

Region 10 Videoconference Network (R10VN)

Network Considerations & Guidelines

1 What Causes A Poor Video Call?

There are several factors that can affect a videoconference call. The two biggest culprits are packet loss and duplex mismatch. In this document, we offer considerations and provide some guidelines to avoid and/or alleviate these problems. But first, here is a little bit about what a videoconference endpoint does when it is impacted by one or both of these problems.

1.1 What the VC gear expects

In the best of all worlds, the VC Codec (Coder-Decoder), also described as an endpoint, would receive every packet transmitted, it would arrive on time, in the exact order it was sent and with no jitter, latency or lag. Unlike PCs, H.323 videoconference devices can not ask for packets to be retransmitted if they do not arrive or arrive with errors. Since the video is near real time, they require a robust network to insure delivery.

1.2 What happens if packets are lost or arrive out of order?

A VC Codec watches the amount of errors it is experiencing. It understands that audio delivery is the most critical. In order to maintain the voice, at all costs, it will actively down speed the video stream to give more priority to the audio. It may even decrease the screen size or, temporarily or permanently, freeze the video. If packet loss is extensive, you may also experience broken or garbled audio. If audio quality is bad there is normally a serious problem with packet loss on the network. The device attempts regularly to recover but, based on the quantity of errors, may be unable to redisplay video.

2 Considerations & Guidelines

2.1 WAN Connectivity and Bandwidth Planning

2.1.1 Network Bandwidth

Network bandwidth is the data rate that can be supported by your network connections and pipelines. Network bandwidth can refer to the theoretical limit or to the actual usage. Most often when people discuss network bandwidth they are talking about the perceived speed of their local area network, but network bandwidth alone does not measure speed. The latency or lag, or delays in processing, associated with the network also affects the speed of the network. Network bandwidth monitoring can identify bottlenecks as well as underutilized pipelines and must be part of the planning process.

2.1.2 Network Bandwidth - Capacity Planning

Another reason to monitor network bandwidth usage is for capacity planning. You need to know how network bandwidth usage fluctuates at different times of the day as well as from month to month if you are to make an informed decision about capacity growth or contraction. Bandwidth planning requires that you evaluate two different metrics: the total bandwidth and the highest bursting bandwidth.

2.2 Connectivity from Telcos and Internet Service Providers (ISPs)

Connectivity and bandwidth planning must also be accomplished when connectivity is ordered from independent ISPs or telephone companies. For a videoconference to be successful, all LAN configurations and conditions recommended in this document must

also be considered for circuits ordered through Telcos and ISPs. It is crucial to provision your circuit with enough bandwidth incoming and outgoing to handle all of your site's video, voice, and data applications, and to allow for a reasonable amount of growth.

2.3 Quality of Service

To insure that voice and video traffic on your internal network gets the highest priority through the various routers and switches it is suggested that, if available on your equipment, Quality of Service is enabled. Video and voice packets will be given the highest priority, over other data packet types, since these packets are expected to arrive at their destination near real-time.

2.4 LAN Configuration

2.4.1 Wiring

On local area networks (your campus or building network), Category-5 (or better) horizontal network wiring or fiber optic vertical wiring is necessary. If wiring does not meet this minimum specification, it will be necessary to upgrade it.

2.4.2 Switched vs. Hub Networks

R10VN recommends a switched 100 Mbps Ethernet connection to all videoconference end-points. Switched Ethernet provides a more controlled and reliable connection for your data traffic than do data hubs. Switches are normally intelligent and know the direct path to a given device. Data hubs, on the other hand, use a broadcast methodology to find devices. This creates an undo amount of traffic on the various legs of your network. Broadcast traffic uses up bandwidth and creates packet congestion which and can result in lost packets and, cause latency & jitter.

2.4.3 Videoconference Bandwidth

The industry standard videoconference call is made at 384 Kbps. For a 384 Kbps. call you will use roughly 416 Kbps. of bandwidth on your network. The R10VN MCU and other endpoints can also support the lower speeds of 128 and 256 Kbps. The lower the speed the less video quality the participants experience. If there is a mixture of sites with different speed capabilities, the MCU uses transcoding to bridge the different rates together. Depending on the equipment being connected, there may be an issue that the event will down speed to the lowest common denominator. IP connection must provide enough bandwidth to support IP video applications at the selected bandwidth of the call.

2.4.4 Duplex Mismatch

Duplex mismatch is the number one cause of packet loss and video freezing. The switch port that a videoconference end-point is connected to MUST match the the VC device Ethernet card duplex setting. When possible, both the endpoint port and the switch port may have to be hard-coded to match duplex and speed capabilities. R10VN will assist the clients to make certain that duplex settings match switch settings. The R10VN recommends hard codeing switch ports connected to a videoconference device to 100 full duplex.

2.5 LAN Network Segmentation

The R10VN may recommend segmenting your Local Area Network, changing out hubs for switches, or possibly buying more WAN connectivity. A detailed assessment of your current network configuration will allow you to determine your network needs.

Segmentation can be accomplished either physically or virtually by creating a VLAN specifically for videoconference traffic. A VLAN will segregate the videoconference traffic for all other traffic on your network and eliminates congestion that may be affecting packet delivery to the VC gear.

2.6 Firewall Configuration, NAT or Private IP Addresses for Videoconferencing.

1. If the video conferencing system is an appliance (not PC Based) you can connect the device outside the firewall or in a public DMZ with a public IP address. Refer to the section covering System Security and Password Protection to secure and protect your endpoint from intrusion.

2. Connect the VC device inside the firewall with a private NAT address and forward all H.323 related ports to the IP address of your video endpoint. Make a rule that will allow any IP address to and from the IP address of your endpoint for all ports listed in the table below. Port forwarding of IP video traffic is one option that can be used to enable two-way communications with your video system. A more reliable and secure option is to use an H.323 proxy or a firewall traversal solution. Refer to the section covering System Security and Password Protection to secure and protect your endpoint from intrusion.

3. Establish the end point behind firewalls and use the endpoint software to limit the number of ports that need to be opened. A firewall technician will then need to make exceptions to and from this IP address with the specified ports. Some equipment manufacturers, Polycom for instance, allows you to keep the large port range 1024-65535 closed and open only 6 ports 3230-3235 for audio, video and control. This is known as using fixed ports.

4. Establish the end point behind the firewall and use the STNS Backend firewall traversal solution. R10VN can provide you information on this inexpensive way to circumvent firewall configuration issues and, once purchased, can assist you with setup and configuration. The service uses only one well-known port (443) to pass video traffic through your firewall. The rule of thumb is if you are able to check your bank balances from inside of the network, the STNS device is generally a plug and play solution to firewall traversal. With this solution the video system's IP can be assigned via DHCP and the VC device is assigned an E.164 alias. The STNS takes care of routing the incoming call to your VC device by sending the call to the system's alias. This service allows both outgoing and incoming calls to your unit with no special firewall configuration. This solution is the preferred method of handling NAT and firewall traversal because it allows your video system to use both its dial-in and dial-out features. IP Video bridging and scheduling services have the ability to dial into your system if they powered on and available.

2.7 Gatekeeper Registration

When a client subscribes to R10VN Services their video endpoint is configured to register to the R10VN gatekeeper. Each endpoint is assigned a unique number that follows the TEA assigned school numbering system. It is sometimes referred to as an E.164 number. Registering to the R10VN gatekeeper allows other locations to dial your site using both the IP address AND the GDS number. In cases where your unit is behind a firewall or using NAT, the GDS number may be the only way for someone to dial into your site.

2.8 Site Certification

Each site that subscribes to the video services provided by the R10VN will be certified for operation on the video network. It is recommended that prior to scheduling a

certification, your video endpoint is at a location that will not be changed. Certification to use the network is not only given to the video endpoint but the entire network connection including network switches, routers, firewalls, cabling, and circuits. If firewall configuration or network topology changes after an end point has been certified, recertification will be necessary. Recertification will test the recent changes and ensure that future conferences are launched at an acceptable quality level. The R10VN supports several major manufacturers of videoconference equipment.

3 Glossary of Terms

Definitions provided by Wikipedia

3.1 Duplex Mismatch

In Ethernet, a duplex mismatch is a condition where two connected devices operate in different duplex modes, that is, one operates in half duplex while the other one operates in full duplex. The effect of a duplex mismatch is a network that works but is often much slower than its nominal speed. Duplex mismatch may derive from manually setting two connected network interfaces at different duplex modes, but also derives from connecting a device that performs autonegotiation to one that is manually set to a full duplex mode.

3.2 Ethernet Hub

A network hub is a fairly un-sophisticated broadcast device. Hubs do not manage any of the traffic that comes through them, and any packet entering any port is broadcast out on every other port. Since every packet is being sent out through every other port, packet collisions result--which greatly impedes the smooth flow of traffic.

3.3 Ethernet Switch

A network bridge (commonly termed a switch), operating at the Media Access Control (MAC) sublayer of the data link layer, may interconnect a small number of devices in a home or office. This is a trivial case of bridging, in which the bridge learns the MAC address of each connected device. Single bridges also can provide extremely high performance in specialized applications such as storage area networks. Once a bridge learns the network topology through a spanning tree protocol, it forwards data link layer frames using a layer 2 forwarding method directly on the path to the destination device and not on paths to other devices.

3.4 Jitter

Jitter is an unwanted variation of one or more characteristics of a periodic signal in electronics and telecommunications. Jitter may be seen in characteristics such as the interval between successive pulses, or the amplitude, frequency, or phase of successive cycles. Jitter is a significant factor in the design of almost all communications links (e.g. USB, PCI-e, SATA, OC-48). In clock recovery applications it is called timing jitter.

3.5 Latency or Lag

In computing and especially computer networks, lag is a term used where the computer freezes and then continues some time later when an action is performed, for example clicking a mouse button. If there is different latency, such as distance between computers connecting, the term used is delay although many get it mixed up with lag. Latency is the time taken for a sent packet of data to be received at the other end. It includes the time to encode the packet for transmission and transmit it, the time for that data to traverse the network equipment between the nodes, and the time to receive and decode the data. This is also known as "one-way latency". A minimum bound on latency

is determined by the distance between communicating devices and the speed at which the signal propagates in the circuits (typically 70-95% of the speed of light). Actual latency is much higher, due to packet processing in networking equipment, and other traffic.

3.6 Packet Loss

Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination. Packet loss is distinguished as one of the three main error types encountered in digital communications

3.7 Quality of Service (QoS)

In the field of computer networking and other packet-switched telecommunication networks, the traffic engineering term quality of service (QoS) refers to resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice or video over IP, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required.

3.8 Videoconference Codec

A codec is a device or computer program capable of encoding and/or decoding a digital data stream or signal. The word codec is a portmanteau of 'compressor-decompressor' or, most commonly, 'coder-decoder'.

3.9 VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices. VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. By definition, switches may not bridge IP traffic between VLANs as it would violate the integrity of the VLAN broadcast domain.