50 Broadway, Suite 1205
New York, NY 10004
Tel 212-221-0057
www.r-rtele.com

Call Troubleshooting Guide

Information for this article was compiled from multiple sources including an unknown article found at: http://www.the-crankshaft.info/2010/02/familiarizing-yourself-with-wireshark.html

Table of Contents

Troubleshooting Basics

- Getting the troubleshooting basics
- Figuring out a call problem's category and frequency
- Finding patterns in the frequency, geography, and time of day of a problem
- Defining your troubleshooting responsibility
- Troubleshooting logically

You'll spend far more time troubleshooting and maintaining your VoIP network than you did preparing to deploy it. This period of time represents the final stage in VoIP Lifecycle Management and is punctuated by bursts of extreme stress and frustration in a landscape of otherwise mundane maintenance and review. I guarantee that, one day, all the planets will come into alignment, and it'll seem like every telecom catastrophe that could possibly happen is happening.
Troubleshooting doesn't need to be painful or frustrating, as long as you have a plan. This topic gives you that plan and the standard rules of engagement necessary to reduce the impact of any problem on your network and your company. Keep your cool, use your tools, and you'll be back up and running in no time flat.

Understanding Troubleshooting Basics

Troubleshooting is a process in which you dissect a problem to identify the source of the perceived anomaly, which allows you to take actions to resolve the issues. It seems simple enough on the surface — a call is failing, so you need to find out why and correct it. The challenge comes when you have to decide the course of action to find the problem.
If you've been troubleshooting telephony problems for five or ten years, you may be able to tell the source of a problem before someone even finishes telling you the symptoms. If you haven't been doing it long enough to develop a sixth sense for it, you need a logical progression of tests to run through. Every test you conduct should build on your current information to further narrow down the source of the issue.
You're the beneficiary of a great gift — easy access to the overhead banter between your SIP server and your VoIP carrier. Traditional telephony lines or circuits don't allow you to gather information and pull it apart so easily. They don't have a Wireshark capture that you can download to gather up information in the overhead of your analog phone line or dedicated digital circuit.

Using diplomacy

The first rule of troubleshooting is that you must maintain complete objectivity. There's no better way to delay the resolution of a problem than to start the troubleshooting process with something fixed in your brain that "must be" the source of the problem. The worst part is that the data may

outright refute what you believe the problem is. It's very common to jump to this type of conclusion, but you need to avoid obsessing that the problem must be a calls per second issue, or a carrier routing issue, or anything but your phone system.

In the end, you need to simply read and interpret the data. The data is the one thing in the whole troubleshooting equation that's unbiased and unemotional. Look at the information and pull it apart. It may lead you to one conclusion on Monday and in the opposite direction on Tuesday. Don't take it personally, the test results aren't lying to you, the conclusions drawn previously simply lacked the clarity brought to the issue today.

The main element of the troubleshooting process is people. The people working in the VoIP department for your carrier are nice people, just like you. I can assure you that they don't intend you to have problems, and they genuinely enjoy some aspect of the troubleshooting/repair process. Your carrier's employees are human. They probably react coldly if you come in on a troubleshooting call with guns blazing and an attitude that "you guys are all screwed up." Someone can always find a way to spin a problem and make it "not their responsibility." If you strike up a good relationship with the technicians helping you, they respond to your calls more quickly and go the extra mile to solve your problem. If your conversations with your carrier are generally prefaced by you stating how worthless their network is and rhetorical questions about "why should I stay with you for service?", they avoid you and do their best to throw the blame on your hardware. VoIP is still a relatively new technology, and nobody knows everything about it.

Even if someone knows everything about VoIP today, a whole new realm of VoIP will emerge a few days from now about which he or she hasn't a clue. This fact makes everyone you chat with a potential resource of new information. The more the technicians and support staff like and respect you, the more apt they'll be to show you all the shortcuts and tricks they've figured out over years of working in their specific area of VoIP.

Troubleshooting can be a very emotional event. If you see the emotions getting too heated on a conference call, conclude the call and separate the two people fueling the argument. The main reason troubleshooting calls degenerate is because someone has decided that, whatever the problem is, it absolutely, positively can't be his or her hardware or issue. The finger-pointing mindset doesn't promote an environment in which people can effectively work together. You need to diffuse the situation and still get the requested tests done by following these tips:

Separate the antagonists. End the conference call and act as the neutral third party. It may take a bit

more time for you to relay information from your VoIP hardware vendor and your VoIP carrier, but in the end, it resolves your problem faster.

Tell your VoIP carrier that you know it definitely isn't its issue. Even if every shred of data points to the fact that your VoIP carrier isn't processing the CANCEL request properly or that your software guy has an issue within your Call Plan, you can't tell him that. It might take a day for him to cool down, and you don't have that much time. It's always the most efficient to talk to each person individually and tell him, "I know this isn't your issue, but if you can just do this one test, we can prove that there's nothing in your system causing this problem." The opportunity to prove someone else wrong — and vindicate yourself in the process — is always a much better motivator than being browbeaten or threatened into doing a test.

Identifying the Variables

Troubleshooting a phone call isn't as daunting as it may appear at first glance. The vast majority of the call path happens outside the realm of your LAN, over hardware that you don't own and through switches that you aren't responsible for maintaining. So, the quickest path to resolution is for you to do as many tests as possible to isolate the issue down to the responsible party, get the issue into it hands, and then empower it to resolve it.

Reviewing an outbound long-distance call

Before you can begin troubleshooting any call, you need to isolate the variables. The components of a call vary, depending on whether it's inbound, outbound, local, or long distance. The most common call you probably make is a standard outbound long-distance call.

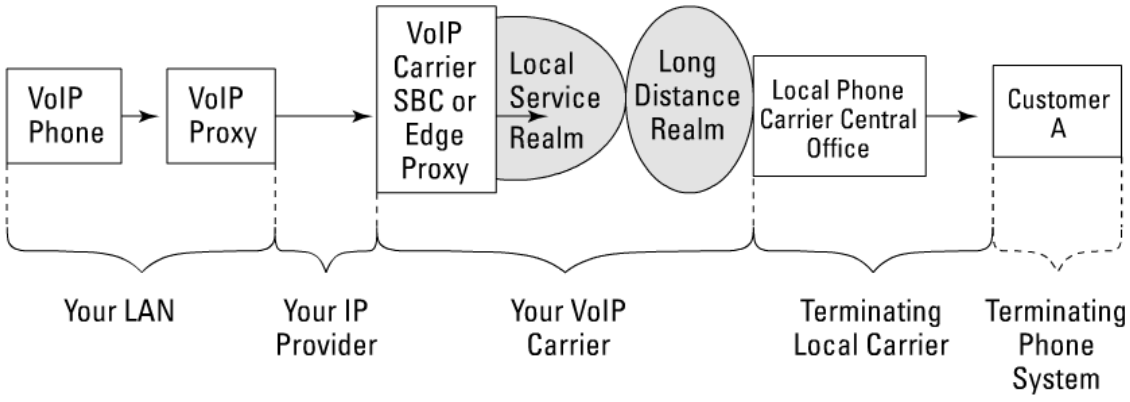


Figure 1: Call variables.

If you want to know all the specifics of what qualifies a call as local, longdistance, outlying area, or international, Telecom For topic, by yours truly (Wiley), covers all this and much more.
Figure 1 shows the five main variables affecting an outbound call that's transmitted via VoIP and terminates to a non-VoIP phone number. Each segment in the call encounters a path for which a different entity is responsible. Starting from the origination of the call, the responsible organizations are

Your company: The call originates from a VoIP phone, traverses your LAN, runs through your VoIP phone system, and finally leaves your responsibility when it's sent from your VoIP server to the SBC of your VoIP carrier. The majority of fluctuations in latency, jitter, and packet loss occur within your VoIP LAN. You need a fully-evolved VoIP Lifecycle Management (VLM) software package to effectively troubleshoot and manage this link in the call chain. I recommend the VLM solutions by Packet Island that are covered in detail in topic 9.

Your IP Provider: It has the simple responsibility of transmitting your packets to arrive at the IP address of your VoIP carrier. It can potentially add latency and jitter to the transmission (sometimes caused by flap), as well as packet loss. It also has responsibility for delivering the packets sent to you in response by your VoIP carrier. Much of those transmissions traverse your VoIP carrier's IP provider, but your IP provider handles the final leg of that journey.

Your VoIP carrier: Your VoIP carrier has the responsibility of receiving the VoIP call, transmitting it through its network, and potentially converting it from VoIP to integrate the call into the PSTN before delivering it to the local phone carrier that provides service to the phone number you dial.

The terminating local phone carrier: The call is processed by the local phone carrier, which identifies the pair of wires belonging to the business or residence to which the phone number is assigned. After it identifies the phone number, the call is routed to ring at the recipient's site.

The destination phone system: The telephone or telephone system of Customer A must ring, answer, route the call to the extension (if necessary) and send the proper signals back through the local carrier to indicate when the call is answered and hung up.
A call can fail because of problems at any point in this chain of events. Packet loss on your LAN or with your IP provider, SIP signaling issues, routing within any carrier along the way, or a bad phone at the far end can all kill a call.

Only the on-ramp to your carrier may be VoIP. Your carrier may convert your VoIP-originated call

to traditional telephony directly after receiving the call. Your call may also be converted to and from VoIP several times during the transmission from end to end. The final leg of the call will probably be analog because most phones in America aren't using VoIP service yet (although the number of residences and small businesses making the switch is climbing).

Figure 1 isn't the only possible scenario for an outbound call. VoIP has been deployed within the network of long-distance carriers for years. Even before they released VoIP products to their customers, they were using VoIP internally. During those early years, many customers connecting into long-distance networks were surprised when troubleshooting issues with their carrier that their traditional telephony circuits were being instantly converted into VoIP after initial connection. The protocol flip-flop may have happened several times, when a carrier's internal network hardware converted the call back to traditional telephony, and then an underlying carrier converted it back to VoIP a second time. In international calls, VoIP is a common technology used to maximize the number of concurrent calls possible over a fixed bandwidth, because the cost of renting the circuit to the country it services is a huge expenditure and the more calls you can push over the same connection, the more money you make.

The good news is that you don't have to concern yourself with the sections of the call that are converted to or from VoIP. Your only focus is isolating an issue to a single company. It's the company's responsibility from that point to work through the complexities of its network and the networks of its underlying carriers.

VoIP technology changes some aspects of the troubleshooting process. Your VoIP provider replaces both the local phone carrier and long-distance carrier that you'd encounter in a normal telephony call. The local and long-distance functions are still separated, even within your VoIP carrier, because different hardware is required to provide local or long-distance service. If you're replacing your local analog lines, the VoIP carrier you select probably has a contract with one or several long-distance carriers to handle all your outbound calls. Even if you're paying a flat monthly rate for your service with no per-minute charges, they're still sending your call out to someone who's charging them a normal cost per minute.

Deconstructing a local call

Call quality issues, such as static, echo, and clipping, can occur at any stage in the call path. One of the easiest ways to eliminate some of the potential variables in the call equation is to see whether the same call quality issue is also present on other types of calls with different variables.

Figure 12-2 identifies the variables of a call to your VoIP phone from a normal analog phone in a neighboring town. The call flows from the analog phone, through its long-distance carrier, into the

local service side of your VoIP carrier, and finally to your VoIP LAN.

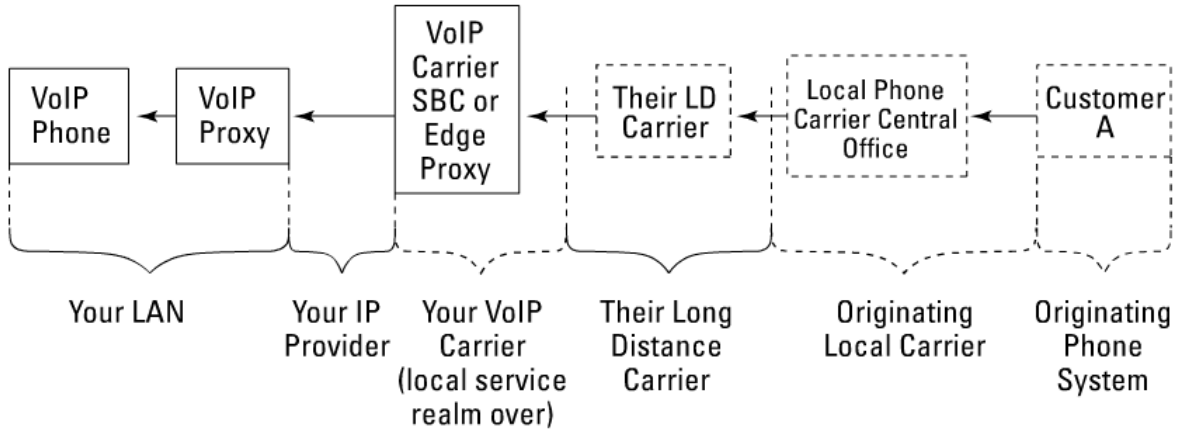


Figure 2: An inbound long-distance call.

You can use the two call types represented in Figure 1 and Figure 2 to qualify or rule out similar and dissimilar variables. If you have static every time you call Customer A, but Customer A never has static when she calls you, you can rule out every similar variable as a possible source of the static. Simply comparing the two different types of calls allows you to remove the following elements as potential sources of the static:

Your VoIP phone Your VoIP proxy Your IP provider

The local service realm of your VoIP carrier The local carrier for Customer A The phone system for Customer A This side-by-side analysis is sometimes referred to in telecom as stare and compare. The simple act of placing the two calls next to each other provides you with the data that you need to prove out, or eliminate, some variables. If every call outbound to a certain phone line has static, but no inbound calls from that same phone line have static, then any piece of hardware that's used in both calls is vindicated as a potential source of the static. This logic isolates the issue down to the one dissimilar variable present on the affected calls, the long-distance side of your VoIP carrier. Many call issues reside within the realm of the long-distance portion of the call, for no other reason than that leg of the journey usually covers the greatest geographic distance. The call may progress a few miles from your office through your Internet provider to the SBC of your VoIP provider. It starts the second leg of its journey when your VoIP provider sends the call to the longdistance carrier, which is responsible for transporting it across the United States (or across the world) before terminating it to another local carrier. The miles over which the long-distance carrier transmits the call means that the call potentially encounters more hardware and cabling while it spans from end to end. Every new piece of hardware or cabling is another aspect of the call that can fail and cause problems.

Now, not only does the long-distance portion of the call cover a lot of distance, so can the VoIP

portion of your call.

Figure shows what may be hidden behind the curtain of your VoIP provider. It may not be the only VoIP entity in the equation. The current market of VoIP providers allows for several layers of telecom carriers in the mix. The call represented in Figure is a local call and never reaches a longdistance carrier's network. It might be an extremely local call, traveling only down the block to your office. The close proximity between the origination point of the call at Company A and the termination of the call at your office doesn't guarantee a geographically stunted transmission. This simple call in Figure hits the following entities:

Company A: Its analog phone dials your VoIP-provided phone number.

The local carrier for Company A: The call hits Company A's local carrier, which identifies the call as being local and then queries the national database to determine who owns the phone number. In the example in Figure 3, the local carrier that actually "owns" the phone number is Level 3 Communications.

The VoIP carrier: The actual VoIP carrier recognized as the legitimate owner of your phone number. It's easier to sign a contract for service with a VoIP carrier than it is to go through all the certification required to be a recognized local carrier, so most VoIP companies that sell you service don't go through the hassle. Because the VoIP carrier in this example is an established local carrier, it has presence in New York, and the call traverses only a few miles before it hits its network.

The VoIP reseller: This VoIP middleman is named Juggernaut Telecom in Figure 3. Juggernaut Telecom is located in Dallas, so the call is sent to the switch that it uses to aggregate its traffic before sending the call on to your VoIP provider. This company doesn't own the phone numbers in the eyes of the national database, but it isn't the company
you bought your VoIP service from, either. It's a VoIP reseller, among other telecom services, and it has enough traffic with the VoIP carrier to accomplish two important business functions:

• It can easily cover the minimum monthly payment that the VoIP carrier requires. The commitment always boils down to an expected level of revenue from the reseller. For instance, it must either have $25,000 in usage per month or pay the difference.

• The amount of traffic it has with the VoIP carrier is substantial enough that it can negotiate an aggressive rate structure, making it cheaper for your VoIP provider to buy service through Juggernaut Telecom than go directly to Level 3.

Your VoIP provider: The wonderful guys and gals at VoIP R Us provide all the great features available with VoIP in this example. They don't own your phone number, and they don't have direct contact with the Level 3 — but they have a contract to provide service for you. The only problem is that they're located in San Jose, where their soft switch aggregates their calls and gives you all the fun VoIP features. So, the local call from Company A across the street from you in New York is now sent to California.

Your Managed Switch: In Figure 3, the VoIP R Us server in San Jose sends the call all the way

back to your office in New York, where it rings your phone, and you pick up to speak to the guy across the street. Maybe you can see him through the window, and you wave, completely unaware of the fact that your call has run all the way to California and back.

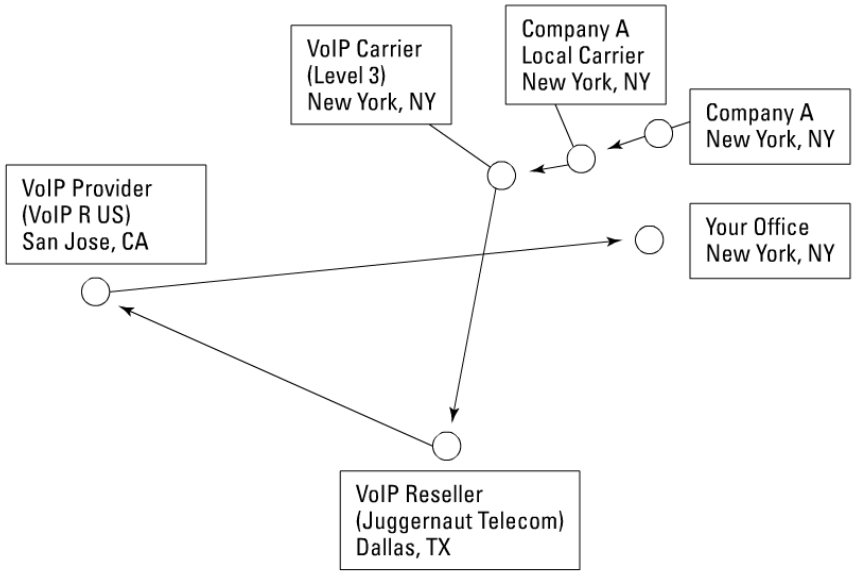


Figure 3 : A local VoIP call.

The distance that your VoIP call may travel doesn't have to be a frightening thought. As long as every leg along the way allows the RTP portion of the VoIP call to be re-INVITEd, only the SIP messaging has to take the circuitous route through the layers of your VoIP supply chain. In the end, the audio portion of the call may be traversing only from the Level 3 site in New York to your office. This short distance is preferable because every hop induces more latency and adds another potential variable to the equation that can cause latency, jitter, packet loss, and call failure.

Identifying the Categories of Call Problems

Trouble issues fall into two categories — call completion and call quality. These types of issues are different in both how they manifest themselves within the reporting of the network and the troubleshooting techniques required to isolate and repair them. You can generally find and resolve call completion issues easily, but call quality issues are more subtle and require more intensive research.

Digging in to call completion issues

Call completion issues refer to any call terminating in a manner other than a standard answer at the far end by either a person or a phone system. A call failure can be the result of SIP messaging issues, packet loss (within the VoIP portion of the network) or non-VoIP issues within the long-distance side that affect all calls to the destination phone number. You can quickly and easily isolate all the potential variables that can cause a call failure issue, from routing through the PSTN, to the terminating local carrier, to the recipient's phone or phone system.

It isn't your responsibility to fix issues within the networks of your VoIP carrier, the local carrier, or the destination number. But your carrier always greatly appreciates information that you can provide to unequivocally narrow down the source of the issue to one of these variables, and this information expedites resolution.

The specific nature of call failures are further identified by their call treatment, the symptoms of the failed or substandard calls. Call treatments don't have to relate to only call completion issues — the term is also used to describe call quality issues. The main call treatments you encounter and their meaning can be found here.

Listening for tones and tags

Tones and tags are supplemental sounds or recordings that can be attached to a standard recording. Tri-tones are three tones in ascending pitch that generally sound like they're being played by a cheap synthesizer. They precede a recording played by a local phone carrier, as opposed to something added by a long-distance carrier. The tri-tones let you know that you've reached the wrong local phone carrier, or the wrong Central Office (CO) at the correct local carrier.

The tags are more important than the tones because tags frequently provide valuable information to your carrier. Tags are attached to the end of a recorded message and usually consist of a group of numbers. A tag may be added onto the end of a recording, such as, "Your call cannot be completed as dialed____17-2."

The tag of 17-2 usually identifies the specific switch in the long-distance carrier's network that's playing the message. This information helps your carrier troubleshoot because it can go directly to the switch that's playing the recording to find out why the call failed, instead of chasing down the call example to finally determine the final switch.

Despite the wealth of information in SIP, it doesn't directly translate tones or tags into a SIP response. Your carrier may not provide you with the audio recording, it may respond with only an appropriate SIP code, preventing you from receiving this additional tone and tag information. Your carrier can still find the call and resolve the issue; the process simply takes a bit more time if you can't relay the tag information.

Understanding the fast busy signal

A fast busy signal is a busy signal that sounds twice as fast as the normal busy signal. You probably hear a fast busy signal when part of your carrier's network is down, so your call can't be completed. Because this call treatment is interchangeable with the "all circuits are busy" recording, your carrier invariably gives you the same SIP response messaging identifying it.

Dealing with dead air

Dead air is when you hear nothing on your call after you dial a phone number. You don't hear the dial tone anymore, but you also don't hear any ringing; you just hear nothing. When you have a call with dead air, stay on the line for 30 to 60 seconds; the call treatment usually reverts to a fast busy signal if you wait long enough. It is possible for the call to eventually complete, despite not hearing any ringing on the line, or could fail to a recording. It's worth the minute or two of waiting to see what happens. The additional information could be the key to a quicker resolution.

Dead air is generally caused by failure to transmit a ringback signal or one-way audio.

Dead air isn't the same thing as Post-Dial-Delay (PDD). PDD is the silence you hear that usually lasts a few seconds between when you finish dialing the phone number and when you hear ringing from the far end.. International calls are notorious for long PDD; anywhere from 15 to 30 seconds may pass before you hear the phone ring on the far end.

Encountering the aberrant recording

If you receive any recording referring to your carrier, it probably wasn't made by the carrier's network. Always start your investigation by checking with your VoIP provider to ensure that it doesn't have the recoding in its library. If it confirms that it doesn't have it on file, then capture a bad call with Wireshark.

Picking up dropped calls

Phone calls that are disconnected before either person hangs up are deemed dropped calls. If your phone system loses power while you're talking, it drops your call. The same thing happens if you're calling over a dedicated circuit that suddenly fails, whether it's the Internet circuit over which your VoIP is running or a circuit within your long-distance carrier's network.
The good news is that every call is monitored to see who disconnects the call. Your long-distance carrier's network records whether your SIP server sends the BYE or the analog phone on the other side hangs up and sends a disconnect signal. R&R switches handling the call actually have three possible options that it can use to identify the disconnect call:

✓ Origination end disconnect (Calling party)

✓ Termination end disconnect (Called party)
✓ Internal

The first two options are pretty self-explanatory. Your managed switch saw either the originating or terminating party hang up. One of these results generally moves the troubleshooting along quickly. If you were dialing out from your VoIP server and the person you called had a power outage, the call could drop, and the network would see a disconnect signal from the far end.
The third option of Internal indicates something curious — this option tells you only that disconnect wasn't the result of one of the ends hanging up or sending a BYE or CANCEL. An Internal indicates that the call ended because your switch dropped the call, that might be due to internal timeouts (like remote party does not answer) or failure to negotiate certain call parameters with one of the sides.

Analyzing call quality

Both VoIP and non-VoIP issues can potentially cause call quality issues. Each technology has its own propensity for call quality issues. A short on the line can much more easily generate static on an analog call than the SIP side of the call can produce anything remotely akin to it.

Hearing the echo

Echo (also called audio gain) occurs when the audio portion of the call has excessive amplification that causes an audio reverberation the listener perceives as echo. Echo can be a VoIP-related issue, but it's more commonly associated with the long-haul section of the call while it routes through the PSTN. The main challenge with echo is that, like latency concerns in VoIP, it's a cumulative issue that collects from one end of the call to the other. Every piece of telecom hardware that processes your call adds a bit more volume to it, compensating for the audio loss while the signal is pushed from the originating local carrier through the PSTN to the terminating local carrier. This issue is more common with calls that cover long distances (such as coast-to-coast calls).
Usually, only one person on a call hears the echo. Carriers have specific pieces of hardware installed throughout their network called echo cancellers (or echo cans) that eliminate echoes on calls. These devices can fail over time, be mis-optioned, or be mistakenly installed backwards. If one person hears an echo on a call, a bad echo on the other end of the call is probably causing that echo. Sometimes, both people can hear the echo, but it isn't as common.
Echo doesn't manifest itself in a way that's immediately visible to the technicians at your carrier. If your call fails to a fast busy signal, your carrier can pull the call record and find the piece of hardware in its network where the call failed. Some issues, such as dropped calls or static, are visible in a circuit's performance report, which indicates an electrical or protocol-related anomaly. Echo on a call doesn't leave a trail of breadcrumbs, so it's a difficult issue to isolate and repair.

Clipping bits of your call

Clipping is the telecom term used to identify when random portions of your call are dropped. If you've ever spoken to someone on a cell phone in an area with bad coverage, you've experienced clipping when you lose bits and pieces of the other person's words and sentences.
In the non-VoIP world, clipping is seen as the mechanical opposite of echo. An amplification of the signal causes the reverb-generating echo; insufficient or negative amplification results in clipping. Communication between traditional analog land-line phones don't often have to deal with clipping and echo because the amplification levels of the carrier's switches and the local carrier COs have been refined over years to ensure sufficient signal strength without echo or clipping.

Finding static

Static is the loud white noise you hear on the line, at times overpowering the conversation and forcing you to hang up and try your call again. This isn't a VoIP issue. It's generally caused by an electrical short in a specific section of cabling or hardware in the call path. The most challenging aspect of static is that you hear it only when your call passes over that one failing piece of hardware or cabling. So, the problem is generally intermittent because not every call to a specific destination takes the same path. Even if you call the same phone number ten times in a row, you may hit the identical path only twice. If you have static on 5 percent of your calls, the mathematical possibility of capturing one of the bad calls and getting it resolved in 24 or even 48 hours is slim.

Isolating a Pattern

The process of qualifying a problem should progress from general to specific. After identifying the problem and its frequency, look for a pattern in which calls are affected. Depending on the depth and breadth of a problem, you may need to look beyond what you've identified in the general troubleshooting to find the source of the issue.
Any consistent problem is easy to find and track down. If every one of your outbound calls is failing 100 percent of the time, you can bet that something at your switch, IP provider, or your Carrier is causing the problem.

The smaller the problem, the more difficult it is to correct. If you experience a troubling but intermittent issue, you can help the repair process along by providing as much detailed information as possible to R&R technical support.

Matching up the time of day

One of the last troubleshooting patterns you'll use to troubleshoot a failed or affected call is the time of day at which it occurs.

Identifying the Frequency of a Call Problem

After determining what the problem is, your next job is to estimate the consistency of the problem. Can you get the same call treatment or call quality issue 100 percent of the time, or is this more of a 20-, 10-, or 5-percent issue? The frequency of the issue has a large impact on how you go about troubleshooting. The larger the problem, the easier it is to find and fix. Smaller issues that affect less than 10 percent of your calls can linger for months without being resolved unless you stay diligent and keep very good notes.

The key to resolving these kinds of issues is to be in full communication with your carrier and provide as much information as possible about both affected and unaffected calls.

Figure shows the paths taken by three calls, all originating in Portland, Oregon, and terminating in Miami. The first call (represented by the single solid line) experienced static, but the second and third calls didn't experience any static. Your carrier can analyze these three calls to locate the path they took and then isolate or eliminate legs of the call, depending on whether the calls had static.

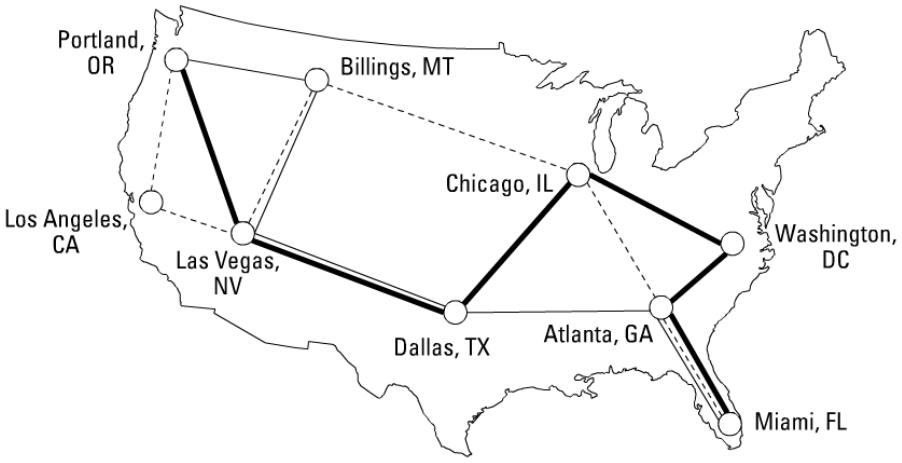


Figure: An intermittent call issue.

Laying the individual call paths over each other, you can see that the affected call took only two legs of the path that the two unaffected calls didn't take. Your carrier can assume that every leg of the unaffected calls is clean, so only paths that aren't shared with a clean call are identified as suspect. Your network technician can therefore isolate the sections of the network (in this case, the leg from Portland, Oregon, to Billings, Montana, and the leg from Dallas to Atlanta). You can see how more information helps to isolate an issue because every affected or unaffected call further clarifies and reduces the possible variables.

Figure is a simplification of the possible route choices available on each call and indicates the calls being routed within the carrier's network, which allows your long-distance technicians to see the

exact path. In reality, a call can take a multitude of possible routes, depending on the route cost, quality, and congestion.

Beware the underlying carrier. No long-distance carrier has direct connectivity to all destinations. So, it uses other carriers to transmit calls in areas in which it doesn't want to install fiber, switches, and service. Every carrier operates this way for the simple reason that it's a very good way to do business. The downside of these arrangements is that R&R technicians can't see a call after an underlying carrier takes it. If a problem is specific to one underlying carrier, your Carrier can easily take it out of route or open a trouble ticket with it, alerting it to the problem and requesting resolution.

Performing Your Due Diligence

Your network is your responsibility. Every link in the chain of your VoIP communication has a point of demarcation beyond which one company's responsibility ends and another company's begins. Your VoIP carrier isn't responsible for correcting problems in your Dial Plan or how your managed system responds to specific SIP methods or responses. Before performing all of the required testing to ensure a call quality of completion problem is not within your area of responsibility, you need to know where the responsibilities reside:
Your Client: Your Client is responsible for sending accurate SIP and RTP packets with the correct headers, structure, and information. They also need to make sure that their switch responds to all incoming RTP, as well as SIP methods and responses, according to the latest RFC or ITU-T standards.
Your Carrier: shoulders the greatest range or responsibility because it must respond to your SIP/H323 and RTP packets; convert them, as necessary; and complete your calls to the destination by accurately sending them through the PSTN.

Before you open a trouble ticket with your carrier for any issue, perform at least the most basic analysis using CDR Search ensuring that calls are being send out to Carrier and that disconnect is coming from the Called Party. The five or ten minutes you spend doing a cursory examination not only provides direction to the troubleshooting, it also shows your VoIP provider that you know what you're doing.

Worrying about what your carrier thinks of you may seem odd, but the big faceless company that provides your VoIP service is run by people, just like you. If you call them up screaming because all your outbound calls are failing, they may drop what they're doing and call in all their best technicians to look at it. They'll work over the issue, and if they discover that they aren't receiving

any packets and your IP provider is down, they're going to be less inclined to jump through hoops for you the next time you call.

To do your call-completion due diligence follow these steps:

1.Get a Wireshark capture of the failed call.
2. Read the Wireshark capture.
Review the banter between yourself and your VoIP provider. Identify where the call fails, and the specific response you're receiving on the failure.

Look at the last packet before the call failure response to determine whether it may be a response to something your managed system sent/did not send. Do you think it came from the far end of the call on the other side of the PSTN?
Try to have a capture of a completed call to review next to any failed call you're investigating. You can much more easily stare and compare the two calls when they're sitting side by side. The side-by-side comparison allows you to check every aspect of how the call is handled.

Using Logic when Troubleshooting

Nothing happens in a vacuum. The process of troubleshooting involves finding a pattern for the issue that fits a profile. You need the correct mindset before you even open the trouble ticket with your Carrier.

Troubleshooting should progress from general to specific, with each test building on the knowledge of the previous test, further eliminating variables. To hit all the targets of troubleshooting, follow these steps:
1. Identify the variables.
Draw how all the business entities engaged in the call interact with the call.
2. Isolate the variables.
Confirm that every section in the call path is either suspect or proven good based on a comparison of call types or testing.
3. Find the level of the issue.
Is this a global issue affecting all calls, or is it isolated to one phone number or region? You can link the profile of call failure or poor call quality to the level of the OSI model in which the problem exists.

4. Identify a pattern.
If the problem always crops up at 5 p.m. on Friday or only when you call to Guinea, you can refine your data to eliminate more variables, making it easier for your Carrier to identify the issue.
5. Trace back to when the issue first began.
VoIP can seem to disconnect at times. While you're dialing out, a port may suddenly seem to lock up. As far as you know, your server is sending the SIP messages, but your VoIP provider isn't responding anymore on a specific RTP port. Whenever you have an issue where the communication seems to have just stopped on a specific call for duration of time, you have to dig in a bit deeper to the issue.

The interaction between your managed system and your Carrier is very methodical. If you send a SIP method, you receive a SIP response. If you don't receive a response, something has gone awry. The issue is probably related to how the last call ended, rather than a failure in sending packets through your IP provider or a glitch in the SIP/H.323 stack at your VoIP provider.
You can find a trouble issue only when it's present. Call captures of completed calls don't help unless you also have a failed call to look at, which is why large issues that affect 100 percent of outbound calls are so much easier to troubleshoot than a 5-percent issue.

Avoid any method of troubleshooting that resembles grasping at straws. A random series of "well, let's try this" attempts doesn't isolate or eliminate variables — and it's a sure-fire way to prolong the issue and increase your frustration. Before you dive in to a problem, make a plan that allows each additional test to build on the knowledge of the previous test. Each new action that you take must further isolate the issue or prove out variables — anything else is just an exercise in futility.

Investigating Carrier Trouble Reporting Structure

Most carriers have a two-tiered structure for handling problems. The first tier is the entry-level customer service folks. These people generally work from a script and ask you specific questions to qualify your issue. The customer service agent works through all the required questions and then gives you a trouble ticket number for tracking purposes.
Depending on your Carrier, this first line of defense may be able to get packet captures on VoIP calls and do rudimentary troubleshooting, or it may simply be an interface to begin the entire process. Speak to your Carrier to find out the testing and visibility capable that their first tier of support has. If it can pull packet captures and see detailed information, it may be able to resolve most of your problems without having to complete a trouble ticket and relay it to a technician —

which can save you time and frustration.

If the first tier of customer service can't resolve the problem, the trouble ticket is sent to the VoIP network technicians, who make up the next level of support. These people can manipulate the network, update switches, and perform more intrusive tests, and they're empowered to fix the complex things that go wrong. You want to speak with this group of people when you have a complex issue.

If you have a difficult and intricate issue, give the first-level customer service people just enough information to open the ticket and then ask whether you can chat with a technician as soon as possible

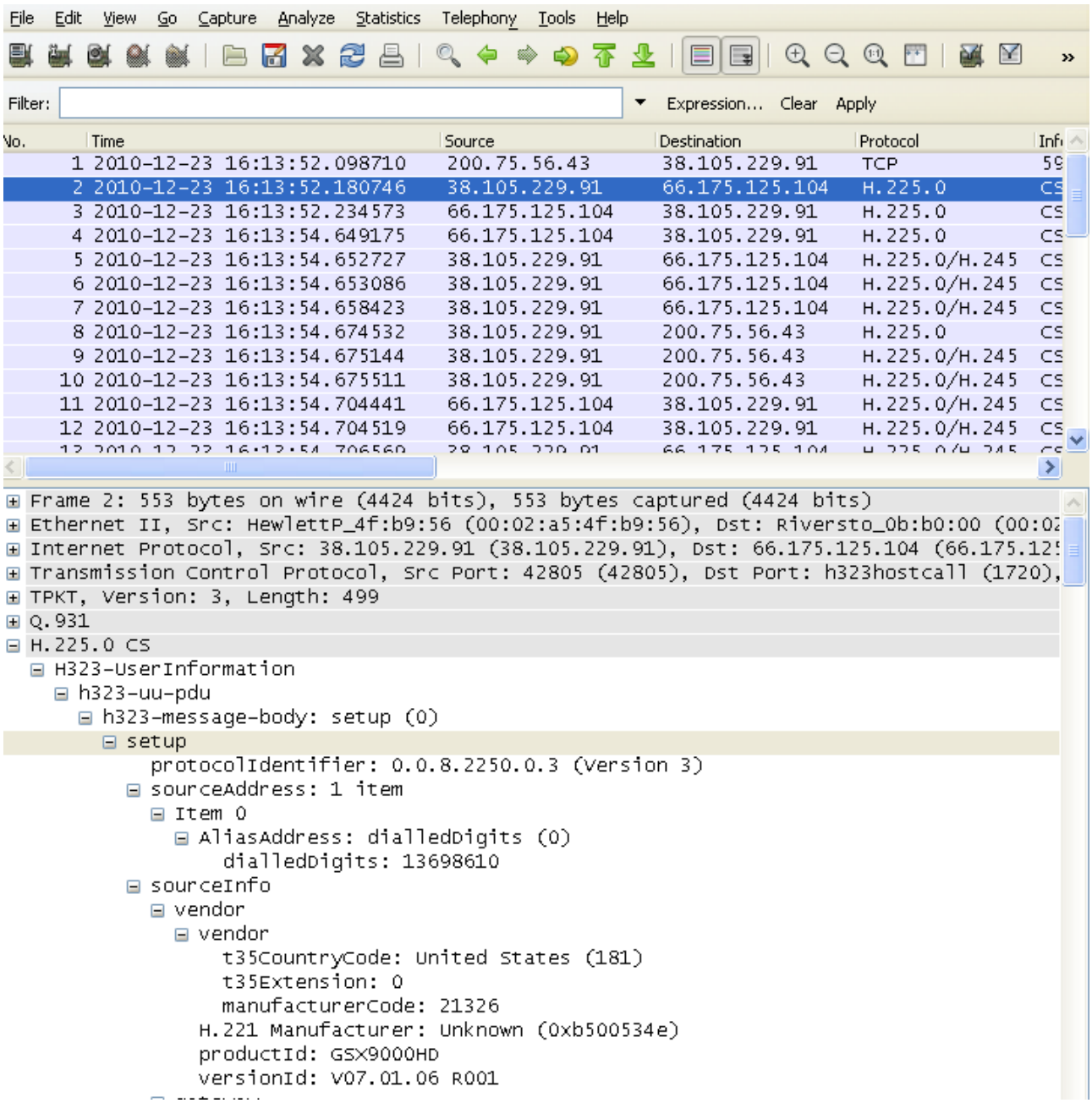
Familiarizing Yourself with the Wireshark GUI

The Wireshark GUI is the gateway to unraveling the mystery of your VoIP calls. The main window for the Wireshark GUI consists of

Menu bar: Contains drop-down lists of options for the standard applications. The only two items on this bar you use when capturing and analyzing VoIP calls are the Capture section (if you're starting captures from the GUI) and the Statistics section (to isolate VoIP calls).
Tool bar: Provides buttons to quickly start and stop captures, as well as navigate quickly through a capture. These are great shortcut buttons that you should investigate after you're comfortable with the basics of Wireshark packet capture and analysis.
Filter bar: You use this bar frequently. The Filter: button automatically generates the filters that Wireshark uses in many instances. You need to generate a filter manually only if you're isolating RFC2833 DTMF packets to investigate why your DTMF touch tones aren't being sent or received properly.
Data windows: Wireshark displays the data from the packet capture in these three windows allowing you to analyze the SIP banter on the call between the SIP nodes:
Summary: Provides a summary of the packet captured. The SIP/H323 messages are displayed in this section, allowing you to see a high-level overview of the packets that make up the VoIP call.
Protocol Tree: This window displays the nuts and bolts of the SIP information. Selecting a row in the Summary window populates the specifics for that packet in the Protocol Tree window. The Protocol Tree window allows you to expand the SIP messaging, the SDP, and the RTP to view the specifics of each and validate the information provided and negotiated.
Data View: The Data View window shows the raw data collected in the capture and highlights the information that corresponds to the element of the protocol tree you've selected. You don't use this section of the screen for VoIP call analysis because you can find all the data you require in plain English in the Summary and Protocol Tree windows.

Figure shows a VoIP call capture displayed with Wireshark. Opening a capture with Wireshark is very easy. As long as the capture being opened has the .pcap suffix, Wireshark may be automatically selected to open it.

The Wireshark GUI.
Right-click the file and select Open With. As long as you have Wireshark loaded on the computer, it will be listed on the pop-up menu of programs, and you can click on it to select it.
Open Wireshark and then choose FileOOpen from the main Menu bar. A pop-up window allows you to navigate around your computer to find the Wireshark capture file you want to view.
Highlight the desired file and click the open button to view the file with Wireshark.
After the file opens, the entire content of the capture is displayed.



Using the Summary window

The Summary window of Wireshark provides you with an overview of the packets in the capture. The capture covers everything flowing through the device.

The data in the Summary section is grouped into six columns:
Number: This column identifies the frame number of the capture. This very helpful section of the Summary window allows you to reference a specific line in the capture when speaking to someone.
Source: This is the IP address of the device that originated the VoIP packet listed.
Destination: This is the IP address of the device to which the VoIP packet was sent.
Protocol: This column identifies whether the packet listed was SIP, SIP/ SDP, H.225, H.245, T.38, or any other protocol.
Info: The Info column provides a summary of what's being said in the packet. In this column, you see whether the packet was an INVITE, 100 Trying, 180 Ringing, or 200 OK or ACK, to name a few.
The Summary window provides the general information allowing you to identify specific packets that need further investigation.

Branching into the protocol tree

Selecting a row of data in the Summary section of Wireshark populates the Protocol Tree window with all the information contained in that packet. The information is displayed from general to specific, and you can expand each section to reveal more detailed information by clicking the plus sign (+) to the left of the section.
Frame: Lists the size of the frame captured.
Ethernet: Covers data from layer 2 of the OSI model on the frame. (More information on the OSI model is available in topic 5.)
Internet Protocol: The origination and destination IP addresses.
User Datagram Protocol (UDP): This would be TCP in a standard Internet packet. The example in Figure shows that the standard SIP signaling port of 5060 is being used for the source and the destination.
Session Initiation Protocol: Used to research SIP and higher level VoIP issues. Expanding the lower-level section of the SIP protocol reveals the specifics of the IP addresses, ports, and codecs offered or established in the call. The SIP message in Figure 11-2 is expanded to show:
• Request Line
• Message Header
• Message Body
• SDP. The Protocol Tree window of Wireshark allows you to see the specifics for the selected packet, ensuring that protocol mismatches or blatant SIP handshaking issues aren't affecting the packet.

Finding VoIP Calls

Digging in to a VoIP call is fun, but first you have to find the call. Not every capture you execute will be so clean as to start with the first INVITE message and finish with a BYE.
Wireshark provides an easy way to isolate the individual VoIP calls in a capture, filtering out the unrelated packets. Click Statistics in the top menu bar and select VoIP Calls. Wireshark scans the entire packet capture, identifying all VoIP calls and populating them in a Wireshark: VoIP Calls pop-up window, shown in Figure.

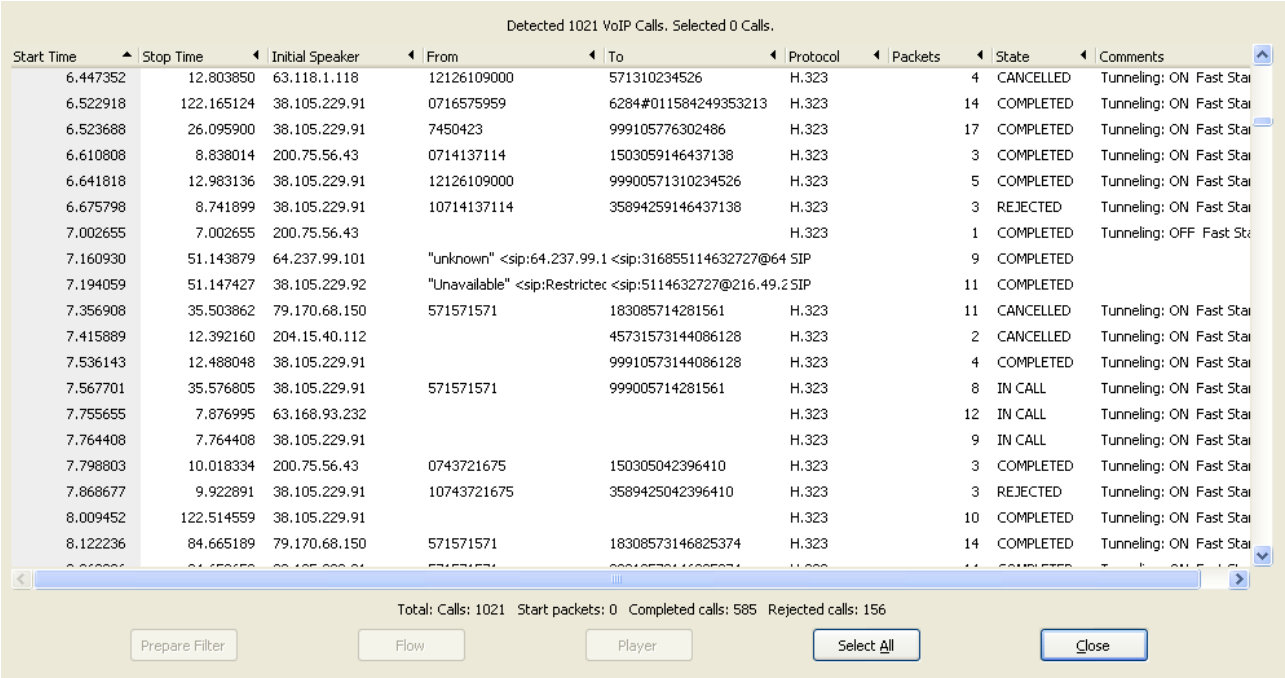


Figure: Viewing VoIP calls.

The window summarizes the calls by their general profile, allowing you to quickly see
Start Time: This isn't the time of day the call began, such as 8:49 p.m. or 20:49 in military time, but the amount of time between the moment the capture being analyzed began until the call was initiated.
Stop Time: The amount of time between the initiation of the packet capture and the final BYE message ended the call. This is not the duration of the call from INVITE to BYE, but the time in the capture when the BYE for the call was received.
Initial Speaker: The IP address that originates the call. The first call in Figure originated from the IP of 63.110.1.110
From: The origination SIP URI on the call. To: The destination SIP URI on the call.
Protocol: Because you're looking at a VoIP call, it's listed as SIP/H.323.
Packets: Provides the total quantity of SIP packets listed for the specific VoIP call.

State: Identifies the disposition of the call. The options include
Completed: Indicates a VoIP call that was established and was disconnected with a normal BYE.
Rejected: This call was refused by the called party.
Cancelled: Identifies a call forcibly disconnected with the SIP method CANCEL.
Call Setup: The call listed in the capture was never established and includes only the initial INVITE message and provisional responses, such as 180 Ringing.
In Call: Call is in progress during the packet capture.

Graphing a call

The bottom of Wireshark's VoIP Calls window has four buttons that remain grayed out until you select a VoIP call to analyze.
The first button to select when analyzing a VoIP call is the Graph button. This option allows you to see a call tree for the specific VoIP call selected.
Figure shows the call tree for a completed call. The dotted lines extending below IP addresses function as a reference point for the IP as either the originator or recipient of each packet. The example is a very simple voice call.

The graph provides you more information about the call setup. Figure 4 shows that three codecs were offered in the initial SETUP — G729, G723.1 and G729B. The (23610) and (1720) to the outside of each dotted line represents the port used for signaling on the call.

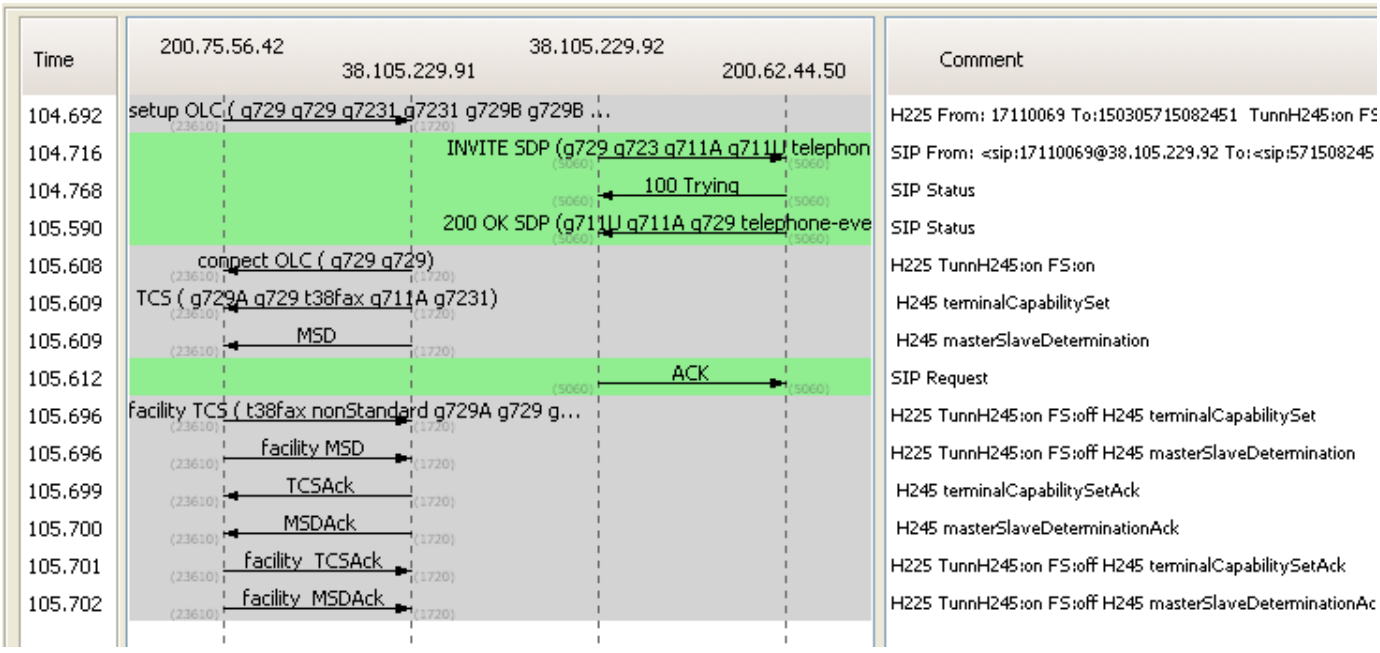


Figure 4: A graph analysis.

The example in Figure 4 is a version of a normal VoIP call. A single incoming VoIP call includes two legs:

Inbound from your VoIP Client

Outbound to your Carrier

In this example, both legs of the call are populated in the VoIP Calls pop-up window, but since they represent call messages cascading in from one leg of the call and out the other, it isn't helpful to look at each graph separately. You need to view both pieces as an integrated whole so you can instantly see how each call responded to SIP methods and responses that originated from the other leg of the call. Wireshark allows you to do this just as easily as viewing a single call graph.
Select both calls in the VoIP Calls window by clicking them individually or Ctrl-clicking the other call. After you highlight both calls, click the Graph button. The calls are now displayed together as one large graph with a different background color identifying each call.

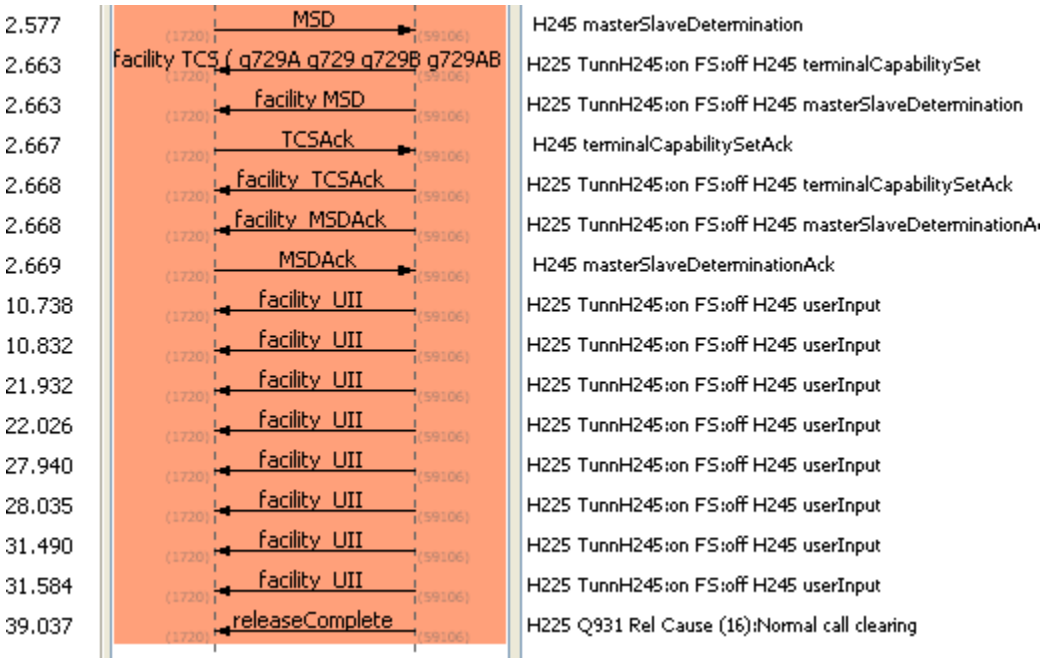
Filtering down to one call

The call tree allows you to take a quick snapshot of the SIP messaging on the call before deciding to investigate it further. If you need to dig deeper into the individual packets of the SIP or SDP messaging, simply close the graph analysis with the close button at the bottom of the window and, with the individual call still highlighted in the VoIP Calls pop-up window, click the Prepare Filter button. A filter designed specifically for the selected call appears in the Filter toolbar of Wireshark. Close the VoIP Calls window and then click the Apply button to the far-right of the Filter toolbar. The Summary window of Wireshark now includes only packets associated with that call. You can use this method to quickly and efficiently eliminate packets associated with other VoIP calls or auxiliary LAN traffic.
Now that Wireshark has filtered out all packets not belonging to the one call you're investigating, expand the sections of the packet in Wireshark's Protocol Tree window to display the Call Header, Message Body, or SDP sections, as you require. If you're attempting to follow the RTP port used for either the outbound or inbound stream, drill down into the SDP sections of the packet so that you can see the port number in the first line of the Media Description. After you expand the view in the Protocol Tree window, it displays all packets that you select in the Summary window expanded down to identify the first line of the Media Description if the highlighted packet has and SDP element to it. So, you can quickly scroll down packets in the Summary window, confirming that the details of the SIP methods and responses translated accurately from end to end.

Locating Touch Tones in a Capture

One of the challenges of VoIP is handling DTMF tones. They're used all the time, but they aren't really the ideal candidate for VoIP transmission. So, they come with their own set of complications. Of the two types of DTMF transmissions currently promoted by the VoIP community, only the out-of-band DTMF tones are easy to find with Wireshark. You have the option to listen to in-band DTMF in the audio portion of a call with the player to confirm the receipt and transmission, but this option is available only if you use uncompressed codecs.
The out-of-band tones are more mechanical. They aren't a tone at all, simply an event notification that your VoIP phone system reads to play the tone.

Packets arriving out of sequence can be confusing. If one of the last packets of a DTMF digit arrives late because of route flap, jitter, or any other reason, it can cause some problems within your VoIP phone system. Ensure that your hardware is discarding out-of-sequence packets; your SIP server could perceive a DTMF end notification followed by a late arrival as a second unique digit. Instead of discarding the packet and understanding the transmission as 5, the wayward DTMF packet could make your phone system read the transmission as 55. Reviewing the capture with Wireshark can very easily decipher this situation because the sequence number and event duration validate that the DTMF 5 packet that arrived late was a continuation of the original 5 DTMF digit and not a new transmission of the same digit.



Am out-of-band DTMF capture.

If you need to view the DTMF event in context of the entire call, select a row in the Summary section and click the Clear button on the Filter toolbar. The selected packet in the Summary section remains in the same position in the Summary window, but all the other packets are now available to you, as well. So, you can place the DTMF packet in the context of the call or the flow of traffic on the LAN.

Using Wireshark to Troubleshoot

Wireshark allows you to see the messaging and signaling banter between your switch and your Carrier. This visibility was restricted in the days before VoIP to only large customers who used SS7 signaling to connect to their carriers and large dedicated circuits equivalent to 672 phone lines. Even if you had SS7, you still had to have capture software and a technician who could make sense of it all.
VoIP and Wireshark place the power in your hands. The more comfortable you are with pulling information in Wireshark and dissecting your calls, the more quickly you can resolve issues — and the less frustrated you feel.

You can best use Wireshark to troubleshoot call completion issues. You can't as easily identify call quality issues (for example, clipping, echo, and static) by using Wireshark.

Your VoIP carrier requests specific information from you when you report the issue. You may not have direct access to this information without a capture. You might not know exactly which outbound port it took.

When troubleshooting a failed VoIP call with Wireshark, follow these steps:
1. **Open a packet capture and redial the failing number.**
If the call completes, then you have an intermittent issue. Continue to make test calls until you capture another failed call.
2. **Open the failed call in Wireshark.**
Open the file that contains the packet capture and identify all VoIP calls within the capture by choosing StatisticsOVoIP Calls from the main menu bar. Select the specific failed call in the pop-up window that appears.
3. **Graph the failed call**, review the messages passed between your switch and your Client/Carrier, and identify the source of the failure.
It may be as simple as your Carrier responding to your invite with a 4XX response code or one end of the call issuing a CANCEL order. If the call failed because of a 4XX response from your carrier,

open a trouble ticket with it engaging it for resolution.
4. **If the information in the graph is inconclusive, review all sections** of the packet to isolate any mismatch in the handshaking or negotiation by expanding all sections to include
• Session Initiation Protocol — Message Header: Check the SIP URIs, IP addresses, and port numbers in the FROM, TO, and CONTACT sections.
• Message Body — Session Description Protocol: Focus on the IP addresses and port numbers listed for the RTP, as well as the specifics of the media description, including the codecs offered and negotiated, as well as specifics for the RTP required in the media attributes section.
If you must open a trouble ticket with your VoIP carrier, it may ask you for specific information on the failed call. Figure shows the information your carrier may ask you to provide.
Here's the information circled in the SIP message header, by location:
FROM field: Origination IP address and phone number for the call
TO field: Destination phone number and IP address for the carrier's SBC to which the call was sent
TO field (below the destination phone number and IP address): The Call ID of the failed call.

Your carrier also needs the basic information required in a call ID, as well as one final piece of VoIP specific information — the 4XX or 5XX SIP response that results in the call failure. Not every VoIP call failure is rejected with a clean SIP response, but if one is presented, your carrier may ask for it.

Fax call handling

Faxing is the other telecom necessity that VoIP wasn't designed to handle. The transmission of faxing over IP is so specialized that it has its own acronym: FoIP (Fax over Internet Protocol).
Just like DTMF, faxes are transmitted over VoIP networks in two main ways. A VoIP network can either transmit the squeaks, squawks, and squelch of the fax in the audio stream of an uncompressed G.711 call, or it can convert the call into tiny .TIF files and send it with T.38.

The basics of a T.38 fax call are very straightforward. The call is established as a voice call and the RTP streams are established. After the call establishes RTP steams, one end sends a re-INVITE (SIP) or RequestMode (H.323) message that requests T.38, and the whole call is reconfigured in the same process of SIP methods and responses used to establish the call initially as a voice transmission, but this time negotiating T.38 as the transmission method.

Despite the similarities in transmission options, sending a compressed fax is more complex than just sending DTMF digits. The T.38 protocol builds on and utilizes existing fax and modem standards to complete a transmission. This intensive protocol is built like Russian nesting dolls — the T.38 packets contain UDP Transport Layer (UDPTL) packets that in turn contain primary and

secondary Internet Facsimile Protocol (IFP) packets.
The T.38 specification identifies the protocol as a two-phase protocol that includes the following steps:
A primary IFP packet must be encoded (you also have the option to encode a second IFP packet).
The encoded IFP packet is then installed into a UDPTL packet structure, which is also encoded, creating the finished T.38 message.
The stacking doesn't end there — a T.38 transmission may have two IFP packets, identified as a primary and secondary packet, each carrying a pay-load that uses yet another protocol called T.30 (a legacy fax protocol used for analog transmissions, as well as transmissions over IP with T.38). T.30 isn't the final supporting software of the transmission because it is in turn supported by a legacy modem format called V.21.

If you're sending a fax by using T.38, your Carrier may initiate the re-INVITE to T.38. Every SIP node interacting with the T.38 must be employed to handle the protocol, otherwise the call will fail. You can easily see this variety of failure when you use Wireshark because you receive either

488 Invite Rejected or 415 Unsupported Media Type

You must filter the packets by choosing Telephony->VoIP Calls on the menu bar and either viewing the graph or employing the filter on the call to see whether the T.38 failed. The VoIP Calls pop-up window may display a failed T.38 call as COMPLETED because setup and tear down of the call were normal. The FoIP call was most likely established as a G.711 VoIP call and then re-INVITEd to T.38. If the T.38 fails, the call re-INVITEs to VoIP and issues a normal BYE. For this reason, you can see only the 4XX response code by viewing the filtered packets or the call graph.

For more information about Wireshark VoIP troubleshooting read here:

http://wiki.wireshark.org/VoIP_calls

http://www.linuxjournal.com/article/9398

http://toncar.cz/Tutorials/VoIP/VoIP_Protocols_SIP_Call_Flow.html

Troubleshooting and Reporting Process

- Reviewing your carrier's trouble reporting structure
- Giving your carrier a call example or two
- Managing your trouble tickets
- Troubleshooting outbound calls
- Troubleshooting inbound calls

This topic begins with an introduction to the trouble reporting structure of your Carrier. I cover the information it requires when you open up a trouble ticket. That information is essential for it to solve the problem. I explain where to find the data, why it's necessary for resolution of your problem, and how to manage the trouble issues and your trouble ticket history.
The second half of the topic covers the methodical testing process that I advocate in topic 12, fleshing it out for standard inbound and outbound calls. You isolate and resolve issues with the individual legs of calls, down to the companies responsible. The testing in this topic isn't focused only on your VoIP LAN, but also the entire call path. The investigation of areas of the call outside your network consumes only a few more minutes but can greatly reduce the amount of time required for your carrier to correct the problem.
Depending on the size of your company and VoIP deployment, you may be troubleshooting a new issue every day, or you may have to troubleshoot only once a year. Regardless of how often you need this information, you'll be glad it's here waiting for you.

Providing a Call Example

A call example contains detailed information that allows your carrier to follow the call's path from the moment the INVITE message was received to the point where it either completed or failed. As technical as the idea sounds, a call example is just basic information that you've written down about a failed call. After you dial out and get a "cannot be completed as dialed" recording, dial the number again and write down the necessary information (see the following sections for more information about what to include in your notes). When the carrier finds the call's endpoint, the technician can begin correcting the issue.
Call examples tell the technicians where to look for the problem and also allow the customer service rep to categorize the issue. Based on the information you provide, the customer service rep sends your issue to a specific department for repair.
Call examples might not be easy to come by in all instances. If you're calling a number that you dial often and the call fails, you have all the necessary information at hand to open a trouble ticket. The challenge comes when customers who are dialing in to your VoIP phone numbers have issues. Most

people won't dial back into your company to report a problem that they had in reaching you. Unless they have your cell phone number, they may not have another way to reach you to report the issue. Even if they get through to you, you probably don't want to begin your conversation with a quiz about the specifics of a failed call attempt. As a result, you might have to ask one of your customers to make test calls for you.

Call examples have a shelf life of about 24 hours. The specific information about how the call is routed is kept in your carrier's switches for a finite amount of time before it's overwritten with new, more recent calls. If an issue crops up on Friday at 5 p.m., you need to relay it to your carrier immediately. If you provide the call example from Friday when you come into the office on Monday, your carrier will probably reject it and ask for a fresh example from within the past day.

Providing call example basics

Every call example, whether VoIP or non-VoIP, must begin with basic information:

Date and time of call: The technicians at your carrier must look for your specific call on a switch that processes millions of calls per day. Each switch stores call information in individual folders broken down by time. Telling your carrier that the call was placed at 10:05 a.m. CST today gives them the information necessary to go directly to the correct file within the switch.

Origination phone number: Your carrier needs to know the phone number from which you were dialing when the failed or affected call was made. In pre-VoIP days, a carrier used this information to identify the carrier's switch that was geographically the closest to where the call originated. The new VoIP world still needs this information to isolate your call from all other calls on their network that called the destination phone number that same day.

The number dialed: The dialed number indicates to your carrier's technician the most likely final switch in their network that would have processed the call.

The call treatment: Your carrier needs to know what it's looking for — is it a failed call to a fast busy signal or a completed call with static? The call treatment tells the carrier the real reason why this specific call example is of interest.

The physical origin and termination of the call gives your carrier a place to begin searching for your call example. It knows its network switches, and it can methodically run through them at either the origination or termination of the call. After it locates a likely switch, it uses the origination or termination phone number to query the file in the switch for the specific time the call was made so that it can find the call. In instances in which you're calling a popular number, your carrier needs the phone number from which you originated the call to differentiate it from the hundreds of other calls terminating to the same phone number. You may need to pull a Wireshark capture for a failed call to identify the specific originating phone number used on the outbound call because VoIP is dynamic and you can populate any phone number you want in this field.

The fresher the call, the easier to find. The easier to find, the faster your carrier can resolve your

issue. If every call you make to a specific phone number fails, make another test call right before you call into your carrier to make it easier for it to find the call.

Introducing VoIP-specific call example requirements

Because your calls are being delivered as VoIP, your carrier most likely also wants this information:
The IP address from which you originated the call: You have one or more IP addresses for each protocol SIP/H.323 from which you originate VoIP calls to your carrier. Your origination IP address is used just like the origination phone number in a non-VoIP call. It provides an origination point to find the specific call.

The IP address of your Carrier to which the call was sent: Your carrier may have several different and geographically unique IPs assigned to you. It may have deemed it necessary to accommodate your volume of calls or simply to provide redundancy in case one of its switches fails. It has to know which one you sent your affected call to in order to have any chance of finding the call.
The SIP reject sent for the failed call: If your call was rejected to an "all circuits busy" recording, the specific SIP response provides information to your carrier.

Filter failed call with Wireshark before you call your carrier with the issue to ensure that the origination and termination phone numbers, IP addresses, date/time of the call, and response that you're providing to your carrier are accurate. The Wireshark capture can also help you if your carrier requests the call ID for the failed call or the capture itself to compare against its switch records that show how the call was handled.

Managing Trouble Tickets

You may open several trouble tickets per month or only one a year. The more calls you send, the more likely to have one fail or experience poor call quality. You need to track your trouble ticket and keep a good log of how it progressed.
If you work for a VoIP carrier or reseller, create a database to log in all the trouble tickets, identifying
The Client reporting the issue: This information can include the specific origination or termination phone number or IP address. You need this field populated so that you can pull reports

to see whether any customer is experiencing chronic issues. Either he doesn't know his hardware, or a network issue may be frustrating him. If anyone has a high incidence of reported troubles, he or she may be growing unhappy and will probably stop being your customer.
The carrier to which the issue was reported: If you have multiple VoIP carriers, this field allows you to view the volume of problems on each carrier. If you have too many issues with any one carrier, you probably should move your traffic off that carrier and find another.
Call treatment: This field allows you to find trends. One carrier may be great on completion, but the last 15 trouble tickets opened with it were for clipping, probably caused by packet loss. Reports pulled from this field help identify troublesome areas of your carrier or end user's networks.
Notes/resolution: List how the trouble issue progressed, who you spoke to at your carrier, what he or she said, and at what time you had the conversation. Every time you call in for status, write another note, listing the date and time. After the troubleshooting process is complete, write down how it was resolved. This information is invaluable for chronic issues or if anyone gets into a finger-pointing match a year later.
Other fields: You can add additional fields to identify the time to repair and the frequency of trouble issues, but most companies don't need anything that detailed.
If you don't expect to have more than a few trouble tickets per year, you don't need to make a database to track them, but keep your notes. You can simply jot everything down on a piece of paper and stick it in a Trouble Tickets folder in your desk.

Understanding the timelines

The service side of telecom ebbs and flows based on the triage of incoming trouble issues. If someone has a huge circuit failing that normally sends out a million calls a day, he or she is going to be pushed to the top of the list, and a 5-percent Post-Dial-Delay issue goes to the bottom of the pile. The telecom triage is a way of life in the industry — and a large outage or issue can, and should, get people out of any staff meeting or conference call to jump in on the problem and work it to resolution.
Every carrier has a different timeline for response, but somewhere in every company, that timeline exists. Ask the customer service rep when you open your ticket when you can expect a call back from a technician. You may have to wait as little as two hours for a large network issue or as long as a day or more for international call completion or call quality issues.

The time that the customer service rep gives you when you open the trouble ticket is generally a response interval. That doesn't mean that they can resolve the issue in two or four hours. It simply means that a technician should call you back in two to four hours for testing, for clarification, or to provide an update. The technician may be able to fix the problem at that time, but don't base the life or livelihood of your company on it.
If you need to know an average time to resolution, ask your Carrier for that information in a generic context, not specific to your trouble issue. You probably won't be able to get an Estimated Time to

Repair (ETR) for your specific trouble issue. If you're trying to decide whether to send your staff home or make a business decision about when a telecom issue will be resolved, ask your customer service rep (in your most relaxed and non-accusing tone of voice), "How long do these problems usually take to get fixed?" If the rep doesn't think that you're going to use the information against him or her in a court of law, you can probably get a ballpark time frame that you can use to make a decision.

Working your escalation list

Every company that provides telecom service should have a solid structure for reporting problems and escalating issues. The telecom carrier or provider should have provided you with an escalation list when you first activated service with your carrier. If you ever lose your copy, it should be able to send you a fresh copy via e-mail within minutes.

Some companies have strict rules of engagement for escalations, especially when it comes to the traditional local phone carriers, such as Bell South and Verizon. It may specify that a customer can escalate a call quality trouble ticket only once every four business hours. Other companies allow you to escalate as you see necessary. Remember these bits of advice when you're escalating a trouble ticket:

When you go higher up the escalation list, you don't necessarily reach more sophisticated technicians. The tier 1 and tier 2 technicians can solve the majority of issues handed to them. Escalating up to their manager may put you in contact with the most senior technician in the department, or you may just reach someone who has good management skills and only basic troubleshooting prowess. Escalation to director, senior director, and vice president levels doesn't put you in contact with a more skilled technician, it simply raises the visibility of the issue.

The wrong way to escalate is by making your carrier the enemy. It's possibly the only entity that can fix your problem, and at the least, you need its cooperation in testing to resolve an issue, even if that issue isn't directly within its specific area of responsibility. Pointing the finger at the carrier, screaming, and threatening is no way to enlist it to go the extra mile.

The end result of an escalation is that you resolve your situation, and you build a stronger working relationship with your carrier. VoIP issues can quickly escalate to the realm of the technically esoteric. You need every resource available to unravel some of these mysteries, and alienating your carrier (one of your largest technical resources) is never helpful. You can make your life much easier by establishing a healthy working relationship with all your technical support staff.

Providing Multiple Call Examples

A single call example sometimes isn't enough to resolve complex issues — especially with intermittent issues. Your carrier may have ten different IPs to which the calls can be sent.

Any intermittent issue may be caused by any one leg of the journey, any one piece of hardware, or a cumulative response to multiple issues along the way. These intermittent issues require you to provide multiple call examples to your carrier. It may ask for only two or three examples of affected calls, as well as two or three examples of unaffected calls. Even if the initial customer service representative opening the trouble ticket doesn't want the other call examples or doesn't have room in the ticket to input the information, keep those call examples handy. The technician who picks up the trouble ticket and eventually calls you back will appreciate your diligence and gladly take down the information.

Intermittent issues are the most troublesome because they can easily persist for weeks or months. By keeping an accurate log of both affected and unaffected calls, and maintaining a consistent dialogue with your carrier, you can generally resolve the problem in a matter of days.

The reason intermittent issues persist is because people lose focus. After the initial report of the problem, your carrier responds by attempting to bypass a specific portion of its network or re-option a suspect piece of hardware. Its fix may not be complete and may remove only one more variable from the equation, so it asks you to retest after it completes the changes. It's difficult to maintain focus on a problem that takes days or weeks to work through, and the transition point between the carrier and yourself can cause the problem to drag on.

Your job probably isn't devoted to chasing down 15- or 5-percent trouble issues on your phone system. You're taking the emergencies of the day and doing your own version of triage. If a customer has an emergency because something was shipped late or to the wrong address, or it arrived broken, or the wrong thing was sent, you can't make those test calls on the 5-percent static issues and get back to your carrier in a timely manner. You might take three or four days to work your way down to the issues that affect 5 percent of your life. By then, your carrier has closed the original trouble ticket, and you have to start all over again. Stay focused, make the five or six test calls, and reply to your carrier in less than 24 hours to put the phone-issue ball back in its court. Its technicians do nothing but work on trouble issues, so you can go on with your normal job and expect a call back in about another eight business hours for the next round of testing.

Troubleshooting an Outbound Call

Although you can have many types of calls — inbound local, outbound long-distance, toll-free, international, and so on — the only classifications that you need to worry about for VoIP are

inbound and outbound calls. All the other permutations of calls, including international and toll-free, are simply add-on steps to deliver an outbound call or receive an inbound call. The VoIP interaction between your carrier and your switch is of greatest importance to you in the troubleshooting process. If you're looking for a step-by-step breakdown of all varieties of calls, as well as a detailed troubleshooting process.

The majority of the calls running through the average business phone system are outbound calls. These calls begin at your VoIP phone, traverse your LAN, are aggregated by your SIP proxy, and are sent via your Internet provider to your VoIP carrier.

Figure shows the variables in a standard outbound VoIP call. The level of troubleshooting available to you depends on the complexity of your network design. The more redundant carriers and ISPs you have, the more opportunity you have to surgically isolate and prove out each section of your call.

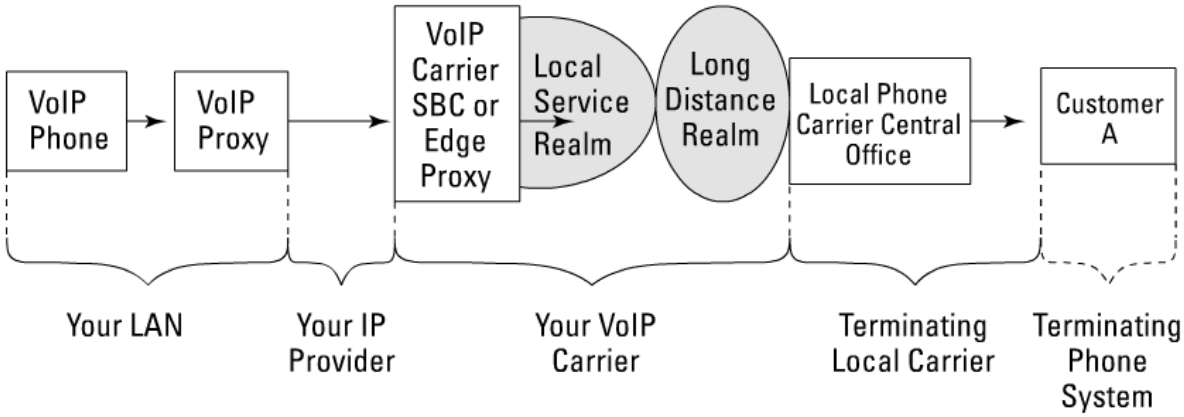


Figure: A standard VoIP outbound call.

Troubleshooting must follow a logical progression in which each test proves out another section of the call, removing it as a potential cause of the issue. Troubleshooting individual call issues should begin by proving out your own hardware and then moving out through all other variables until you reach the phone system at your destination.

Troubleshooting Step 1

You must make an outbound call to the same dialed number that experienced the failure or call quality issue, but execute it in a way that changes one of your outbound variables, keeping all other variables the same. This first test may not be easy if you have only one VoIP carrier, one Internet provider, and no analog lines connected to your VoIP phone system.

If you have any redundant services connected to your VoIP phone system, have the programmer who set up your phone system create extensions that are dedicated to specific IP providers, VoIP carriers, or ports on your system (including analog). That setup allows you to hit the extension, dial the phone number experiencing the issue, and ensure the call is sent over a specific carrier. The more extensions that you can set up to direct your call over a specific route, the more quickly you

can isolate an issue.

Bypassing your Internet provider

Your Internet provider is a small but vital variable in the outbound dialing equation. It has the simple task of routing packets between your switch and your Carrier. It probably doesn't indiscriminately lose hundreds of packets, unless it's experiencing a huge outage or congestion.

If every SIP packet sent has an appropriate response, you can reasonably deduce that the call failure is related to something other than latency induced by your Internet provider.
Don't assume that every packet you believe you're sending is being properly sent. If your Carrier doesn't respond to the INVITE packets that you send, you might incorrectly assume that either your Internet provider isn't delivering the packets, or your VoIP carrier isn't responding to them. If you're seeing packet loss across the board on random outbound packets, and not just INVITE packets, then your Internet provider could be causing the issue.
Your VoIP carrier's SBC is designed to respond to every INVITE with a 100 Trying before it even tries to do anything. If you claim that you're sending calls and your VoIP carrier claims it isn't receiving the INVITE, you have one of two possible problems:

*You're overloading your Carrier. The accidental equivalent of a Denial of Service (DOS) attack where you are sending so many packets to your carrier that it can't respond to anyone else. Your Carrier may have provisioned you for both a specific limit of concurrent calls and a number of maximum allowable calls per second that you can transit. If you exceed the calls per second, you may overload its switch. You could send so many calls in such a short duration of time that you eventually send INVITE messages to which your carrier doesn't respond, but that's unlikely. Before it gets to that point, you can expect this kind of evolution of the problem:
1. The increase in incoming INVITE messages prevents other customers assigned to the SBC from having their calls processed. Their calls are rejected with a 487 Request Terminated SIP response.
2. Your excessive call attempts are rejected with a 487 Request Terminated SIP response.
3. You push through and continue to ramp up the volume of calls being sent, overloading every resource on your carrier's SBC. Finally, after thousands of INVITE messages have been sent by you, receiving the 487 Request Terminated, a few begin to see no response at all. The SBC has run out of processor strength, and you've outstripped its ability to generate enough 487 responses.
4. The NOC at your VoIP carrier realizes that you're overrunning its SBC with INVITE requests. It sends an urgent e-mail or call you, demanding that you throttle back your traffic or face it turning your service off.

Your VoIP carrier can run a capture for the same duration of time that your INVITE messages were sent to confirm that it saw the INVITE messages arrive. The INVITE message may not be arriving at your VoIP carrier's SBC because your SIP server may block it. In this case, check the last call transmitted before the problem occurred on the specific port that's failing the call. That call probably ended in an abnormal manner. Your VoIP server may have cleaned up the call by sending a CANCEL or timing out, but that doesn't mean that your SIP server is ready to go. Your IP provider probably can't successfully deliver all the SIP banter between you and your VoIP provider on every completed call — but likely just drops some random INVITE messages. Also, your VoIP provider probably can't respond to every SIP message on active calls, so it likely just ignores random INVITE messages.

If your issue is intermittent, whether call completion or call quality, you have to make several test calls to validate whether the issue is gone. If you have a 5-percent issue, make 20 to 40 test calls to validate that it's been resolved.

Bypassing your VoIP carrier

You can easily set up additional VoIP carriers to provide redundancy, which allows you to pick and choose the best rates from more than one carrier for outbound calling.

Figure shows the area of the call that you isolate when you send your call over an alternate VoIP carrier. If the problem you're experiencing is related to how your primary VoIP carrier handles your SIP methods and responses, you should see an improved response when transmitting to another VoIP carrier.

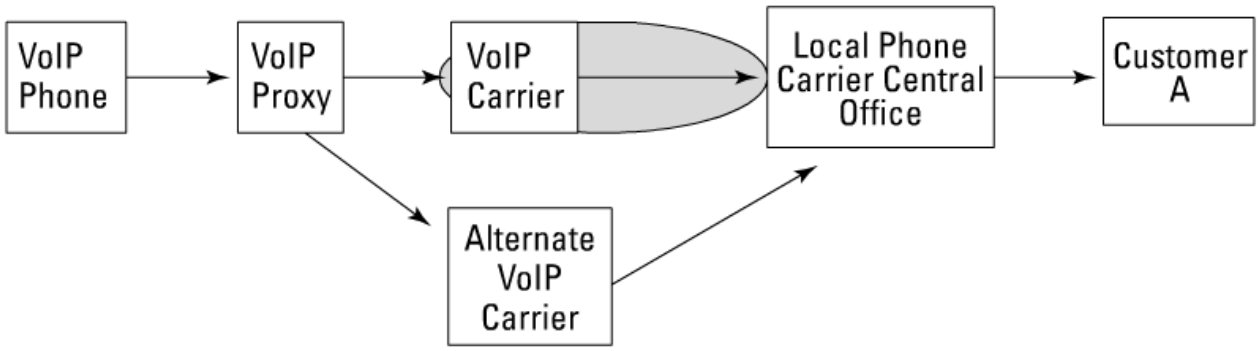


Figure: An alternate VoIP carrier.

Unless you're using VoIP service rolled out by a traditional long-distance carrier, you're probably in the dark about who your VoIP provider uses to handle the long-distance portion of the call. It may use one long-distance carrier or several. This long-distance question affects the troubleshooting process because if both your primary and secondary VoIP carriers use the same long-distance carrier, your test call over the alternate provider isolates only the front-end SIP interface section of its service. Only when you know for certain that they use different long-distance carriers does this test actually isolate the area form your VoIP carrier's SBC to the point at which the call is dropped off at the local phone carrier for the phone number dialed.

Take a Wireshark capture of the failed or affected call over your primary VoIP carrier, as well as over the alternate VoIP carrier. You can much more easily identify a problem with the specific details of the call when you can look at these calls side-by-side, going through every layer of every SIP message sent and received.

If your call treatment improves when you dial over another VoIP provider, then you need to call your primary VoIP carrier to open a trouble ticket. Give it all the information that it needs, and it should be able to resolve the issue quickly.

If the issue you identify is a SIP interaction problem, your VoIP carrier may or may not make changes. If you experience the exact same call treatment or call failure when you send the call over an alternative VoIP carrier, all isn't lost. You may not have positively identified the specific source of the issue, but you've eliminated a large section of it as the possible source. You've just validated the entire center section of the call, from the millisecond that the packets reach your VoIP carrier to the millisecond that they're delivered to the local carrier at the terminating end, so it's no longer in question.

Trying it on an analog line

You may still have an analog phone line which handles faxes, modems, or security systems, or is just a general backup in case your IP provider or VoIP carrier have a catastrophic failure.

Figure identifies that all external SIP messaging, as well as your Internet provider, VoIP provider, and the long-distance network they're using are all bypassed when you execute an analog test call. Going analog cuts out a huge section of your outbound call and quickly narrows down the potential sources of the problem. The analog bypass allows you to definitively prove out your Internet provider, as well as the variables isolated on the test call to the alternate VoIP carrier.

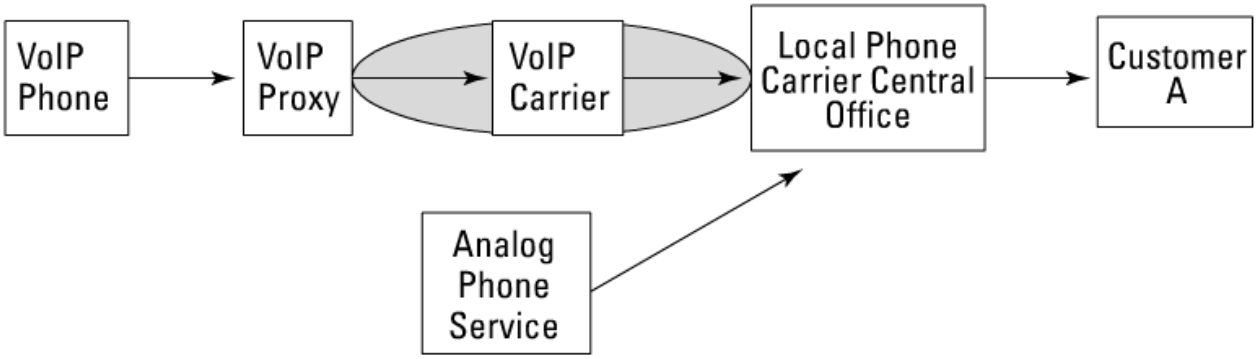


Figure: An analog bypass.

Calling out over another long-distance carrier

The non-VoIP world has an easy way to bypass the long-distance portion assigned to your phone line. Almost all local phone carriers allow you to place your call on another long-distance network by dialing their access code prior to the phone number you want to reach.

Testing with your Cell Phone

Of the three remaining variables in the outbound call problem, you have an alternative to only one of them. No matter how you dial a phone number (whether with a VoIP phone, an analog phone, or a cell phone) and which long-distance carrier transports the call, eventually, all the calls terminate to the exact same Central Office (CO) of the exact same local phone carrier. The CO then identifies who owns the phone number and sends the call down the exact same set of fiber or cables to the company's building and rings their phone system. Most companies and residences don't have redundant phone systems or local phone carriers. If they have a separate VoIP phone system running through an IP provider, you probably avoid using a VoIP carrier whose purpose is to connect your calls to traditional analog phones, and instead send your calls directly to the IP address of their SIP server over the Internet.

With that in mind, the one piece of technology that nearly everyone has access to is the cell phone. Calling from a cell phone doesn't change the local carrier's CO or the phone system of the person you're calling, but it does prove out every other variable in the call stream.
The gray oval in Figure shows the area of the call tested when you dial the destination number with a cell phone. If your call fails with the same echo or static, or terminates to the same error recording, then you know the problem, unfortunately, has nothing to do with any company or hardware with which you have the authority to open a trouble ticket.

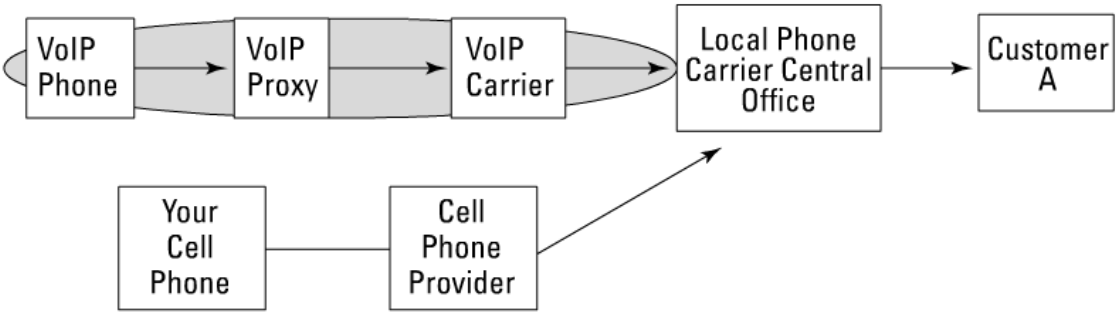


Figure: A cell phone call.

The recording you're given may vary, depending on the long-distance carrier that you use to place the test call. For example, if your VoIP carrier uses QWEST, you receive a fast busy signal, but the analog line at your office uses SPRINT and plays a recording of "all circuits are busy." If you call to the exact same number with your cell phone that uses AT&T for the long-distance portion, you may get the message that "the number has been disconnected or is no longer in service." If you make three test calls over three different longdistance carriers and they all fail, you can only believe that it's a valid failure. If not a single long-distance network can complete the call to anything but a recording, then the local phone carrier for that phone number is having an issue.

The person you're calling at Company A may already know that his or her phone system is down, and it's actually the hardware on site (not the local carrier) that's ultimately at fault. If you have the person's cell phone number, call that before you worry that Company A has gone out of business. If you don't have a Company A cell phone number, send an e-mail with a subject of Your Phone System Is Dead. That e-mail generally gets people's attention and quickly results in someone from Company A calling you back.

Troubleshooting international issues

From your perspective, troubleshooting an international call is just like troubleshooting any domestic call. You can run through the outbound troubleshooting steps in the preceding sections to isolate the issue, just as if you were calling New Hope, Minnesota. The only twist to troubleshooting international calls is that you might find some interesting similarities when your call hits different long-distance carriers.

Call treatment similarities over different long-distance carriers occur because your long-distance carrier doesn't use its own network to complete calls to every country in the world. I guarantee you that MCI, Sprint, and AT&T don't own all the phone cables and hardware in the world, and they probably don't have a staff of technicians in every country to connect your calls into Senegal, Papua New Guinea, and India. The long-distance carriers that your VoIP provider uses in turn use an

underlying carrier that's a company specifically designed for delivering international calls from the United States to a specific country or region in the world. Only so many underlying carriers provide service into each country, and every large domestic long-distance carrier probably has a contract for service with every large underlying carrier. In other words, more that one long-distance carrier uses the same path to complete calls to Tokyo or Prague.

Carriers monitor their completion rates daily to every country in the world. If you try hard enough, your VoIP carrier may even send you a list from the long-distance carrier that it uses, identifying what that long-distance carrier considers to be acceptable completion rates. Don't be shocked if you see that a completion rate of 60 percent for Western Europe is acceptable; the rate drops to around 7 percent or less for some African countries.

The long-distance carrier that your VoIP provider uses can route your international call over several underlying carriers. The choice of underlying carrier depends on the underlying carrier's completion ratios, compared with all the other carrier choices at that time, as well as the price you're paying for your international calls. Some carriers have a premium group of underlying carriers available for international calls, but they can't place you on that group of carriers because they'd lose money. If your business is focused on international calling, you might want to pay a few pennies more per minute for your calls, if you can get a better call quality or completion rate. If you're opening more than one trouble ticket every few months on international issues, speak to your carrier about a better route.

Troubleshooting an Inbound Call

Many VoIP providers use different carriers or providers for their local services, as opposed to the long-distance services. Each group (local and longdistance) requires different classes of hardware and different types of federal certification. So, a recognized local carrier that uses a class 5 switch must handle the ownership of a phone number and accept the responsibility for terminating calls to the phone number. Keep this fact in mind because your VoIP provider probably uses a minimum of two different companies to supply both the inbound and outbound VoIP service. A long-distance carrier handles all your outbound calls, and a local phone carrier receives and routes your incoming calls.

Inbound calls can come from local points of origin, long-distance points of origin, or through toll-free numbers. Regardless of how the call arrives at your office, you have to worry about only a few variables when troubleshooting:

Your Client

Tech prefix used

Your Client’s Internet provider

Your IP connection

Handling VoIP-Specific Problems

- Dealing with one-way or no-way audio
- Covering outbound and inbound calling issues
- Working with non-voice call issues
- Resolving diminishing completion with increased volume
- Reconciling the name on the Caller ID
- Considering some VoIP troubleshooting wisdom

This topic fits perfectly at the end of the troubleshooting part of this topic. Just like your investigation of any issue should begin by looking at general concerns and working your way to a specific issue, this part progresses in the same manner. topic 12 covers the theory of troubleshooting, topic 13 talks about the troubleshooting tools, and this topic covers the specific issues that can plague your VoIP traffic.
Problems such as one-way audio (or no-way audio) can crop up during a VoIP deployment, and additional maintenance issues can appear when you add on more phone lines and services. Every new VoIP phone that you install should progress through the exact same testing and burn-in procedure, executing a five-minute call from the new phone to confirm configuration and call quality. Performing your due diligence at the time that you make changes and additions prevents those new components from causing trouble down the road.

Working Outbound Call Failures

What happens when the calls fail before they ever leave your SIP proxy? Software such as Wireshark allows you to capture the data and realize that the call never left your LAN. The challenge is answering this question — why?
Your outbound call failures may be the result of an overcomplicated and insufficiently designed Routing system. It may have been designed so tightly that calls are routed based on the first 6, 7, or 8 digits of the phone number. Building routing system to this level of detail isn't inherently bad, it simply creates more work for your programmer in charge of maintaining your Dial Plan when a new area code is released and he or she must update the entire matrix.

When you build routing, make it as granular as you can, assigning a default path for all calls that don't fit the profile in the pattern matching. If you're a smaller long-distance customer, select a

carrier that can provide a flat rate or a simple rate deck that you can easily replicate in your phone system.

Handling One-Way Audio

VoIP is a unique creature because it consists of four completely separate flows of information. The overhead of the each call and the outbound audio from each end are all potentially sent on a unique path from end to end. Even the SIP and media sent from the same end over the same Internet provider may traverse different routes before landing at your Carrier.
This route variation generally has minimal impact on how the streams of information work together, but the way in which the streams interact with the intermediary VoIP nodes can have a large impact on your call quality and completion. One of the issues associated with the unique nature of the individual data paths that you may encounter during implementation is one-way audio. One-way audio isn't an uncommon problem when deploying VoIP because one RTP stream carrying the audio portion of the call can be misrouted or blocked. So, the correct IP address and port can't receive the audio, leaving only one active outbound audio stream.
Figure identifies the most common reason for one-way audio on VoIP — Network Address Translation, otherwise known as NAT. You can hide the IP address that you use within your LAN from the outside world by using NAT. NAT literally translates public IP addresses and ports visible to the public Internet into internal IP addresses and ports used within your LAN. It establishes a translation table between these IP addresses and ports, keeping the data present and available for use as long as the active transmission of data needs the connection. NAT refreshes that data every time it receives another packet from the origination site.

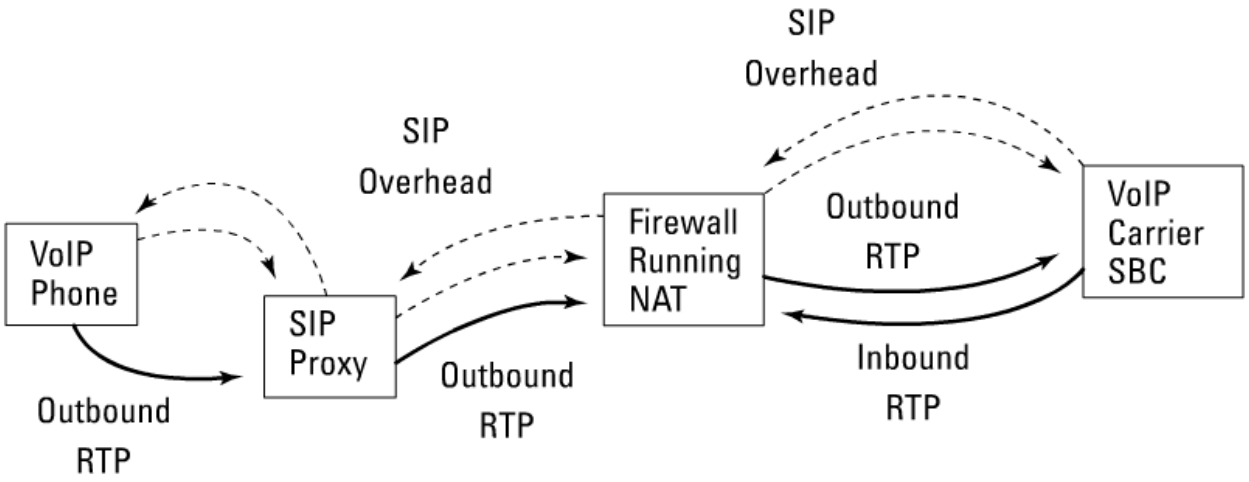


Figure: One-way audio caused by NAT.

The initial INVITE message sent by the VoIP phone in Figure identifies the RTP IP address and port of the phone to which the far end should direct its RTP. The aggregating SIP proxy takes that information and replaces it with its own RTP IP address and port to receive the media while it initiates the INVITE message sent to the VoIP carrier through the firewall. If the IP address assigned to the SIP proxy is an internal IP address and not a public IP address, the firewall blocks the incoming RTP stream from the VoIP carrier's SBC, and the audio stream is rejected because The incoming RTP stream is of a different protocol than the SIP messaging that initiated the response.

The IP address and port that receive the RTP stream didn't initiate the transmission. The call setup in Figure progresses normally with the originating VoIP node sending the INVITE, and receiving responses of 100 Trying and 180 Ringing. But when VoIP carrier's SBC sends the 200 OK, the firewall intercepts the audio, and the caller who originated the call doesn't hear any audio back from the far end.

A firewall is designed to prevent uninvited media streams from entering the LAN based on standard firewall processes of validating the origination and destination addresses, as well as the traffic type, whether TCP, UDP SIP, SDP, or RTP, and deactivating sessions that appear to be discontinued. The SIP messaging that initiates the call can traverse the NAT firewall more easily when the destination SIP node directs response transmissions to the same originating IP and port, as well as transmitting in the same protocol.

A phone conversation has two participants. If one person is long-winded and the other is simply listening, the quiet person's SIP may not be sending any packets because his or her end of the conversation has no audio and RTP isn't sent. The router that receives the incoming call may consider the data transmission complete and tear down the IP address and port information in the translation table, preventing the RTP from re-establishing, leaving the callers with oneway audio or tearing down the call entirely.

Realizing Why You Have No-Way Audio

No-way audio is more likely to occur with VoIP calls than with traditional telephony calls. The independent nature of the media streams give them much more potential to go wayward than traditional telephony, in which the audio is attached to the overhead of the call, at least for the start and finish of the transmission.

No-way audio, or the blocking/misdirection of both audio streams, can occur because of NAT traversal issues or many VoIP phone systems, such as Asterisk, require to purchase licenses to use compressed codecs, such as G.729.

Looking Over Non-Voice Issues

VoIP is designed to transmit voice calls, but fax and DTMF tones have to fit within the VoIP structure the best they can, making them prime candidates for problems. The main thing to remember about faxing over IP is that you can use the features available with your hardware only if you integrate them into the outside world with your Dial Plan. Just because your hardware says it can transcode from T.38 to analog doesn't mean that it automatically knows which phone numbers you've set up for your fax machine and automatically re-INVITEs to T.38. That's still a function of your Dial Plan, so you must design and build that out to tie the fax machine extension together to the re-INVITE to T.38.

Wireshark captures are essential in troubleshooting T.38 issues because the banter between your SIP proxy and the SBC of your VoIP carrier is more involved during this type of call than any voice call you may have.

DTMF issues are another challenge. The specific connections between the long-distance provider that your VoIP carrier uses and the local carriers that your calls use can make receiving DTMF continuity a challenge. It seems like a simple enough task, but some of these connections aren't perfectly established, so you may experience challenges in receiving consistent DTMF from and to all locations. If your phone systems depend on DTMF digits (for example, if you're running a calling card platform or other service), speak to your carrier about the DTMF transmission to ensure that it can provide consistent coverage.

Wireshark can easily capture DTMF tones. If you want the specific code required to filter for the out-of-band RFC2833 tones.

The most challenging aspect of DTMF is transmissions that include packets being sent over more than one route from your VoIP proxy to the SBC of your carrier (also called route flaps), resulting in DTMF packets arriving out of sequence. This isn't an issue as long as the receiving DTMF collector discards any packets that arrive out of sequence. If the wayward packets aren't discarded, the DTMF digit may appear to be two digits because DTMF packets interspersed with END notifications (or vice versa) make one DTMF digit appear like two.

Diving In to Inbound Calling Issues

The key to avoiding inbound calls that fail is to build all the required inbound routing for the phone numbers before they're even active at your VoIP carrier. If you're receiving new phone numbers and they won't be active for two or three days, build your phone system immediately and have it waiting for the numbers to activate. Then, schedule a test call and view the incoming call on the day it's supposed to cut over. You need to either watch your incoming call attempt through the command-line interface of your phone system or execute a Wireshark capture during the test call to ensure you're receiving the incoming INVITE and that your phone system is responding to it properly.
If you're running an array of Asterisk servers, update each and every server with the new routing information. Asterisk is an amazing software package, but it doesn't have the innate ability to network itself together through a cluster of servers. Each server running Asterisk is an island unto itself, and data cascades through the servers only if you design your own after-market software to make it happen or manually input the new routing information into each server. If you install the new phone number on only one server, your calls fail whenever a non-updated Asterisk server receives the incoming call. Again, pull a Wireshark capture to see which server received and failed the call. It should be pretty obvious because your server is probably responding with a 403 Not Found SIP response.

Troubleshooting Wisdom

Every telecom company has its strengths and its weaknesses. Some companies have an efficient troubleshooting structure, some don't. Unless you plan on buying your telecom provider and re-vamping its trouble reporting system, you have to make do with the level of service it provides — and also keep it as your friend and troubleshooting partner. If your level of service drops completely, you need to look for another carrier.
Because you're using VoIP, you have so many more options available to you than the average person who uses traditional telephony. This topic, as well as topic 12 and topic 13, allow you to narrow down almost any issue to the specific carrier responsible. If you take the time to pull the Wireshark capture, analyze it, and work through your VLM software, you can remove almost all the guesswork in troubleshooting.
In every troubleshooting conversation between technicians, someone always knows a little more than the other person. If you're the one with the more extensive knowledge, be gracious. Remember the point in time when you weren't the smartest one on the call. If you aren't the guru on the call, that means you're speaking to someone who can show you a thing or two, so ask every question about VoIP that crosses your mind. Even if it doesn't relate to the issue at hand, he or she may be able to answer it for you.
If all the troubleshooting you've done has been inconclusive, go back and start all over with a clean

slate. Identify the variables, isolate them, and prove them out one by one. After you validate a carrier or a leg of the call, don't look at it anymore. Then, narrow down the issue based on where it fits in the OSI model (see topic 5 if you'd like to know more about the OSI model). List all the potential variables that interact at that level and narrow down the troubleshooting some more. You can find the problem and fix it. Really. Stay persistent, take good notes, and there's no issue you won't be able to unravel.

Seven Common Misperceptions

- Realizing that VoIP isn't necessarily better than traditional telephony
- Accepting that VoIP isn't always worse than traditional phone systems
- Recognizing that VoIP isn't difficult to work with
- Acknowledging that VoIP really is different than traditional telephony

VoIP is a victim of stereotyping. All the challenges, problems, and grower ing pains it went through in its evolution have stigmatized it in the eyes of many people. They don't see it as an evolved technology working hand in hand with traditional telephony, but simply the clumsy, awkward protocol used by techno-hobbyists to make static-filled calls to friends overseas by using their dial-up Internet connections.

VoIP has come into its own. It's a tested and true technology that can do everything traditional telephony can do, and more. This topic covers the lingering misperceptions about VoIP, explaining their truth, their half-truth, and their complete lies. Believing that any of these ten VoIP fables are true only leads to frustration. The widespread acceptance and adoption of this technology, and the maturity of the market, has established it as a legitimate protocol that's the basis for future telephone communications.

Expecting Bandwidth Savings

VoIP is an amazing technology that can cut down on your bandwidth requirements, or it can consume more bandwidth than traditional telephony. The myth comes from the marketing. VoIP is sold as an extremely efficient, cutting-edge technology, which it can be in the hands of a skilled technician.

A standard call that uses traditional telephony consumes about 64 Kbps for the audio portion of the call and precious little bandwidth for the overhead. An uncompressed VoIP call uses the same 64 Kbps for the audio portion of the call, but it also has to grapple with the additional overhead required to form RTP, UDP, and IP packets. All this overhead translates into a single, uncompressed VoIP call that can use up to 83 Kbps, which effectively knocks out any idea of a 1:1 ratio for bandwidth use when comparing VoIP and traditional telephony.

The rumor of bandwidth-efficient VoIP does have some truth to it. Unlike traditional telephony, you have several options for compressing the audio portion of the call for transmission. Table compares the bandwidth requirements of traditional telephony and the VoIP codec options available.

Table : VoIP and Traditional Bandwidth Use

Transmission Method	Audio	Overhead	Total
G.711 Codec	64 Kbps	19 Kbps	83 Kbps
Traditional Telephony	64 Kbps	0 Kbps	64 Kbps
G.726 Codec	32 Kbps	19 Kbps	51 Kbps
G.728 Codec	16 Kbps	19 Kbps	35 Kbps
GSM (Global System for Mobile communications)	13 Kbps	19 Kbps	32 Kbps
G.729 Codec	8 Kbps	19 Kbps	27 Kbps
G.723 Codec	6.4 Kbps	19 Kbps	25.4 Kbps
iLBC (Internet Low Bit Rate Codec)	6.6 Kbps	19 Kbps	25.6 Kbps
*All VoIP codec information listed in this table is based on a 20-ms packetization interval			

Despite the variety of codecs available, don't choose one solely on the compression available. The logic used for each codec dictates the amount of time required to code and decode the voice (which creates latency), as well as the expected audio quality. All these factors reduce the field of codecs that most companies use to either G.711 or G.729.

Every VoIP carrier supports these two codecs. But if you're offering G.729 and G.711 in your INVITE message, your calls may negotiate to either one, depending on the far-end requirements. The industry standard is for the first codec choice offered in the INVITE message to be accepted, as long as the far end supports it, so keeping G.729 as the first option forces more calls to the compressed codec, and you'll see the bandwidth savings.

Believing in the Homogeneous Route Path

Customers who used traditional telephony circuits in the early days of VoIP believed that their non-VoIP connection to the long-distance carrier ensured their calls would remain a traditional telephony call from end to end. This perception was shattered when their dedicated circuits were wired to their long-distance carrier through a VoIP-enabled NGS (Next Generation Switch). Many of the customers believed that their traditional telephony calls were being corrupted by this potential conversion to VoIP, and they were determined that because they ordered a digital circuit, they wanted the calls to be digital from end to end.

The truth of the matter is that regardless of how a call reaches a longdistance carrier, either from an analog or a VoIP phone, it's routed and processed in exactly the same way. The call is converted to or from VoIP when it flows through their network and delivered to an underlying carrier. After the call is with the underlying carrier or carriers, it may be converted to or from VoIP again and again until it reaches the local phone carrier, which rings the phone belonging to the number dialed.

If any end of the call is embedded in the PSTN with a traditional phone number, the call will be traditional telephony at some point in time and may be VoIP for at least one leg along the journey. Carriers don't separate their networks, with VoIP traffic running through one side of it and all the traditional telephony calls sequestered someplace else. It costs too much to build a redundant network just to accommodate a different protocol, especially with VoIP because the telecom switches that make up the long distance carrier's network can relatively easily convert the VoIP traffic into or out of the protocol.

The only time you can guarantee a homogeneous route path is when you're sending a call from a VoIP point of origin to a VoIP endpoint, without referencing anything that looks like a traditional phone number in the INVITE message. The PSTN is built and designed to locate and route calls to phone numbers. VoIP interfaces with the PSTN to exploit the existing infrastructure for calls, so the only way to avoid the PSTN is to avoid anything in your call that looks like it belongs in the PSTN.

No current mechanisms allow you to start a call from an analog telephone in the PSTN and ring into a VoIP phone that doesn't have a phone number assigned to it. You can't just grab the rotary dial phone at grandmother's house and dial a SIP URI of wiley.voip. You may be able to place calls from the PSTN to a SIP URI in the future, but right now, no one has established a national routing guide for SIP URIs. PSTN-originated calls are connected to VoIP phones by referencing the phone number assigned to them, and they're routed just like a traditional phone call. The local carrier that owns your phone number finally converts the call to VoIP only in the last leg of the call, then sends it to your URI.

Dreading the InterOperability

Every new, cutting-edge technology goes through the awkward adolescent stage in which it can't seem to communicate well with its peers. Sometimes, all the hardware, software, and interfaces are different. One format may be Mac, the other a Windows PC. Maybe one was VHS, and the other Beta Hi-Fi. Regardless, the hardware market is always full of competitors running on different platforms or interfaces when any technology emerges. So, some hardware simply can't work with other hardware. As much as you try, that old 8-track cassette doesn't fit in your CD player.
Fortunately for VoIP, VoIP devices don't have a hardware compatibility issue. As long as each device has connectivity to the Internet, it doesn't matter whether it's a fiber-optic, co-axial, or copper connection. The IP platform that VoIP uses paved the way and eliminated these physical barriers to connectivity.
But VoIP still had challenges in the beginning. The challenges weren't that dissimilar to when ISDN was released back in the early 1990s. The industry had some uniformity for the cabling required and standards for how information would be sent. The problem cropped up because, like every written standard, two different manufacturers wouldn't necessarily interpret the specific requirements for how the overhead was going to control the individual channels in the same way. Despite the fact that you have everything set up exactly as it should be for your ISDN line, your Motorola Bitsurfer may still not work with the Livingston router that your Internet provider uses.
Many worried that the new and emerging VoIP technology would spawn hardware equally as incompatible. Yes, VoIP was amazing, and everyone who could write code was capable of drawing up their own SIP software from scratch. But on the downside, everyone who could write code was drawing up their own SIP software from scratch. The VoIP world ended up with a multitude of custom-built software phone systems, all using someone's personal interpretation of the RFC standard.
During that time, if you fired up your Linux server that ran the personal SIP code drawn up by your techie friend next door, it could very well not work with your boutique VoIP carrier. Even after modifying settings and working through all options for codecs, sampling rates, and dial plan settings, you might not have sufficient common ground to consistently pass good completed calls.
Many VoIP carriers were acutely aware of this reality and created InterOperability (InterOp) testing, which they used before releasing a prospective customer into full production because it didn't make sense to build out VoIP ports and allocate resources if the end user couldn't even complete test calls consistently.
Those days are now behind us. Open-source SIP software is readily available, and the fun of hacking your own VoIP code has been exchanged for time spent evolving an amazing dial plan based on the Asterisk software you downloaded. Asterisk and other open source software packages, allow programmers to build on them, adding the features and enhancements that they want while leaving the nuts and bolts of the VoIP software alone.
After a relatively short period of time, carriers have now done away with the pre-installation InterOp testing regime. VoIP hardware is now as likely to function with the software on the SBC of

any VoIP carrier as if it was a traditional telephony connection. The standardization is complete within the VoIP protocols, and any two VoIP platforms should be able to work together seamlessly, after all the standard parameters and options are configured correctly.

Suffering through Poor Call Quality

This specter of poor call quality was the biggest threat used against VoIP when it was first released. This myth, like the others, began a long time ago with a grain of truth. In the early days of dial-up Internet connections, people used to design their own VoIP software and call other techno-hobbyists around the world. In these early times, programmers and technicians were working through the algorithms for compression and only just discovering the impact that latency, jitter, flap, and packet loss had on call quality. In this wild and wooly time before the concept of VoIP Lifecycle Management, half the fun was just making an international call for free, even if you could make out only every third word spoken.

The technology and the industry have grown since those simpler days. Your VoIP-originated call probably is converted to traditional telephony and delivered through the PSTN to an analog phone. So, all the threat of latency and jitter is stopped when the call is converted to traditional telephony. After the call hits your long-distance network, regardless of whether it arrives VoIP, analog, or digital, that call experiences a standard call quality while it travels through to the PSTN and the terminating local carrier.

Therefore, the only specter of VoIP-induced call quality issues exist within your LAN or en route to the SBC of your VoIP carrier. You have complete control over how efficiently or inefficiently your LAN functions. If you're overloading the network and losing packets during peak data transfer times, resulting in poor audio quality, you have the power to resolve the issue.

VoIP does have more potential variables that can impact call quality than traditional telephony. These elements of VoIP calling brought about the concept of VoIP Lifecycle Management and advanced software packages that allow you to track down these issues. Call quality should no longer be a concern for any VoIP deployment, as long as you have

A well-engineered and well-managed network;

A connection to a quality IP provider that has sufficient bandwidth;

A reasonable number of hops required to reach the SBC of your VoIP carrier;

All these factors allow you to reduce the potential that your LAN or IP provider is the source of a call quality issue. After you clear that hurdle and the call reaches the SBC of your VoIP carrier without excessive latency, jitter, or packet loss, everything else in the call path is the same as if you were calling from an analog phone.

Fearing Troubleshooting

Troubleshooting, in and of itself, is a challenge, and troubleshooting a new technology is frequently a daunting task. The problem isn't that VoIP technology is inherently more difficult to pull apart and analyze, but simply that it's new. You invariably find yourself trying to build test scenarios about something, only to realize that you don't even know what you don't know about it. Huge variables could be impacting your calls that you haven't even identified as being involved in the calls.

When VoIP was initially released, the VoIP carriers and resellers probably didn't have a battalion of technicians with complete knowledge of SIP, SDP, RTP, H.323, T.37, T.38, and every codec in the industry. VoIP is a specific technology that's a hybrid of so many other disciplines that long-distance carriers rolling out VoIP service often can't find staff who have enough varied experience to quickly grasp the totality of it.

In regards to experience, everyone in the VoIP world benefits from the intense growth that the market has experienced over the past few years. The technicians have had time to figure out all the aspects of VoIP, and they've trained a new batch of technicians who may have never known anything before dealing with VoIP.

The majority of any telecommunications services troubleshooting isn't your responsibility. Do your best to help your carrier narrow down the location of the problem, but most of the standard telephony issues you encounter are probably the same ones you encountered before you switched to VoIP.

The data-centric and packet-based nature of VoIP makes it much easier to troubleshoot than traditional telephony calls. You don't have an equivalent to Wireshark or tcpdump for calls in the non-VoIP world. Your carrier must do any kind of call traps or analysis in the traditional telephony, after you open a trouble ticket, and after a technician calls back, and after that technician sets up the capture. If you have an intermittent issue, the tech might not be able to capture the data before the data they receive overloads the capture buffer of the specific program used.

VoIP allows you to execute captures on the entire call or just the overhead, and the capture remains open until you use up all the remaining available memory on the server (unless you set a limit within the capture software). If you're running SIP, you can then easily open up the capture by using Wireshark and read all the banter that's running through your VoIP server. And you can do all this yourself, in probably the same amount of time it would take to call your carrier, reach a customer service rep, and simply open a trouble ticket. If you need to open a trouble ticket with your carrier after you execute a packet capture, you can provide that capture to it, which can help focus its efforts and shorten the time to resolution.

Cringing at Complexity

The people who work with VoIP can be more intimidating than the technology itself. They speak a strange English that's peppered with acronyms, programming terms, and LAN-speak. So, getting an intellectual understanding of VoIP can be challenging because every question that you ask to clarify an acronym seems to lead to a definition in tech-ese that requires yet more explanation. The same can be said for VoIP information that you can find on the Internet or in many topics (aside from this one, of course).

Most of the available information sources assume that you've spent several years writing software, programming, and designing LANs. All these areas of
study support VoIP, and that's just the technology part. After you understand all the technical elements enough to do something with them, you still need to figure out the industry information. If you're going to use VoIP, you need to know how carriers work together to deliver a VoIP call from end to end and how the calls are rated and billed. That mountain of information still leaves room for the finer points of Local Number Portability, Caller ID transmission, and setting up a white page listing for your phone number.

Well, you don't need to know everything about all the elements used to build VoIP. After VoIP is deployed, you can use it just as easily as your standard analog telephone. Think of VoIP like an automobile — you may not know anything about electrical systems, hydraulic systems, computer programming, or internal-combustion engines, but you have no problem putting gas in the car and driving it.

The one aspect of VoIP that frightens people the most is the routing table. You may find the design and construction of the internal routing of calls and the allocation of telecom services daunting if you're starting from scratch.

The one shred of truth to the fear that VoIP is more complex than standard telephony is that, as a customer, you shoulder more responsibility for the call. Anything that impacts the call within your own network is your responsibility to identify and repair. But if you can defrag your computer's hard drive and use standard virus protection software, you can successfully use the VLM software available to clean up your LAN.

Disregarding Traditional Long-Distance Carriers

Traditional long-distance and local phone carriers are conservative entities. They run new technology through a series of tests before they release it internally for their own use. After they work out all the bugs, they release that technology to a few select and friendly customers for testing and feedback. While they do this test-and-release process, they watch the market and crunch the numbers. They have more overhead than a small boutique carrier that's running one VoIP soft

switch and has a handful of technicians.

Because of this need to run through a slow and methodical deployment of VoIP, the big long-distance companies, such as QWEST, Sprint, and Verizon, didn't offer VoIP when VoIP was still evolving. They knew that they hadn't figured out all the costs yet, and they wanted to see how big VoIP was going to be before they jumped into the market.

Well, they've jumped into the market now, every company in different ways. Some chose the high road, offering VoIP to only other carriers that use their service, and others took the low road, rolling out residential packages for homes across America. The VoIP market has by no means matured. Multitudes of VoIP offerings still have yet to be released that will come to the market in the next three to five years. The natural shift in the industry is toward VoIP, and if your long-distance carrier doesn't offer VoIP access today, just wait a few years.

One of the main reasons that some carriers are slower to enter the VoIP market is because of the hardware cost required to open up the technology. The existing networks for every carrier in America have evolved over decades, all designed around the idea of supporting traditional telephony calls. VoIP does have benefits that traditional telephony doesn't, so companies feel a definite pull to provide service. The downside to rolling out VoIP is that it entails the addition of VoIP gateways in front of the long-distance carrier's existing network backbone. So, the long-distance carriers must pay capital expense to purchase these expensive gateways and hire additional technicians to deploy them. At the same time, their long-distance customers expect them to provide the VoIP service at the same cost per minute as traditional telephony. Finally, many companies are moving to VoIP or opening up new offices with VoIP, so the market to make money exists.