

OUR 15TH YEAR

PACKET

CISCO SYSTEMS USERS MAGAZINE

THIRD QUARTER 2003

Wireless LANs 30

Going Mobile
in a Big Way

9 IP Telephony
Troubleshooting

19 All About Tunnels

27 Identity-Based
Networking

53 **Special Report:**
High Availability—Define It,
Measure It, Improve It



Tech Tips & Training

IP Telephony Detective

Developing a Troubleshooting Methodology for Cisco IP Telephony

BY PAUL GIRALT

IN A PERFECT WORLD, NETWORKS would diagnose problems for you, tell you the root cause, and resolve problems automatically. In the real world, problems arise and it is up to you to troubleshoot and bring them to resolution. IP telephony networks are particularly challenging to troubleshoot because they involve a wide range of components that work as a system to provide voice and data services. When troubleshooting a problem, you should employ a solid methodology for dividing the problems into smaller, manageable components and investigate each one until you find the root cause.

Troubleshooting problems can be broken down into two stages: *data gathering* and *data analysis* (although your analysis might lead you to collect additional data). Generally, these two stages encompass the following:

1. Gather data about the problem:
 - a. Identify and isolate the problem.
 - b. Use topology information to isolate the problem.
 - c. Gather information from end users.
 - d. Determine the problem's timeframe.
2. Analyze the collected data:
 - a. Use deductive reasoning to narrow the list of possible causes.
 - b. Verify IP network integrity.
 - c. Determine the proper troubleshooting tool(s), and use them to find the root cause.

Sometimes, several service-affecting problems occur simultaneously. In fact, this is not uncommon because multiple problems often manifest themselves as symptoms of the same root cause. When multiple problems occur simultaneously, focus on the problem that has the greatest impact on users. For example, if some users are reporting dropped calls and others are reporting occasional echo, the two problems are probably

unrelated. Troubleshoot the dropped-call problem first, because keeping calls connected is more critical than removing the occasional echo on an active call.

Stage 1: Gather Data About the Problem

Half the battle in troubleshooting a problem is determining which piece of the puzzle is the source of the problem. With so many different components to an IP telephony network, the first step is to isolate the problem and, if multiple problems are being reported, determine which of them might be related to each other.

Identify and isolate the problem. You must determine which parts of the problem are symptoms and which are the root cause of the problem. For example, if a user complains of an IP phone resetting itself, it's logical to assume that something is wrong with the phone. However, the problem might lie with Cisco CallManager or one of the routers and switches that make up the underlying data network. So, although the symptom is a phone reset, the root cause could be a WAN outage or CallManager failure.

Always remember to look at the big picture when searching for the root cause and not let the symptoms of the problem steer you in the wrong direction. To help you visualize the big picture, detailed topology information is essential.

Use topology information to isolate the problem. One of the first lines of defense in the troubleshooting process is possessing current topology information. One of the most important pieces of topology information is a detailed network diagram, which should include network addressing information and the names of all the devices. It should also clearly show how the devices are interconnected and the port numbers used for the interconnections.

In addition to a network diagram, you should use some method to store information such as IP address assignments, device names, and password information. For a small network, you can use something as simple as a spreadsheet or even a plain text file. For larger deployments, a database or network management application, such as CiscoWorks, is recommended.

You also need documentation of your dial plan. Some deployments—especially those heavily using toll bypass—have very complex dial plans. Knowing where a call is supposed to go just by knowing the phone number and from where it is dialed helps you quickly understand a problem.

When your topology information is complete, it should include all the following information:

- Interconnection information for all devices, including device names and port numbers. If any patch panels exist between devices, the port numbers should be listed.
- IP addressing for all network devices (routers, switches, and so on)
- IP addressing for all telephony and application servers and voice gateways (including data application servers)
- IP addressing for endpoints; that is, scopes of a Dynamic Host Control Protocol (DHCP) pool
- WAN and PSTN service provider names and circuit IDs for each circuit
- Spanning-tree topology, including root bridges for all virtual LANs (VLANs) and which ports should be forwarding and blocking
- Dial plan information
- Software version information for all devices

If you are troubleshooting a network you didn't design, topology is one of the first pieces of information you should obtain, if it is available. If it is not available, obtain

the information from someone who is familiar with the network, and then make a quick sketch. A general topological understanding of the network, or at least the piece of the network in question, helps when you are trying to differentiate the problem from its symptoms.

What is worse than not having topology information? Having *incorrect* topology information can lead to countless hours heading down the wrong path. If you are going to keep topology information, make sure it is updated often.

Use all the topology information you have to narrow down which pieces of the network might be involved in the problem you are troubleshooting. To further isolate the problem, interview the end users who reported the problem to gather additional information.

Gather information from end users.

The more detail about the problem you can gather before you begin troubleshooting, the easier it is to find a resolution—and that means less frustration for you. Here is some information you should collect from users:

- Details about exactly what the user experienced when the problem occurred
- Phone numbers for all parties involved in the problematic call or calls (you can use this as search criteria if you need to look through traces)
- Actions performed by the user when the problem occurred, including which buttons were pressed and in what order
- End-user observations, including text messages displayed on the phone or recorded announcements
- Information about the user's device. For example, if the user experienced a problem while using a Cisco IP Phone 7960, get the phone's MAC address and IP address, along

PAUL GIRALT is an escalation engineer with the Cisco Technical Assistance Center (TAC) in North Carolina and trains TAC teams around the globe. He has been troubleshooting complex IP telephony networks since Cisco CallManager release 3.0, and has resolved problems for some of the largest Cisco IP telephony deployments. Co-author of the Cisco Press book *Troubleshooting Cisco IP Telephony* (ISBN: 1-58705-075-7), Giralt holds a bachelor's degree in computer engineering from the University of Miami, Florida. He can be reached at pgiralt@cisco.com.

with registration information and any other statistics available from the phone.

The information provided by end users might not be enough to even begin troubleshooting. Sometimes the proper diagnostic tools are not enabled when the problem occurs, forcing you to ask the users to inform you the next time the problem occurs. Be sure to turn on tracing or debugs before making the request so that when the problem occurs again, you will capture the data. Also, point out to users the importance of letting you know immediately when a problem

Always remember to keep the IP network in mind and look at every layer in the OSI model, starting from Layer 1. Check your physical layer connectivity. . . . Then make sure you have Layer 2 connectivity by checking for errors on ports, ensuring that Layer 2 switches are functioning properly, and so forth.

occurs, as many of the diagnostic trace files overwrite themselves within several hours or days (depending on the amount of traffic on your system).

Determine the problem's timeframe. In addition to *what* the problem is, you should try to determine *when* the problem occurred. Determining the earliest occurrence can help correlate the problem with other changes that might have been made to the system or other events that occurred around the same time, such as scheduled maintenance windows or known network outages.

If relying on end users to provide the "when" information, ask them to note the time on their IP phone when the problem occurred. The phone's time should be synchronized with the clock on the Cisco CallManager to which the phone is registered. As long as you have your CallManager servers and network

devices time synchronized, getting a phone-based time from the user makes finding the proper trace files very easy.

Time synchronization throughout your network is vital to troubleshooting problems, especially when many devices are involved. For example, a call could traverse several CallManager servers, interactive voice response (IVR) servers, voice-mail systems, and gateways—each of which has its own clock to write timestamps to the log files. The best way to synchronize the devices in your network is to use the Network Time Protocol. To find out more about this topic, see "How to Configure Time Synchronization for Cisco CallManager" at cisco.com/packet/153_4a1.

Although it is important to use information about when the problem started happening, it is equally important to not assume that the problem was a direct result of an event. For example, if a user reports a problem the day after an upgrade was performed on CallManager, the upgrade might have caused the problem—but you should not automatically assume that this is the root cause.

**Stage 2:
Analyze the Collected Data**

Now that you have collected data from a variety of sources, you must analyze it to find the root cause and workaround for your problem.

Use deductive reasoning to narrow the list of possible causes. The next part of your fact-finding mission is to identify the various components that might be involved and to eliminate as many of them as possible. The more you can isolate the problem, the easier it is to find the root cause.

Although not all of the following factors apply to every problem, where applicable, you must check the following pieces involved in the call. You can use your topology information to help obtain this information.

- Cisco CallManager nodes involved in the signaling
- Network devices that signaling, voice traffic, or both traverse
- Gateways or phones involved in the call

Continued on page 12

IP Telephony Troubleshooting, Continued from page 10

Methodology for Troubleshooting Cisco IP Telephony



Troubleshooting Cisco IP Telephony: A Cisco AVVID Solution from Cisco Press lays out the methodology you need to identify and resolve complex problems in an IP telephony network. Written by Paul Giralt, Addis Hallmark, and Anne Smith, the book provides comprehensive coverage of all parts of a Cisco IP telephony solution, including Cisco CallManager, IP phones, gateways, analog devices, database and directory replication, call routing, voice mail, applications, network infrastructure, and more.

You'll learn how to read trace files and when to turn on tracing, IOS voice debugging, and how to troubleshoot voice quality issues. The book also shows you how to

break down problems to find the root cause.

Descriptions of each part of a Cisco IP telephony solution are provided, to help you in understanding the functionality of each part, how each part interacts with other parts in the solution, and what steps to take and tools to use to identify and resolve the cause of a problem.

Troubleshooting Cisco IP Telephony (ISBN: 1-58705-075-7) is available at online booksellers such as Amazon.com, local bookstores, computer and electronics superstores, and other venues where computer technology books are sold. For information on corporate bulk or education purchases and sales outside the US, visit ciscopress.com/sales.

- Other devices involved, such as conference bridges or transcoders

Concentrate your energy on the smallest subset of devices possible and try to find a commonality to multiple users' problems. For example, if all the users on a particular floor are having the same problem, concentrate on the problem one user on that floor is having and determine which device in the network the users share that might be causing the problem. If you fix the problem for that one user, in most cases you will fix it for all the affected users.

Verify IP network integrity. Remember that your IP telephony network is only as good as your IP network. A degraded network or a network outage can cause a wide range of problems, from slight voice quality degradation to a total inability to make or receive calls on one or more phones.

Network health is especially important when troubleshooting voice quality problems because most voice quality problems

stem from packet delay and/or loss due to network congestion or degradation.

Always keep the IP network in mind and look at every layer in the OSI model, starting from Layer 1. Check your physical layer connectivity (cables, patch panels, fiber connectors, and so on). Then make sure you have Layer 2 connectivity by checking for errors on ports, ensuring that Layer 2 switches are functioning properly, and so forth.

Determine the proper troubleshooting tool. After you narrow down the appropriate component(s) potentially causing the problem and have detailed information from the user(s) experiencing the problem, you must select the proper troubleshooting tool or tools. Use the tracing and debugging facilities available in Cisco CallManager and other devices to determine exactly what is happening.

Because CallManager is central to almost all problems, you will typically want to look at a Cisco CallManager (CCM) trace file on the CallManager(s)

involved in the problem call. This step is the most demanding on your troubleshooting skills, because you analyze the detailed information provided in the various tools and use it to search for additional clues using other tools.

Some tools you can use to troubleshoot problems in an IP telephony network include the following:

- CallManager trace files: CCM, Signal Distribution Layer (SDL), computer telephony integration (CTI), and so on
- Application server trace files (MIVR, JTAPI)
- IOS® Gateway **debug** and **show** commands
- Q.931 Translator
- Dick Tracy Utility (for troubleshooting WS-X6608 and WS-X6624 gateways)
- Call detail records
- Microsoft Performance (PerfMon) or CallManager Serviceability's Real-Time Monitoring Tool
- Network Packet captures (Sniffer Pro, Ethereal, for example)

Remote Access to All Devices

To make troubleshooting your network as easy as possible, ensure you have remote access to all the devices on your network. Use either Secure Shell (SSH) or Telnet to access routers and switches. Enable Windows Terminal Services or Virtual Networking Computing (VNC) on your Cisco CallManager servers and application servers to access them remotely.

If there is a chance that you will have to troubleshoot a problem when you are not on your corporate network, consider adding a virtual private network (VPN) concentrator to your network, which will enable you to connect to the network regardless of where you are.

◆ ◆ ◆

When troubleshooting IP telephony problems, remember to first put on your detective hat and gather enough information to isolate the problem to a few components of the system. Then dig deeper into each component by dividing the problem into more manageable pieces. Finally, apply your expertise to each of these smaller pieces until you find the resolution to your problem. ▲▲