Voice over Internet Protocol (VoIP) places extreme demands on your network. A slow network can be frustrating to end users as they access websites or corporate email. For VoIP environments, however, a slow network can spell disaster; poor call quality and dropped calls might mean the end of your business. This white paper examines the factors that lead to poor VoIP call quality and outlines the best practices for monitoring, analyzing, and troubleshooting VoIP networks using WildPackets® OmniPeek™.
Finding and Fixing VoIP Call Quality Issues

About WildPackets, Inc.

Since 1990, WildPackets has been developing innovative, high-quality, easy-to-use and valuable solutions to maintain the health and integrity of networks and applications. From the desktop to the datacenter, wired to wireless, distributed and local, WildPackets products enable IT organizations to monitor, troubleshoot, and secure their network systems. Sold in over 60 countries through a broad network of channel and strategic partners, WildPackets products are deployed in all industrial sectors, including 80% of the Fortune 1000. For further information, please visit www.wildpackets.com.

Driving Innovation

The networking industry continues to rapidly evolve. As a provider of world-class network analysis solutions, WildPackets both influences and monitors industry developments through active participation in industry and standards-settings organizations. WildPackets is engaged in the following organizations, which include both traditional, network standards bodies and new initiatives for establishing innovative metrics and industry interoperability.

Introduction

Voice over Internet Protocol (VoIP) is changing the rules on how we monitor, analyze and troubleshoot our networks. Unless all of your VoIP users are sitting in your data center, the only way to truly understand call quality and network performance requires you to have visibility into all your VoIP traffic—at both ends of the conversation!

VoIP, like wireless, often requires “point-of-presence” troubleshooting to see exactly what the user is experiencing. Unlike traditional data protocols, VoIP is sensitive to delays, network congestion, and jitter as it traverses your network. Network packets that pass through the core without a problem may present a totally different story by the time they reach the remote office.

This white paper examines the various factors that can lead to poor VoIP call quality (including additional information on special considerations for voice over wireless) and how a network administrator can use WildPackets® OmniPeek™ Enterprise to pinpoint issues and keep the VoIP network running smoothly and efficiently.

Mechanics of a VoIP Call

Unlike traditional telephone networks that form a circuit switched connection for a phone call, VoIP breaks up signaling and voice into packets for transmission over IP networks. Such packets can be broadly classified into three categories: signaling, voice, and reporting or monitoring.

Establishing a Connection

Before a user can begin talking, the other party must be found and a connection established. This is accomplished using signaling protocols along with proxy servers, call managers, gateways, or soft PBX switches.

The common protocols in use today are the Cisco Skinny Call Control Protocol (SCCP), IETF Session Initialization Protocol (SIP), and ITU H.323. H.323 is actually a family of signaling protocols developed for ISDN and other digital communications technology. VoIP uses a subset of selected protocols in this family. The signaling protocol is chosen by the voice application.

If a user is unable to make a connection, the problem could be in locating the user or with compatibility between the two end-points. For instance, if the end-device is located, but can’t support a specific feature required by the sender, such as conference calling, or does not have a Coder-Decoder (Codec or Vocoder) listed in the caller’s setup request, the connection will be denied.
Initiating the VoIP Session

Once a call is established (assuming the phone is answered), digitized pieces of the speaker’s voice are delivered to the listener. Some call this phase of the call the VoIP “session.” Various methods—Real-Time Transport Protocol (RTP), Time Division Multiplexing (TDM) over IP (TDMoIP), or Skype—can be used to digitize the voice data.

VoIP has become synonymous with RTP over UDP (over IP of course), which represents the majority of VoIP implementations. Technically, you could argue that VoIP is ANY digitized voice sent using IP. We’ll focus primarily on RTP and briefly mention TDM and Skype here.

- TDM occupies slots of time over a T1 circuit (or T3, DS3, etc.). TDMoIP simply takes a slice of digitized voice data from a time slot and sticks it into a UDP packet. Think of it like sending a dedicated T1 circuit over IP such as the Internet, providing circuit emulation.
- Skype is a proprietary protocol that uses low bit-rate Codecs sent in UDP packets.

Some common nomenclature is: “media type” often refers to the Codec used for the call; “media plane” or “media channel” refers to RTP; and “signaling plane” refers to SIP or H.323.

Real-Time Transport Protocol

According to RFC 3550, the latest on RTP, the purpose of RTP is to “provide end-to-end network transport functions for the transmission of real-time data.” This real-time data does not need to be voice—it can be any source of real-time data, including video.

The RFC also makes it clear that RTP does not address issues like reservation and priority, components that help with quality of service (QoS). Protocols like RSVP, 802.11p for wireless, the use of IP DiffServ—formerly Type of Service (TOS)—bits in the IP packet header, packet shaping routers switches/appliances, VLANs, and so on, are often used in conjunction with RTP to improve the quality of experience (QoE) of the VoIP user.

It is important to know that in order to realize good QoE, QoS policies must be implemented end-to-end, which is one reason why having the Internet in the middle makes for unpredictable service quality compared to private networks.

RTP is portless, which means that there are no well-known ports associated with it, unlike HTTP which is associated with port 80. The ports are dynamically assigned by the client, and communicated during call setup. RTP is encapsulated by UDP, which is a stateless transport protocol that does not guarantee delivery of the payload. Even though TCP is a reliable protocol, and does not allow packet loss to be seen by the application using it, TCP cannot be used for VoIP since the time TCP takes to recover from network packet loss is not compatible with the real-time requirements of voice. Thus, lost packets can be a real problem with VoIP networks and thus, one of a chief cause of poor speech quality.

UDP does provide a checksum to protect the integrity of voice data when it reaches the listener. There is of course, the possibility of a man-in-the-middle attack where the voice is altered and a new checksum is created. However, changing a very small 20 ms to 30 ms sample of speech is unlikely, unless there’s an attempt to garble or silence utterances of speech. Such attacks are beyond the scope of this white paper.
Monitoring and Reporting

RTP provides more than just packaging and delivery of voice data. It also contains:

- A sequence number that increments by one for each transmitted packet, and is handy for detecting lost or out of sequence packets
- The payload type which can be of a well-known type or dynamically assigned as mapped by the signaling protocol
- A sync source identifier to uniquely identify an RTP stream, and
- A timestamp set by the sender when the packet is transmitted that is handy in determining the expected packet arrival rate at the listener and for calculating jitter.

This information along with the data from Real-time Transport Control Protocol (RTCP) packets enables you to troubleshoot VoIP call quality issues.

Real-Time Transport Control Protocol Packets

RTCP packets, described in RFC 3550, are optional depending on the VoIP endpoints. They are useful, however, because RTCP type 200 (sender report) packets report on various conditions during a call in progress, including the percentage of packets lost since the last sender report, cumulative packets lost, and jitter. RTCP packets can be captured anywhere in the path between two VoIP users, and analyzed to see how many packets are being dropped according to the listener. You do not need to capture at the physical location of the end point to determine packet loss.

Factors Contributing to Poor Voice Quality

The main contributing factors to VoIP quality are: 1) variable packet delivery (jitter), 2) dropped packets, 3) end-to-end network delay or latency, 4) the Codec, 5) signal level, and 6) echo. To a lesser extent, out-of-sequence packets can also pose a problem, but this is a less significant factor due to brief packet buffering at the listener’s end (more on this later).

Factor One: Variable Packet Delivery or Jitter

Good quality VoIP relies on a nice steady delivery of packets to the listener. In reality, this is rarely the case. In some networks, such as 802.11 wireless LANs (WLANs), packets can be disrupted the instant they are transmitted by a wireless phone by other wireless users. Keep in mind that WLANs are still a shared medium like Ethernets of old. This is in contrast to the majority of today’s wired users that typically have dedicated switch ports. Furthermore, WLAN packets are often retransmitted due to RF disruptions and attenuation.

Store-and-forward and queuing congestion in switches and routers along the way can lead to further packet spacing unpredictability and thus jitter. Generally speaking, the more hops a packet has to travel, the worst the jitter. For example, VoIP packets that are sent at 20 millisecond (ms) intervals may arrive at 20, 45, 10, 15, 25, ms intervals.

Jitter Buffer

Low levels of jitter are easily handled by the jitter buffer at the receiver. Unfortunately, this solution adds additional delay to voice reaching the ear piece when other packets need to catch up. The packet stream is simply delayed for say, 40 ms, in order
Finding and Fixing VoIP Call Quality Issues

to release packets at a steadier pace compared to their arrival time.

High levels of jitter can lead to packet drops at the receiver. Figure 1 illustrates the concept of a jitter buffer.

Figure 1. Jitter Buffer

Direction Independence

Jitter is independent in either direction. If both end VoIP devices send out periodic RTCP packets then jitter (as well as packet loss) can be checked from the perspective of both endpoints, i.e. both ways. If only one device is sending out periodic RTCP packets, then you are only getting information about problems in the direction to that device.

Factor Two: Dropped Packets

Since dropped packets in an RTP media stream are not recovered, we want to do everything we can to minimize this loss of packets. Causes of lost packets include network congestion and line errors at one or more segments along the way. Another source of dropped packets, which is often overlooked, is at the client’s packet receive buffer. Due to delay and jitter, a packet is briefly held in a buffer at the receiver before releasing it to the listener. If a packet is late in arriving and the delay is longer than the length of time the previous packet can be held in the buffer, the late packet may be dropped. If too many packets are dropped in a row, the speech will sound choppy. Part of the secret sauce of VoIP handset vendors is to increase the size of the receiving buffer dynamically and try to balance packet drops vs. too much delay to the ear piece. Only the receive buffer knows for sure if a late packet was discarded, and can indicate such information in RTCP packets that are sent back to the speaker.

As packets drop, some vendors will dynamically increase the jitter buffer size and thus delay. Having a jitter buffer that’s too large can result in a talk-over situation and force the two parties to resort to more of a walkie-talkie style of conversation like this: Caller 1: “Are you there? Over. Caller 2: ‘Yes, Over.” You’ve probably experienced this on occasion when calling from cell phone to cell phone. The problem is worse when calling a user who is on a different provider’s cell network than yours.

Another part of the secret sauce of VoIP handsets is how well they fill in missing parts of speech – existing speech patterns are “bridged in” to fill the gap. This technique is known as “packet loss concealment” and works well for cases of isolated packet loss. Typically, a listener will not notice a packet or two missing every so often. On the other hand, if there is a bursty loss (a loss or discard of several consecutive packets), voice quality will suffer.
Finding and Fixing VoIP Call Quality Issues

Factor Three: End-to-End Network Delay or Latency

In an ideal network, VoIP packets would arrive at the exact same interval as when they were sent. The best quality VoIP has zero packet loss and consistent delivery of packets – not unlike an IV drip to a patient in a hospital. Unfortunately, there may be network delay from the instant a person speaks to the time the user at the far end hears it. In other words, the “mouth to ear” time can be delayed. We saw one cause of this – the jitter buffer that intentionally buffers packets at the receiver to smooth out the delivery to the ear.

Even if two users had offices right next to each other on a LAN, there may be some 40 ms of delay due to a small jitter buffer. This is insignificant until you add in additional network delay. There are various published studies of network delay, but a rule of thumb is that with an additional end-to-end delay of 250 ms (1/2 second round trip) or so, we start to talk-over each other. Usually this is not an issue except perhaps over some extremely long distances with many hops or if there’s a satellite link somewhere in the middle.

Another cause of delay is highly congested networks that lead to high jitter and a large jitter buffer and thus more delay to the ear. Sometimes the time a packet spends in a jitter buffer can be greater than the end-to-end delay of the network.

Factor Four: Codec

A Codec is an analog-to-digital (A/D) and digital-to-analog (D/A) converter. Poor voice quality can actually be a problem from the start, for instance, a problem with the sender’s audio device, depending on how frequently the voice is sampled and to what resolution (bits per sample). In general the higher the speech sampling rate, the better, but the more bandwidth consumed.

G.711a is a popular Codec that samples 8,000 samples per second (8 KHz) at 8 bits per sample or approximately 64k bits per second. This approximates the quality of voice over T1 circuits. If we include the protocol header overhead when G.711 is sent over IP, the actual network bandwidth required is the neighborhood of 80 kbps. “Low bit rate” Codecs, like G.723.1 or G.729A, sample at a lower rate, between the 5.4k to 8k bits per second, and consume about 22 to 24 Kbps on the network (the IP/UDP/RTP header sizes don’t change).

Factor Five: Signal Level

A high signal level can lead to loudness and buzzing. Conversely, a low signal level can result in inaudible and clipped speech. These problems are mostly in the analog components of the handsets or the position of the talker relative to the mouthpiece. In other words, signal level is usually not packet related, and most often can be diagnosed at the user.

Factor Six: Echo

Finally, echo can make for a miserable user experience. The primary source of echo is from analog components, such as a VoIP call via a PSTN gateway (see Figure 2). This echo can be heard during a playback of a VoIP call, but is often difficult to detect by other means without analyzing both streams simultaneously along with some sophisticated voice artificial intelligence. Tools that detect echo are outside the scope of packet analysis and require special test equipment.

The ITU P.861 Perceptual Speech Quality Measurement (PSQM) and the newer P.862 Perceptual Evaluation of Speech Quality (PESQ) are tests that can measure and include echo in the rating. The disadvantage to such tests is that a call must be setup
Finding and Fixing VoIP Call Quality Issues

through the network for each test. With WildPackets® OmniPeek™, you can analyze VoIP passively and non-intrusively (more on this later). The key advantage is that no special test equipment or loads are required to monitor on-going voice quality.

Figure 2. Echo Sources

In addition to echo from analog components, there are two other types of echo: line echo caused by crosstalk, and acoustic echo caused by a loop in the user’s handset when the microphone inadvertently picks up the caller talking from the far end.

Evaluating VoIP Call Quality

Rate the Call

There is a system for taking into account many of the common impairment factors in a VoIP call and assigning a number to the relative quality. The most common term for this is Mean Opinion Score (MOS). An alternative rating scale to MOS is an R-Factor.

Mean Opinion Score (MOS)

A MOS is determined by a group of listeners in a room listening to the same call. They can assign one of 5 numbers (no fractions) to the call:

1 – Bad
2 – Poor
3 – Fair
4 – Good
5 – Excellent

The results are then averaged to form a MOS score. The reason for the “O” is MOS is that it is truly the opinion of the listeners and is thus often called a subjective score.

In the world of VoIP, we emulate what a group of real listeners would rate a call. More correctly, we determine the predicted MOS or PMOS. Another term for this is estimated MOS. Nevertheless, MOS has become the general term for either method.

A call with a score of 4.2 is considered a very good quality call. It’s impossible to achieve a score of 5 mainly due to the bandwidth of the voice sampling. “Wideband” Codecs sample as high as 16,000 samples per second but require significant
processing and consequently are not currently in widespread use for VoIP. Further study is underway for newer technologies such as Enhanced Variable Rate Codec (EVRC) and Variable-Rate Multimode Wideband (VMR-WB).

**R-Factor**

One motivation for using R-Factor over MOS is that it scales from 1 to 120, encompassing both narrowband and wideband Codecs. With MOS, a wideband Codec may have a score of 3.7 even though it sounds better than a narrowband Codec with a MOS of 4.1. Some believe that R-Factor is more standardized than MOS and will thus produce more consistent scores between different tools. This has not been proven to be the case.

<table>
<thead>
<tr>
<th>MOS Score</th>
<th>R-Factor</th>
<th>User Satisfaction of Call Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4</td>
<td>93</td>
<td>Maximum using G.711</td>
</tr>
<tr>
<td>4.3-5.0</td>
<td>90-100</td>
<td>Very satisfied</td>
</tr>
<tr>
<td>4.0-4.3</td>
<td>80-90</td>
<td>Satisfied</td>
</tr>
<tr>
<td>3.6-4.0</td>
<td>70-80</td>
<td>Some users satisfied</td>
</tr>
<tr>
<td>3.1-3.6</td>
<td>60-70</td>
<td>Many users dissatisfied</td>
</tr>
<tr>
<td>2.6-3.1</td>
<td>50-60</td>
<td>Nearly all users dissatisfied</td>
</tr>
<tr>
<td>1.0-2.6</td>
<td>&lt;50</td>
<td>Not recommended</td>
</tr>
</tbody>
</table>

Table 1. MOS and R-Factor vs. User Satisfaction of Call Quality (Using Narrowband CODECs)

**Establish a Baseline for Quality Assurance**

Since MOS is very subjective, you should proactively study existing VoIP calls in their environment to see what the MOS scores are when users are generally satisfied with the quality.

Acquiring such data along with VoIP call quality trouble tickets from the help desk will allow you to establish a MOS baseline for quality assurance. If nothing else, a suggested starting point for suspect call quality is to further examine the packet stream for lost packets, jitter, etc., when the MOS drops below 2.8. This is only a rough guideline. Be sure to make adjustments accordingly to best fit your environment.

**Troubleshooting Poor VoIP Call Quality**

OmniPeek’s Expert checks RTCP reports, looking for both jitter and excessive packet drops, as well as including an independent analysis of RTP streams. This way, if a device does not support RTCP, you can capture RTP streams on the same segment as the listener to get jitter information close to that user.

Don’t forget to analyze at the end-points. To reiterate, the VoIP packets captured at the core is not where the call terminates. Capturing at multiple points allows you to see exactly where the MOS score drops.

OmniPeek Enterprise incorporates expert events that automatically calculate MOS and R-factor scores and can alert the network administrator when the score drops below a given threshold. Call playback, detailed MOS and R-Factor scores, jitter analysis, and packet loss and loss burst analysis are performed for each and every VoIP call over RTP, bi-directionally. Details of call signaling and reporting before, during, and after the call can also be observed. Calls can be diagnosed in real-time, either locally with OmniPeek Enterprise or remotely with OmniEngines, or analyzed “post capture” by opening saved trace files.
Finding and Fixing VoIP Call Quality Issues

Figure 3. OmniPeek Enterprise: Total Coverage for VoIP and Data Analysis and Troubleshooting

When studying existing VoIP calls remember that it's very important to analyze each side of the call independently. For instance, during a call, there will be an RTP stream from say, device A to device B and a second, completely independent RTP stream from device B to device A. It makes no sense to combine the streams when calculating MOS, as you need to know in which direction the call has degraded – you can't tell with a combined score. The section on Jitter illustrates this discrepancy.

Dropped Packets

Lost packets are detected in OmniPeek Voice by checking the RTP header sequence numbers in a VoIP stream. For instance, let's say OmniPeek is examining a sequence of 200 RTP packets as part of a VoIP call and the sequence number starts at 1001. If OmniPeek sees a gap in sequence numbers, such as 1020, 1021, 1026, 1027, 1028, it would note that 4 packets (1022, 1023, 1024, and 1025) were lost. If these were the only missing packets out of the 200, then the percentage of lost packets is 4/200 * 100% = 2%.

Jitter

A robust VoIP analysis tool must go beyond simply reporting the jitter included in the RTCP packets. It must also be capable of examining independent sources of jitter information by calculating jitter directly from the RTP packet stream itself. OmniPeek Enterprise can analyze the RTP packet stream at any point in your network, determining exactly where jitter becomes a problem. The algorithm used to calculate jitter from an RTP stream is described in RFC 3550.

The jitter analysis of an RTP stream has been enhanced to allow notifications not only when reported by an end-device via RTCP, but also in real time via RTP stream analysis as packets are captured. Having it both ways allows the analyst to better pinpoint where in the network jitter starts to become a problem, as mentioned earlier. Let's take a look at a sample call and see how jitter can yield two very different MOS scores.

One user may be perfectly happy and has a MOS score of 3.9. The other user may be experiencing difficulty as shown by a MOS score of 2.4. If we were to average the two together, we'd see a MOS score of 3.2 and the problem may go undetected by our analysis tools. OmniPeek Voice provides independent analysis of each VoIP stream.

Take a look at Figure 4, which shows two simultaneous traces, one taken near the speaker and the second near the listener.
how the voice quality drops as indicated by drop in MOS and R-Factor scores from 3.77 to 2.71 and 78 to 55, respectively. This is partly due to the increase in jitter. Note how we can rule out dropped packets—the stream being analyzed has the same total packet count (4090) at both ends. As an exercise to the reader, check out the voice stream in the opposite direction.

**Figure 4. OmniPeek Analysis Reveals a Drop in VoIP Call Quality**

OmniPeek incorporates highly accurate industry proven predicted/estimated MOS computational algorithms. These algorithms go beyond the simple ITU Recommendation G.108 for E-model used by many vendors and have been validated with independent testing comparing to human listeners of the same call. The algorithms have been licensed by WildPackets from a highly respected third party vendor that specializes in measuring VoIP quality and has already shipped over 2 million licenses worldwide. Users of OmniPeek Enterprise are assured of the best possible MOS algorithms in use today.

Another very useful diagnostic feature of OmniPeek Enterprise is the ability to play back a call in real-time.

**Late Packets**

The OmniPeek Expert system is unique in its use of packet analysis to monitor for late packet arrival as shown in Figure 5. The best placement of the analyzer for such analysis is to capture packets on a segment as close as possible to the listener experiencing problems. When “late packet arrival” events occur, there’s a good chance that many of these packets are being dropped by the receiver. We can confirm this by checking RTCP packets (if the listening device supports it). Furthermore, the OmniPeek Expert checks these RTCP packets looking for excessive packet drops.
Finding and Fixing VoIP Call Quality Issues

Additional Factors for VoIP and Wireless

There are additional considerations for VoIP over 802.11 Wireless LANs (VoWLAN). More issues can impact quality of VoWLAN, including 1) wireless retries; 2) retransmission of packets; 3) number of active users on an AP; 4) roaming; 5) DoS attacks and environmental interference, and 6) encryption.

Factor One: Wireless Retries

Despite intuition, wireless retries are far more valuable to look at than CRC errors. Like VoIP in general, analyzing wireless is best done by point-of-presence. If a wireless analyzer receives a packet with a CRC error, it doesn’t mean that the client or AP did, depending on the location of the analyzer. On the other hand, a wireless retry, on the other hand, means that a packet was received in error (or not received at all) and thus not ACKed by the 802.11 layer.

Factor Two: Retransmission of Packets

Jitter is generally compounded as packets traverse a network, but with wireless we can have major problems from the start. Once again, this is due to the shared nature of the medium with more than one user contending for air time, plus the fact that wireless is far more error prone than wired, leading to physical layer retransmissions of packets (built into the 802.11 protocol).
One of the interesting side effects of retransmitting a raw wireless frame is that we not only re-sending the same frame a second or even a third time, the transmission rate is usually lowered on successive retransmissions, say from 11 Mbps to 5.5 Mbps. Thus, the rate of sending VoIP packets becomes more variable adding to jitter. These retransmissions also shorten the battery life of our wireless device. Figure 6 illustrates what happens when an 802.11 frame is resent, and resent at a lower data rate. This is very costly to VoWLAN.

Figure 6. 802.11n frame being resent at a lower data rate

Factor Three: Access Point Load

There are numerous sources that put the maximum number of simultaneous VoIP calls per 802.11b (the majority of currently available VoWLAN handsets) at anywhere from 5 to 30. Conservatively, you should target the low end of 5 to 8 simultaneous callers. Even comprehensive site surveys for “best” coverage can be misleading—the slightest shift in physical location can have a big impact on quality—and VoWLAN users are the most mobile wireless group of all. Multistory and multi-tenant facilities compound the problem as most site surveying tools work best in flat, one-dimensional spaces.

Figure 7 shows the impact of sharing an Access Point (AP) with other users during a VoIP call. One of the users has an FTP file transfer in progress. A one-way filter was set on the source VoWLAN handset to check for consistent packet delivery by showing the delta time between packets. Note the inconsistency in the packet delivery rate and the VoIP late packet arrivals as diagnosed by the OmniPeek Expert system.

Figure 7. The Effect of VoWLAN Competition with Data Protocols
Finding and Fixing VoIP Call Quality Issues

OmniPeek Enterprise watches all flows and conversations in a converged network, voice or data, wired or wireless. This allows us to understand the impact of other applications on our real-time VoIP traffic. In fact, packets from both the wireless and wired side of an AP can be captured simultaneously at the same OmniPeek remote engine (OmniEngine). This can be accomplished by running an OmniEngine with wireless and wired connections or connected to taps from wired segments (or via switch mirror/SPAN ports) while at the same time collecting remote wireless data from an OmniPeek AP Adapter.

IEEE 802.11e (MAC Enhancements for Quality of Service) can help prioritize traffic for VoIP assuming the wireless network supports it. Since 802.11e is relatively new, some wireless vendors are still using proprietary methods for prioritization. VLAN tagging can also help, especially when using switches. Traffic for the VoIP VLAN can be prioritized within the local switching fabric. OmniPeek Enterprise can be used to monitor the effectiveness of these policies. Effective policies will show minimal change in jitter under network load.

Factor Four: Roaming

Roaming between APs can lead to clicking, brief periods of silence, and significantly worse (or better) VoIP experiences depending on the roaming protocol (fast roaming for instance), load on that AP/channel and environmental noise.

With OmniPeek Enterprise, you can position the analyzer where you can receive a good signal from both APs and simultaneously scan the two channels of interest to see if the user successfully completes the switchover in short order (50 ms or less).

Factor Five: Denial of Service Attacks and Environmental Interference

DoS attacks and environmental interference can also impact the VoWLAN experience. The OmniPeek Expert detects a number of DoS attacks and can also display the signal/noise ratio of each received packet, depending on the wireless card/driver. If there are a large number of wireless retransmissions by a client or AP and the signal is strong at both ends with moderate traffic on the channel, environmental interference such as from microwave ovens, cordless phones, and to a lesser extent, Bluetooth devices, is suspect.

Factor Six: Encryption/Decryption

Encryption/decryption can add additional delay to the call as well as impact our ability to analyze VoIP calls on the wireless side. Many VoIP handsets still use WEP.

OmniPeek has the ability to decrypt WEP and WPA pre-shared key (PSK) packets when the static key is available. In the event of repeatable problems with VoWLAN calls, you can perform temporary test calls without encryption to see if OmniPeek Enterprise identifies problems at the upper layers and to obtain MOS/R-Factor scores. If there are serious issues suspected on the wireless side, the fifty plus physical layer OmniPeek wireless experts will help immensely in pinpointing the problem. You can also set a one-way filter on the MAC (physical device) address of a VoIP user in question, and look at the delta time between packets for consistent spacing to see if they are being affected by re-transmissions and other anomalies.
Conclusion

In every industry, real-time network monitoring and rapid troubleshooting have become mission-critical. Network disruptions are now business disruptions, with financial and sometimes even legal consequences. More than ever, you need solutions to monitor and troubleshoot problems wherever they are occurring on the network, quickly and efficiently, so that business and other essential IT operations are not disrupted.

OmniPeek Enterprise is a "VoIP early warning system," providing core VoIP analysis with its included VoIP decodes and Expert system technology. Whether viewing network activity for application usage, protocol distribution, node activity or the network packets themselves, or leveraging built-in Expert network analysis, OmniPeek and OmniEngine probes together enable you to visualize global network performance and analyze root cause failures more quickly and effectively than any other solution.

VoIP Abbreviations and Terms

Access Point - Provides connectivity between wireless and wired networks

EVRC - Enhanced Variable Rate Codec

MAC - Physical device

MOS - Mean Opinion Score

PESQ - Perceptual Evaluation of Speech Quality

PMOS - Predicted Mean Opinion Score

PSK - Pre-shared key

PSQM - Perceptual Speech Quality Measurement

QoE - Quality of experience

QoS - Quality of service

RTCP - RTP Control Packets

RTP - Real-Time Transport Control Protocol or RTP Control Protocol

SCCP - Skinny Call Control Protocol

SIP - Session Initialization Protocol

TDM - Time Division Multiplexing

TDMoIP - Time Division Multiplexing over IP

TOS - Type of Service

VMR-WB - Variable-Rate Multimode Wideband

VoIP - Voice over Internet Protocol

VoWLAN - Voice over Wireless LANs
Finding and Fixing VoIP Call Quality Issues

OmniPeek™ Product Family

The OmniPeek Product Family gives network engineers real-time visibility into every part of the network—simultaneously from a single interface—including Gigabit, 10GbE, Ethernet, 802.11 wireless, VoIP, and WAN links to remote offices. Using OmniPeek’s local capture capabilities, centralized console, distributed engines, and Expert Analysis, engineers can rapidly troubleshoot faults and fix problems, restoring essential services and maximizing network uptime and user satisfaction.

The OmniPeek Product Family comprises OmniPeek network analyzers and consoles, as well as distributed OmniEngines, which analyze and store data at remote locations on the network.

Capabilities include:

- Complete distributed network and VoIP troubleshooting and analysis
- VoIP real-time and post-capture analysis
- Call signaling and media analysis
- VoIP specific expert that diagnoses events
- VoIP specific protocol decodes
- Call playback
- Quality of call scores
- VoIP performance analysis
- VoIP graphs and reports
- Visual Expert – graphical view of the call flow
- Multi-NIC support
- Expert ProblemFinder settings that include description, possible causes, and possible remedies
- Peer Map - a continuously updated graphical view of traffic between pairs of network nodes, showing volume, protocol, node address, and node type
- Alarms, triggers, and notifications—all user-definable

Learning More

- “Introduction to Wireless Networking” is the first in a three part series. It covers wireless network architecture, topologies and security issues.
- “Getting the Most from Your Wireless Network” is the second in a three part series. It outlines best practices in monitoring, analyzing, and troubleshooting wireless networks.
- “Finding and Fixing VoIP Call Quality Issues” is the third in a three part series. It examines a specific use case and identifies factors that lead to poor VoIP call quality and presents best practices for keeping quality of service high.

All of these white papers and more can be found at www.wildpackets.com under the “Downloads” section.