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

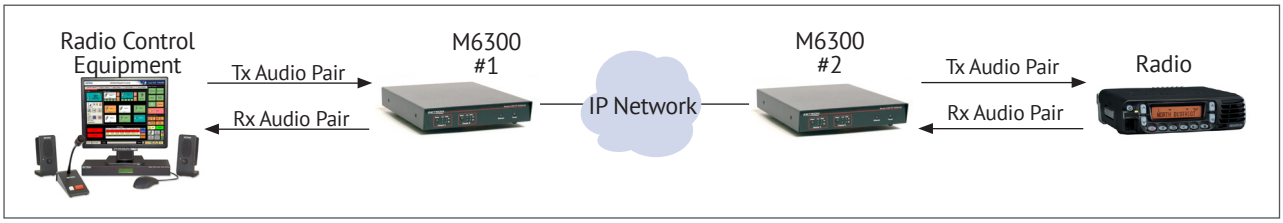

Figure 1. Typical 4-Wire Circuit Application

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

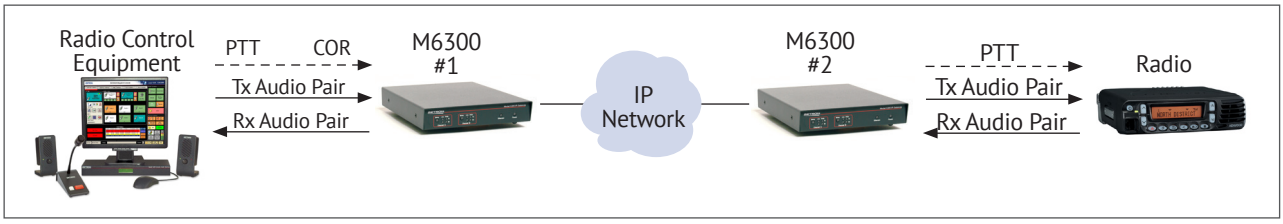

Figure 2. Typical 6-Wire Circuit Application

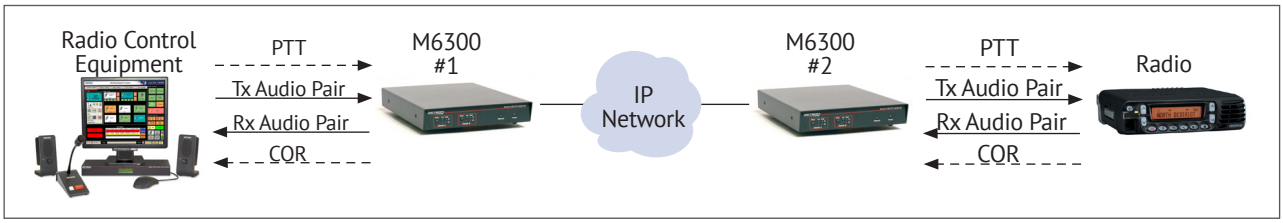

Figure 3. Typical 8-Wire Circuit Application

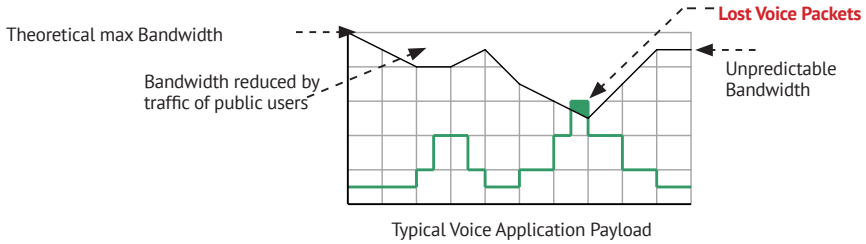

Figure 5. The Effects of a Variable Bandwidth (Public) Network on Applications

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

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 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

www.zetron.com

The Power to Respond

027-0185C April 2018