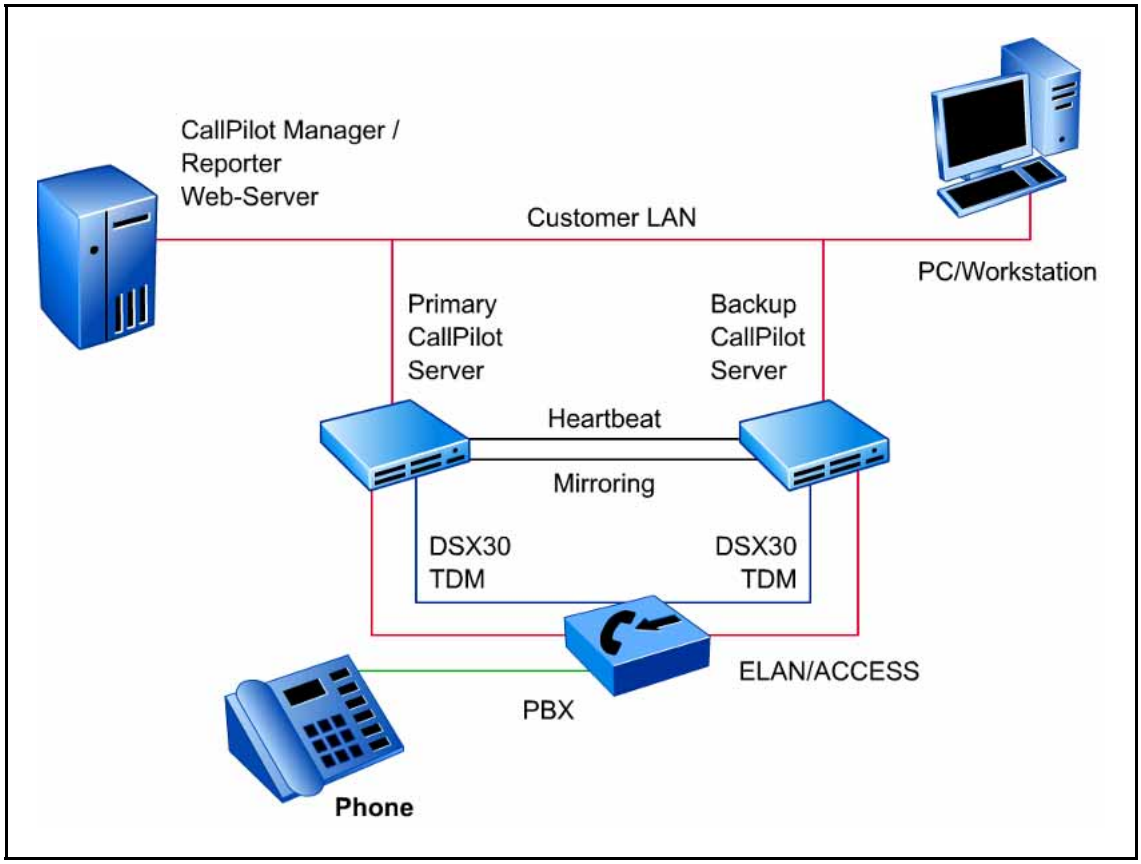
For more information about the UC Campus options for Unified Messaging, see the publication, Nortel Unified Communications Campus Fundamentals, NN49000-100.

Nortel CallPilot

Nortel CallPilot supports the following messaging capabilities:

- Web / My CallPilot
- Answering and routing incoming calls to extensions and mailboxes
- Telephone interface
- Integrated email client
- Internet (IMAP) email client
- Email
- Fax messaging
- Speech Activated Messaging, including email by phone
- Remote notification for pagers, PDA, cell phone, mobile email

The figure below shows the components you may need to troubleshoot in support of these capabilities.



Nortel offers CallPilot troubleshooting documentation and training, and you can obtain access to CallPilot Recovery Trees (symptom-based flow diagrams), as described in the list below. Specifically, some primary Nortel CallPilot troubleshooting resources are as follows:

- Documentation: *CallPilot Troubleshooting Reference Guide*, NN44200-700 -- Describes symptoms that can appear on all CallPilot server platforms, and provides step-by-step troubleshooting procedures. The troubleshooting procedures can be slightly different for different CallPilot releases. Each troubleshooting area contains symptom tables outlining basic checks that include diagnostics and resolutions for each check. This guide is applicable to all CallPilot servers. The exceptions are noted for each server, where necessary, in the heading for each symptom or check.
- Training: Support Expert (NCSE) NCSE - CallPilot Rls. 5.0 -- Includes the following certification courses:
  - *CallPilot Rls. 5.0 Upgrades & System Troubleshooting*, 922-080 -- Includes the following modules: "CallPilot Upgrades and Platform Migrations", "Troubleshooting the CallPilot Server

Platform", "Troubleshooting Switch Interactions with the CallPilot System","Troubleshooting IP Network Interactions with the CallPilot System", and "Securing the CallPilot System"

— *CallPilot Rls. 5.0 Networking*, 922-081 -- Includes the following modules: "Engineering", "Configuration", "Security", "Administration and Maintenance", and "Troubleshooting"

- Recovery Trees: Nortel Business Partners can go to the 30MSR website, click "Recovery Tree Repository", and then open the CallPilot/MPS/Contact_Center folder.
- Recovery Training Videos (RTVs) -- Describe recovery methods used by Nortel's Emergency Recovery team to resolve network outages. The following RTVs are available for CS 1000E:
  - CallPilot Outage Data Collection
  - *CallPilot 5.0 Microsoft RDC*
  - *CallPilot Win32 Time Service*
  - *CallPilot Backup*
  - *CallPilot Unauthorized Software*
  - *CallPilot Patching*
  - *CallPilot KVM Switchboxes*
  - *Call Reception Information*
  - *CallPilot Anti-Virus*
  - *CallPilot Boot IPSEC Error*

Microsoft Exchange UM

Microsoft Exchange Server 2007 integrated with the Nortel CS 1000 call server provides a reliable messaging system including email, voice mail, FAX, calendars, and contacts, all accessible from a wide variety of devices and locations. Specific features that you may need to occasionally troubleshoot include:

- Subscriber access, including:
  - Listen to, forward, or reply to email messages
  - Listen to calendar information
  - Access or dial contacts stored in global address or Personal contact lists
  - Accept or cancel meeting requests

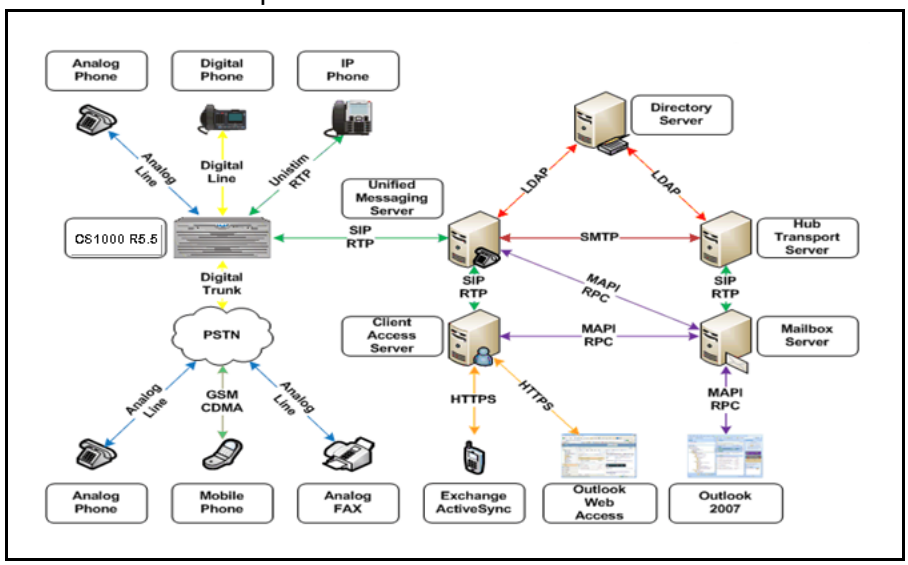
— Set a voice mail Out-of-Office message

— Set security preferences and personal options

- Auto Attendant
- Play on Phone

Exchange UM also provides integrated protection from spam and viruses.

The following figure shows the components, messaging protocols, and links that you may need to troubleshoot in support of UM messaging capabilities:



Nortel offers the following course in support of troubleshooting the messaging infrastructure shown in the preceding figure:

Implementing, Troubleshooting, Maintaining MS Exch Server 2007 Infrastructure, GK7006 -- Shows how to configure and manage a messaging environment in accordance with technical requirements, provide messaging specialists with the knowledge and skills needed to manage messaging and connection security, and recover Exchange mailboxes and servers in a variety of disaster scenarios. This course combines content from three separate Microsoft courses (M5047, M5049, and M5050).

REVIEWERS NOTE: Livelink only shows the above offering in Europe, Middle East, and Africa. Does Nortel support the companion course in North America and other locations? If not, can the course be adopted and delivered in North America and other locations?

The following additional troubleshooting resources are available outside of Nortel:

- Microsoft TechNet Exchange Server TechCenter website, at:

  — http://technet.microsoft.com/en-us/exchange/default.aspx

  Select "Troubleshooting" from the website menu bar.

- Microsoft Learning website: Workshop 5051A: "Monitoring and Troubleshooting Microsoft Exchange Server 2007", at:

  — http://www.microsoft.com/learning/en/us/syllabi/5051a.aspx

- Troubleshooting reference: *Microsoft Exchange Server 2007: The Complete Reference*, by Richard Luckett, Bharat Suneja, and William Lefkovics

Voice applications

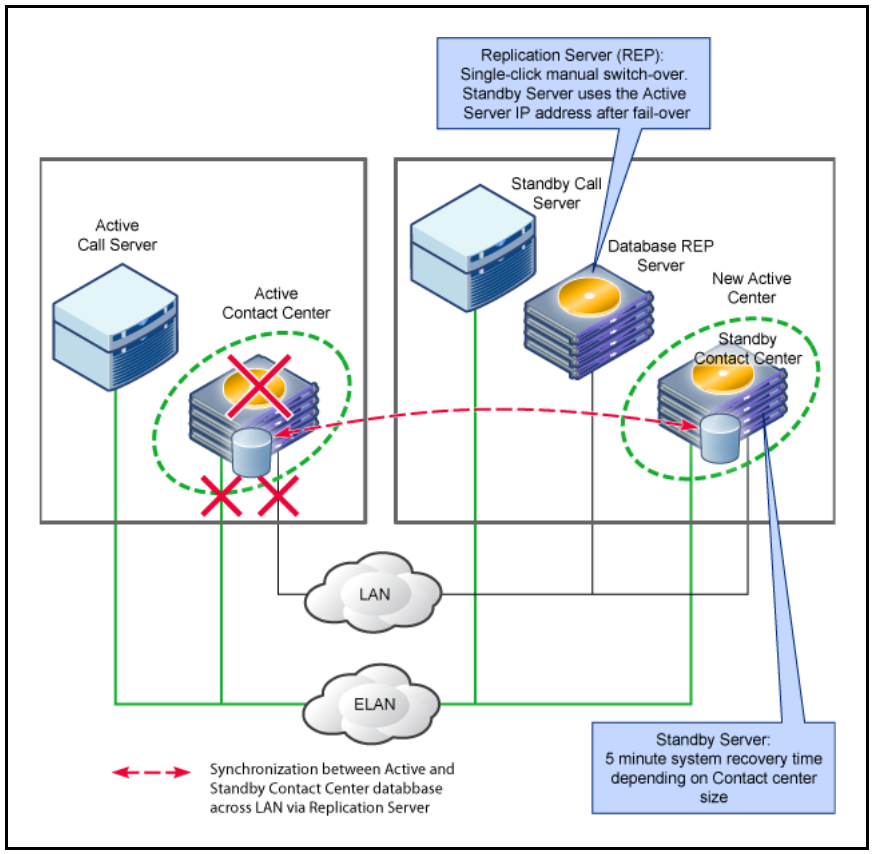
The UC Campus voice applications that you may need to troubleshoot occasionally are:

- “Contact Center and Contact Recording” (page 92)
- “Converged Office” (page 94)
- “Nortel Multimedia Conferencing (NMC)” (page 96)

Contact Center and Contact Recording

Contact Center (CC) is an optional software solution running on a customer supplied Windows Server 2003 that meets defined PVI (Platform Vendor Independence) specifications. This Contact Center Manager Server (CCMS) supports call routing and treatment decisions based on combinations of real time conditions. The UC Contact Recording service automatically (by default) records all calls to the Active Contact Center.

For troubleshooting purposes, the following figure shows the architecture of UC Campus components supporting these applications:



Nortel offers documentation, training, and recovery tree resources for troubleshooting the Contact Center and Contact Recording applications. See:

- “CS 1000 documentation” (page 81)
- “CS 1000 training” (page 82)
- “Recovery trees” (page 94)

Documentation

The following documents describe how to troubleshoot the Contact Center.

- *Nortel Contact Center Troubleshooting* (NN44400-712)

  This document describes the fundamental concepts and procedures required to troubleshoot the server software in Contact Center.

- *Contact Center Manager Server (CCMS): Windows Services Changing Server Time Can Result in Calls Defaulting* (2007008438)

  This bulletin addresses the situation when CCMS is used in the Communication Server 1000/Meridian 1 environment you must disable all time synchronization features of the operating system to avoid potential call processing outages.

- *Contact Center License Manager 6.0 experiences Grace Period count down and potential outages* (2008008789)

  This bulletin addresses the Grace Period that occurs in the event of a communication error between the Contact Center Manager Server and the License Manager.

Training

Recovery Training Videos (RTVs) describe recovery methods used by Nortel’s Emergency Recovery team to resolve network outages. The following RTVs provide troubleshooting information for the Contact Center.

- Contact Center License Manager Recovery Training Video
- Contact Center License Manager Recovery Training Video
- Contact Center Manager Server CCMS Patching Recovery Training Video
- Contact Center Manager Server CCMA Patching Recovery Training Video

Recovery trees

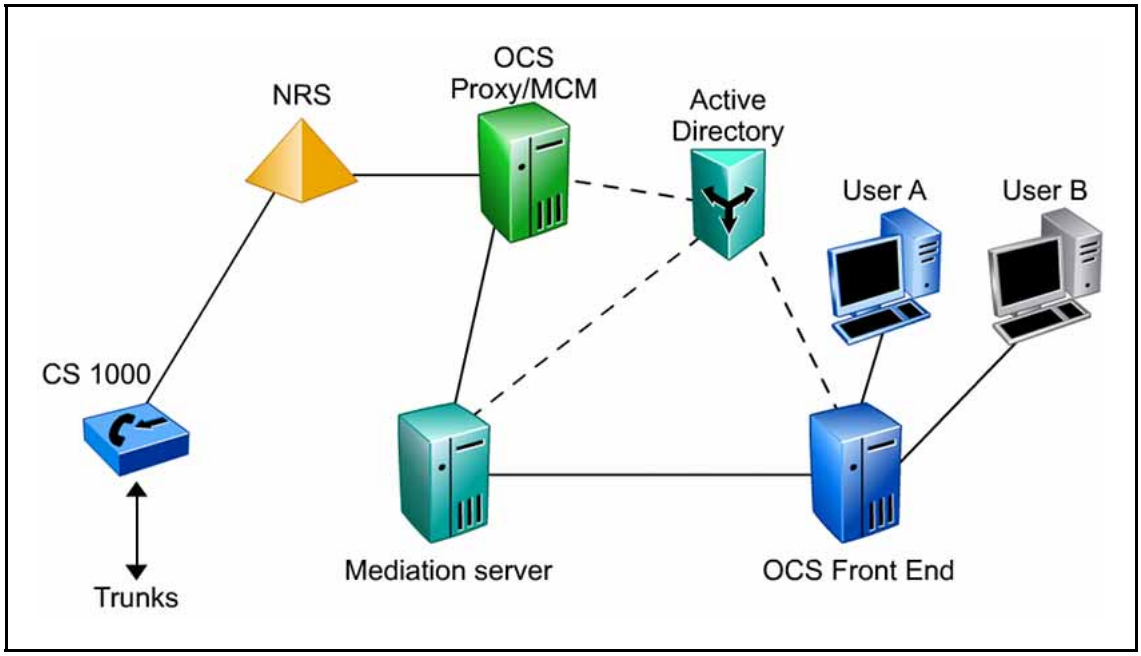
Nortel Business Partners can access Contact Center and Contact Recording Recovery Trees at http://navigate.us.nortel.com/imds?pg=/ss/cs/30msr/process/recovery. From that location, click "Recovery Tree Repository", and then open the CallPilot/MPS/Contact_Center folder.

Converged Office

The Converged Office solution integrates the business-grade telephony of the Nortel CS 1000 with the Microsoft OCS 2007 Enterprise Voice solution. Converged Office capabilities that you may occasionally need to troubleshoot include:

- Remote call control (RCC) with Session Initiation Protocol Computer Telephony Integration (SIP CTI) (TR/87) provides full Microsoft Office telephony integration to control business-grade telephony phones from within Microsoft Office applications, as well as support for a standards-based CTI interface defined by the TR/87 protocol.
- Telephone gateway and services (TGSV) provides a basic SIP Telephony Gateway to connect between Private and Public Telephony networks and OC 2007 clients.
- Telephony services (TLSV) extends to OC clients many features provided by the Nortel CS 1000 to traditional telephones.

The following figure shows the components you may need to troubleshoot in support of these capabilities:



Nortel offers the following resources for troubleshooting Converged Office deployments:

- Message flows: Diagrams associated with setup and teardown of the many different call scenarios supported by the Converged Office solution are helpful for troubleshooting from a normal-operation baseline, knowing which components should send and receive specific messages at each stage of call progress. These diagrams are available on request through Nortel Global Services.
- Documentation: *Nortel Communicaton Server 1000 Release 5.5 support for OCS 2007 Release 2*, 2009009453, Rev 2 -- For troubleshooting purposes, this technical bulletin provides important details for customers deploying Nortel Communication Server 1000 (CS1000) Release 5.5 configured for interoperability with Microsoft Office Communication Server 2007 Release 2 (OCS R2). This bulletin describes the requirements for interoperability between CS1000 Release 5.5 and Microsoft OCS 2007 R2 Converged Office. This is key information to use when comparing current setup to baseline requirements in a troubleshooting scenario. (Information for a Direct SIP configuration between CS1000 Rls. 5.5 and OCS 2007 R2 is not included in this version of the document.) This bulletin also describes the required software versions for MCM, CS1000 and related components as well as the Product Enhancement Packages (PEPs) that must be installed to facilitate interoperability with Microsoft OCS 2007 R2.
- Training: *Nortel Unified Communications: Converged Office*, 6367C -- An iLearning course designed for Communication Server 1000E technicians responsible for the integration of the Nortel Communication Server 1000E 5.5 and the Microsoft Office Communications Server (OCS) 2007. This course provides an Introduction to the Nortel Converged Office, Features, System Components, and Deployment Options, as well as Maintenance and Troubleshooting Procedures for the Solution

External to Nortel, Global Knowledge, Inc. (www.globalknowledge.com) also offers the following certification program with Converged Office troubleshooting orientation: *NCSE - Nortel Unified Communications - Converged Office for CS 1000 Rls. 5.x Configuration*, covering:

- Deploying the Nortel Converged Office Solution
- Integrating the CS 1000E with the OCS 2007
- Telephony Integration with the CS 1000E Rls. 5.x

- Unified Communications End User Devices
- Maintenance and Troubleshooting
- Dialing Plan Design & IP Peer Networking

Nortel Multimedia Conferencing (NMC)

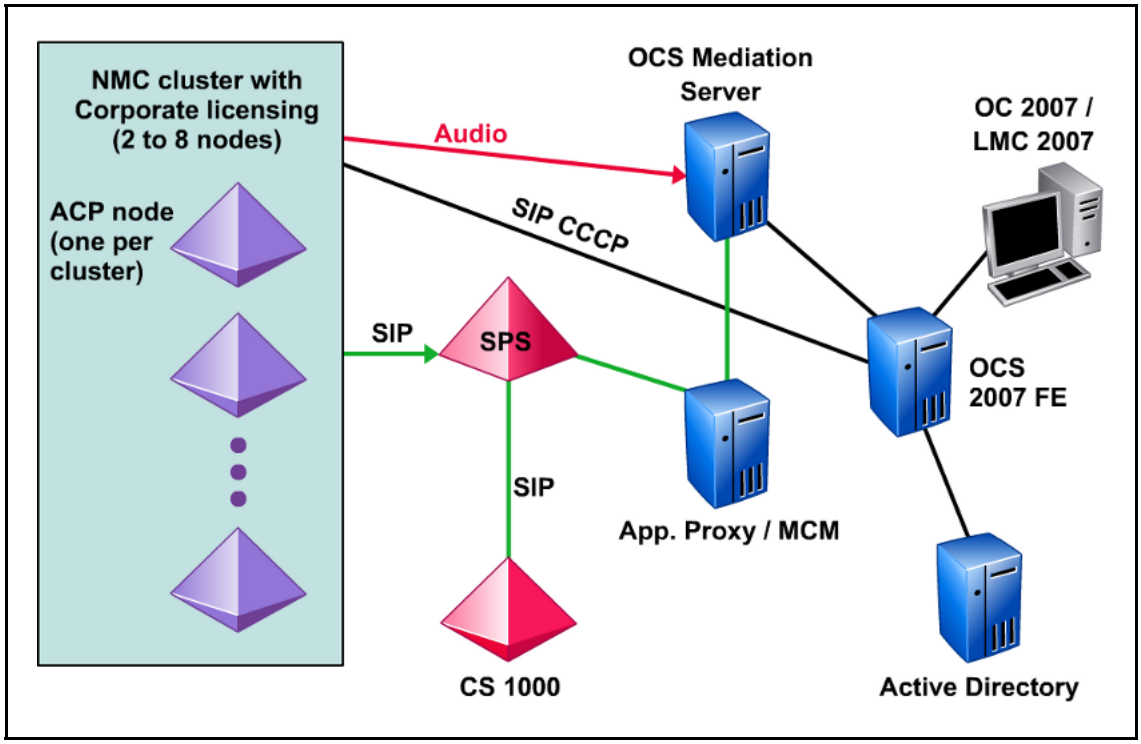
UC Campus provides the option to use the Nortel Multimedia Conferencing (NMC) solution for in-house reservationless audio conferencing. NMC runs on the Nortel Media Application Server (MAS) 5.1 platform, and provides subscribers with access to an always-on multimedia conferencing resource.

NMC services integrate with Microsoft OCS 2007 components, extending the Unified Communications environment to OCS users. NMC provides the following additional capabilities through Microsoft Office Communicator (OC) 2007:

- Instant Messaging
- Web collaboration
- Videoconferencing

Participants in a conference must use Microsoft Live Meeting Console (LMC) 2007 to access collaboration features available with NMC (for example, starting a conference, video, or chat session).

The following diagram shows the components that you may occasionally need to troubleshoot in support of these features.



For troubleshooting purposes, the NMC solution running on the Media Application Server (MAS) platform supports:

- Comprehensive report generation capabilities
- Alarms and logs
- Fault and performance management features

See the following documentation resources to aid in troubleshooting NMC conferencing capabilities:

- *Solution Integration Guide for NMC/CS 1000 and NMC/Converged Office*, NN44460-300 -- Describes the planning, configuration, and troubleshooting of the integration of Communication Server 1000 (CS 1000), with Nortel Multimedia Conferencing (NMC) and, optionally, Live Communication Server (LCS) 2005 or Office Communications Server (OCS) 2007 systems.
- *Nortel Multimedia Conferencing Logs*, NN44460- 700 -- Provides a listing of NMC logs with details about severity, type, explanation, and recovery action.
- *Nortel Media Application Server 5.1 Alarms and Logs* NN44450-702 -- Provides a listing of MAS alarms and logs with details about severity, type, explanation, and recovery action

- *Nortel Media Application Server 5.1 Fault Management*, NN44450-700 -- Provides information about MAS alarms, event logs, and troubleshooting
- *Nortel Media Application Server 5.1 Performance Management*, NN44450-701--Provides information about statistics, operational measurements (OMs), and reporting features of the MAS platform.
- *Nortel Media Application Server Troubleshooting*, NN44471-703 -- Covers troubleshooting-related topics such as:
  - Call Completion Failures
  - Element Manager
  - Email Delivery
  - Emergency recovery trees
  - Enterprise Common Manager
  - Reporting
  - Security
  - SIP
  - SNMP

Nortel Unified Communications Campus Solution

Troubleshooting

Release: 1.0
Publication: NN49000-700
Document revision: 01.01
Document release date: 29 May 2009

All other trademarks are the property of their respective owners.

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com