Series 6300 Radio-over-IP Gateway

This application note is intended to inform potential users and installers of the common applications for the Series 6300 RoIP Gateway, and precautions that will help ensure a successful deployment.

Voice Applications

The most common voice applications for the RoIP Gateway is to connect radio control equipment (such as desktop remotes or radio dispatch consoles) to radios by replacing the existing analog wireline circuit with an IP network. This section focuses on the wireline circuit interfaces.

4-Wire Circuits

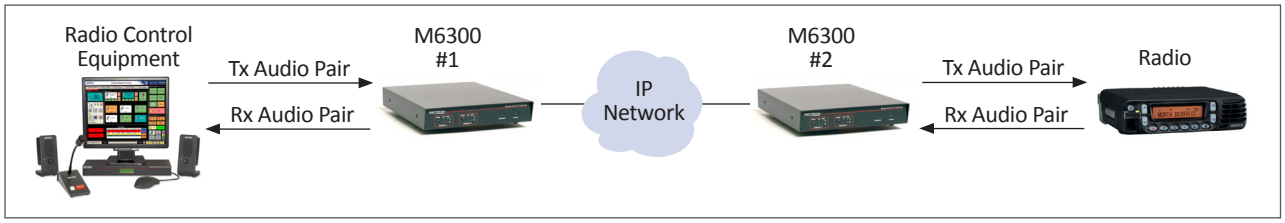

Figure 1. Typical 4-Wire Circuit Application

Four-wire

Four-wire circuits are made up of two balanced pairs of wires; a transmit pair to pass audio towards the radio, and a receive pair to pass audio from the radio. In order to control radio transmissions on a 4-wire circuit, the industry has employed two general techniques; DC Remote Control (DRC) and Tone Remote Control (TRC). DRC superimposes a DC current on the transmit audio pair to provide this radio control, whereas TRC sends a burst of "in-band" tones at the start of a radio transmission, followed by summing the voice with a low-level in-band tone. The RoIP Gateway is directly compatible with TRC. However, external equipment, such as Zetron's Model 251 and possibly third party equipment must be added to the RoIP Gateway to allow it to use DRC. Please contact Zetron's technical support department for more details on using the RoIP Gateway in DRC applications.

6/8-Wire Circuits

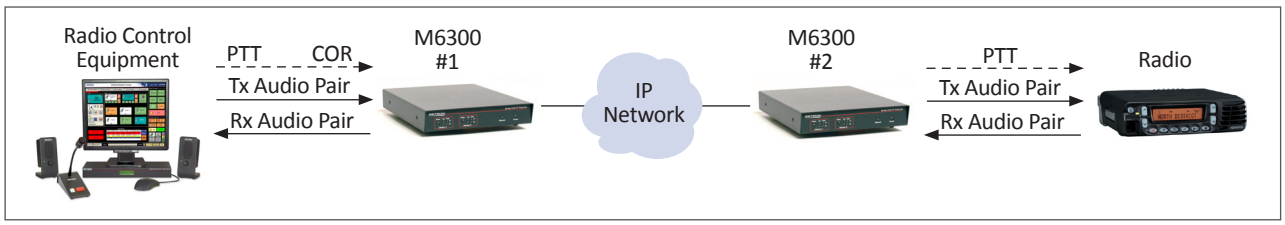

Figure 2. Typical 6-Wire Circuit Application

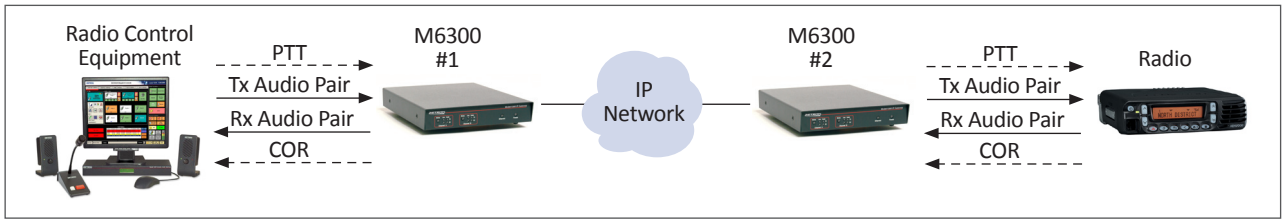

Figure 3. Typical 8-Wire Circuit Application

Six-wire
Six-wire circuits are made up of a two balanced pairs of wires for voice, plus one additional pair for transmission control (Push-to-Talk or PTT). This PTT pair replaces the need for control signals superimposed on the transmission pair of a four-wire circuit. This is commonly known as "Local Control".

Eight-wire
Eight-wire circuits are essentially the same as a six-wire circuit, except that it adds one more pair to convey status of the receiver (Carrier Operated Relay or COR). An eight-wire is also known as an "E&M" (or Ear & Mouth) circuit. Because the RoIP Gateway has provision for connecting external PTT and COR signals, it is compatible with both six and eight-wire circuits.

Precautions When Using In-Band Tones
Land Mobile Radio (LMR) frequently makes use of audible, in-band tones. Some common tones are TRC, paging tones, alert tones, and Push-to-Talk ID tones. "In-band" means that the tones are sent to/from the radio as audio, just like voice. However, sending tones on an IP network does take special consideration.

Most Voice-over-IP (VoIP) equipment, including the RoIP Gateway, has the ability to compress audio to reduce its network bandwidth requirements. These voice compression techniques are tailored to voice, but don't work as well for tones. Consequently, the higher the voice compression, the more distorted the tones become. Therefore, when you plan to make use of in-band LMR tones, be sure to minimize your voice compression, using either 32 kbps or preferably, 64 kbps voice data rate.

The other consideration when sending tones is that if an audio packet is lost on the IP network, the tone decoding equipment on the far end will not be able to decode the tone. When an occasional audio packet is lost for voice, the impact is the loss of an occasional syllable, which the human listener makes up for by context. But when a portion of tone is lost, the tone decoders can not compensate for the lost information. Therefore, to eliminate lost packets it is imperative to make sure that the IP network which conveys the audio is well designed and has plenty of excess capacity. This task is made much easier when an IP network is dedicated only for use with the RoIP Gateway rather than being shared with other unpredictable applications.

Serial Data Applications & Precautions
The RoIP Gateway supports asynchronous serial data as well as voice. The supported electrical interfaces are RS-232 and TTL, with baud rates up to 38.4 kbps. Note that the Gateway's serial port supports only the data signals, not the handshake signals (such as RTS/CTS, DSR/DTR). In typical LMR applications, the uses for the serial data include receive voter status/control, radio control head data and radio programming data. There are several factors however, which can effect the success of using the RoIP Gateway in some of these applications.

If the application is to pass radio control head data, make sure that the control head electrical interface is compatible with the RoIP Gateway. Most radios use something other than RS-232 or TTL, and some require the availability of serial data handshake lines. Thus, it may be necessary to use external media conversion equipment to make the radio's serial port work with the RoIP Gateway's serial port.

Another consideration is the effect of the IP network on the data. All IP networks cause latency or delays from end-to-end. Larger networks cause more latency. Some serial data protocols used by radios are unable to tolerate any significant latency. Thus the delays of an IP network may prohibit the reliable use of serial data.

Lastly, the RoIP Gateway is designed to support short bursts of data rather than a continuous data stream. Assuming a good IP network is used, it can support reliable transport of bursts of data up to 256 bytes long. But if data bursts are significantly longer than this, data may be lost. Radio programming typically uses bursts that are significantly longer than 256 bytes.

Given these consideration, it is prudent to discover as much as you can about the data requirements of your specific application, and do a trial test in a minimal deployment before committing large resources to a wide spread deployment.

IP Network Considerations
This section is an introduction to generic Voice-over-IP installation issues (including RoIP) written for semi-technical readers. For a more in-depth review of technical issues relating to VoIP, please see Zetron's Understanding VoIP white paper, document 005-1389.

There are two essential things needed for a successful Zetron Voice-over-IP (VoIP) installation (VoIP applications include Radio-over-IP or RoIP); they are the right IP network and the right knowledge. And a third thing is helpful – a definition of success.

Let's start with the definition of "success". If the VoIP system is to carry mission-critical voice, then success means no or very, very little disruption of voice and radio transmissions. For example, **although the human mind can make up by context for the loss of an occasional syllable, it can't easily distinguish between "shoot" and "don't shoot" if the word "don't" is missing.** But if the VoIP system is to carry non-critical voice, then some slight or moderate disruption of voice and radio transmissions may be acceptable.

The Right IP Network
Next, let's consider the IP network. Unlike the old analog, copper wire days of point-to-point circuit switched networks, an IP network is designed to carry data from a number of different users, and a number of different applications. Of course it is possible to create a single-purpose IP network dedicated to a task such as VoIP, but doing so may defeat one of the prime advantages of an IP network which is its ability to be used for multiple purposes. So let's assume that you are going to put a VoIP system on an existing IP network. That means that both voice (VoIP) packets and other packets (presumably non-voice data) will be traveling the IP network at the same time. If there is sufficient bandwidth in the network compared to the payload of the devices connected to the network, the VoIP system should meet the definition of mission-critical success on that network.

LAN vs. WAN Bandwidth

It is fairly easy and inexpensive to create a high-bandwidth "internal" Local Area Network (LAN) within a single building to help ensure that the bandwidth-to-payload ratio stays high. However, it can become more difficult once the traffic makes its way onto some Wide Area Network (WAN) if the "external" bearer has limited or unpredictable bandwidth. The bandwidth of various bearers is mostly a function of how much monthly fee the user is willing to pay for service. DSL speeds of 100-200 kbps are fairly inexpensive. Cable and WiMAX are often in the 0.5 to 5 Mbps range (speed may vary depending on loading by other users). DSL and Cable are generally used for public (Internet) rather than private networks, where security can be an issue, and where bandwidth can not generally be guaranteed. T1 and E1 are 1.5 or 2 Mbps respectively which can have less bandwidth than Cable or WiMAX, but they do offer a guaranteed bandwidth, and they can be used for a private (non Internet) network. Fiber offers the best bandwidth, but at a cost generally higher than other options.

Data Vs. Voice Traffic

It is hard to quantify how much payload data-traffic uses unless intelligent network equipment is configured to intentionally control the amount of payload allowed through. Without such limits, data applications can briefly take up the entire available bandwidth of a limited pipe such as a T1 or E1 circuit (e.g. during file downloads). Unlike VoIP applications, where lost packets are audibly recognized, dropped data packets are usually not recognized by the application user. This is because data packets have built-in retry mechanisms – if one gets dropped, the same packet is sent again until it makes its way through the network. However, with VoIP packets, there are generally no such retries – lost packets are usually not recovered. Thus the most notable effect of lost data packets is increased delay in getting the data (e.g. web pages take longer to load, etc.), but the notable effect of lost voice packets is gaps in the received audio – missing syllables and words. A sparse number of dropped packets is usually unnoticeable to a data user, while still very noticeable to a voice user. For this reason **a network that may have been perfectly adequate for data-only applications, could be unacceptable for voice applications.**

While VoIP traffic is unforgiving of packet loss, its load on the network is thankfully fairly predictable – a function of the number of calls in progress (see Figure 4A). But data traffic, although forgiving of packet loss, is usually unpredictable (see Figure 4B).

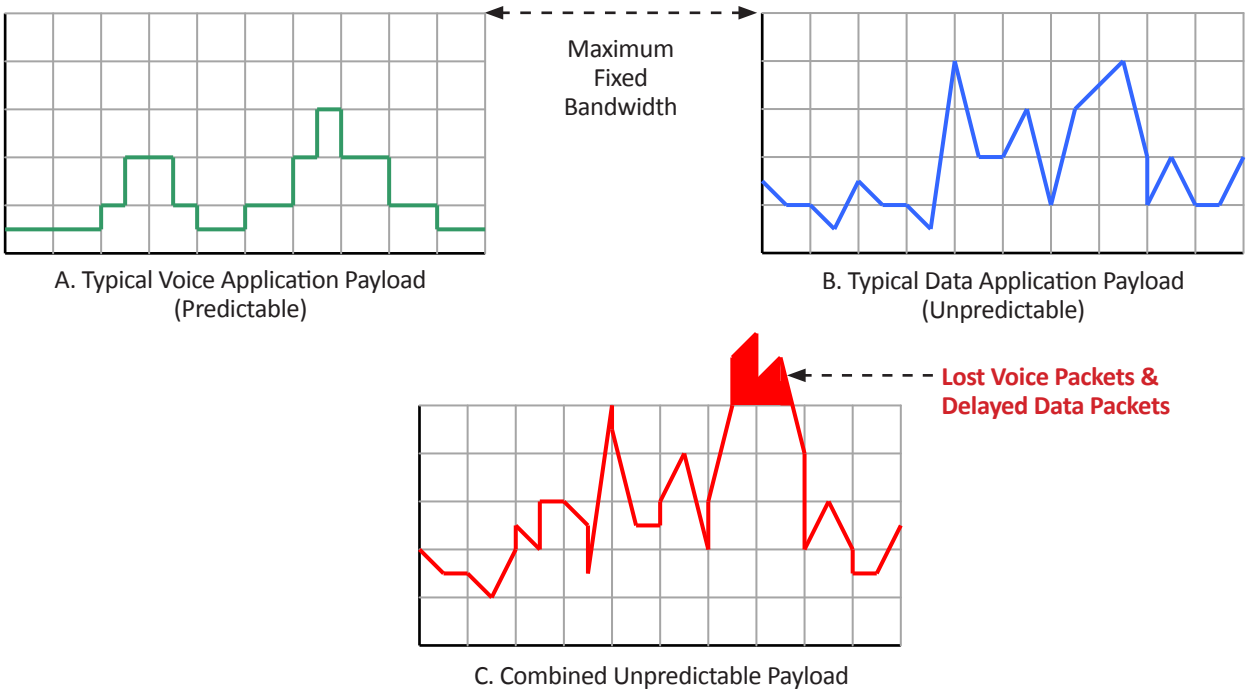

Figure 4. The Effects of Multiple Applications on a Fixed Bandwidth (Private) Network

Shared Private vs. Public Networks

The goal of making VoIP reliable is hampered when the bandwidth-to-payload ratio is unpredictable. The problem with shared private networks (even LANs) is that the combined payload is not only variable but often unpredictable (see Figure 4C) and the more applications that share the network, the more unpredictable it becomes (see the sidebar for potential solutions to this problem). The problem with public networks (like the Internet) is that the bandwidth is variable – its theoretical maximum reduced by traffic from public users (see Figure 5). If either the bandwidth or the payload are variable and the degree to which they vary is unknown then the bandwidth-to-payload ratio is unpredictable.

The best network for mission-critical VoIP traffic is one in which both the bandwidth and the payload are predictable and which has ample spare bandwidth left. That usually means avoiding public networks, and knowing or controlling how much peak payload traffic all applications on a private

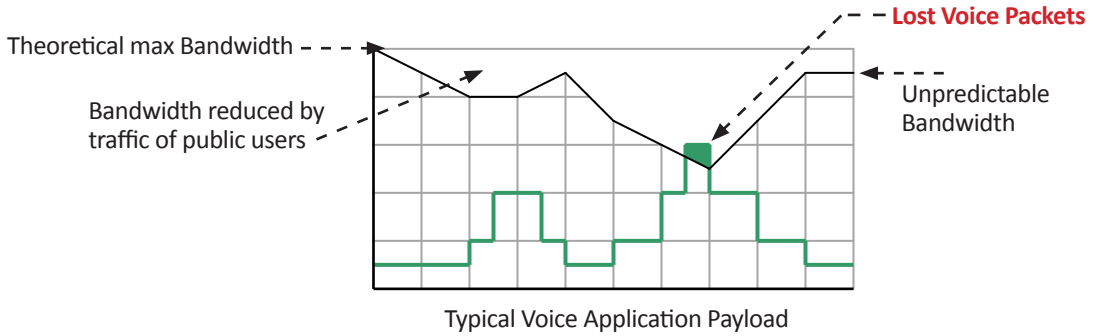

Figure 5. The Effects of a Variable Bandwidth (Public) Network on Applications

network are generating. **The easiest of all configurations to reliably support mission-critical VoIP is a private, dedicated (non-shared) network.**

The Right Knowledge

This brings us to the other key to success, and that is the right knowledge. By this we mean the knowledge of the technical staff planning and installing the system. The planning staff need to know how to calculate, measure and/or control traffic on the target network, so that they can determine the peak payload being used. And they need to know the end-to-end bandwidth capability of the target IP network. Then they should compare this against the payload, delay and jitter requirements of the VoIP system (which can generally be found on the product specification sheet). This information will then tell the technical staff whether or not the VoIP system is compatible with the target network.

The installation staff will need to know to configure equipment to work on the IP network; they must be familiar with IP addresses, IP ports, routers, switches, and the like. Basic computer networking skills may be sufficient if the installation is occurring only within a dedicated LAN, but **if an IP network includes shared traffic or multiple subnets or a WAN, then the installation staff should be qualified IT professionals.**

Non-Critical Applications

What about non-critical applications? The problem with considering the non-critical definition of success is that if you have a network that can't carry mission critical traffic, then it may be on the ragged edge of being acceptable for non-mission critical traffic – depending on how non-important the "non-critical" voice is. When operating with payload near the available bandwidth, a slight increase in shared payload, or a slight decrease in network bandwidth can increase the dropped packets from just an occasional syllable, to whole sentences. This could significantly inhibit the ability to receive even mildly important voice traffic.

Solutions for Shared VoIP & Non-VoIP IP Traffic

When there is no choice but to put your VoIP application on the same network as other applications, there are some things you can do to help ensure that the VoIP packets are not lost. The solution is to use a priority scheme that gives VoIP packets higher priority than other traffic. This can be done by proper setup of configurable routers and switches; by giving priority to the switch & router jacks to which VoIP equipment is connected, or by giving priority to IP addresses and ports numbers used by VoIP traffic. Better networking equipment also allows you to specify the priority of VoIP packets themselves so that intelligent routers and switches in the network deliver the VoIP packet with priority end-to-end. But beware that you can only provide such priority on the private portion of the network you control – not on traffic which flows through a public network such as the Internet.

Using the Internet

Zetron never recommends putting mission critical voice over the Internet (the worst of all public networks) because once on the Internet there is no way to ensure necessary bandwidth. Also, there is no provision in the Internet infrastructure to prioritize voice packets over other traffic. There may be special tunneling devices (or services such as VPN) that improve voice packet delivery, but no device or service can absolutely guarantee loss-less delivery over the Internet. However, the Internet may work just fine for non-critical voice, especially casual monitor-only audio.

ZETRON

www.zetron.com

Zetron Americas
PO Box 97004, Redmond, WA USA 98073-9704
(P) +1 425 820 6363 **(F)** +1 425 820 7031 **(E)** zetron@zetron.com
Zetron EMEA
27-29 Campbell Court, Bramley, Hampshire RG26 5EG, United Kingdom
(P) +44 (0)1256 880663 **(F)** +44 1256 880491 **(E)** uk@zetron.com
Zetron Australasia
PO Box 3045, Stafford Mail Centre, Stafford QLD 4053, Australia
(P) +61 7 3856 4888 **(F)** +61 7 3356 6877 **(E)** au@zetron.com

027-0185B November 2012