

Network Considerations for IP Video

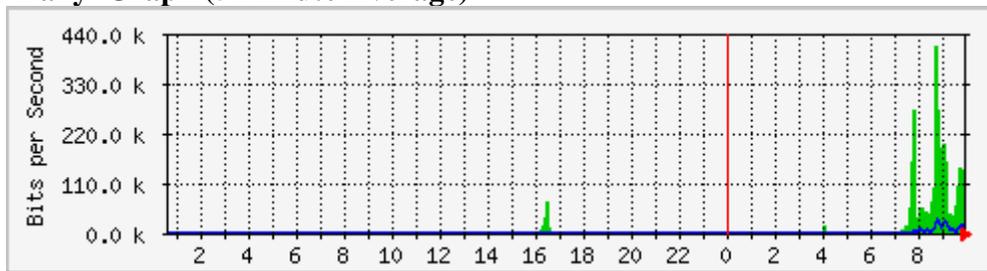
H.323 is an ITU standard for transmitting voice and video using Internet Protocol (IP). It differs from many other typical IP based applications in that it is a real-time application using dynamically assigned ports and has higher and more sustained bandwidth requirements. IP Video requires limits on end-to-end delay (latency), the variability of that delay (jitter) and packet loss. Implementation of IP video on your network will require you to address various issues outlined below.

The ICN Access Link

IP video will introduce new traffic to your ICN connection that may be different than most now traversing the link. For example a typical business quality videoconference at 384 kbps will actually require steady bandwidth in the 480kbps range. The rule of thumb is video connection speed plus 25% for H.323 protocol related overhead. Current link utilization should be reviewed to determine how video might affect the link. Bandwidth used by a video call will be unavailable to other applications while it is active. ICN RTC staff <http://www.illinois.net/rtc/rtc.htm> can provide utilization reports. A sample is shown below:

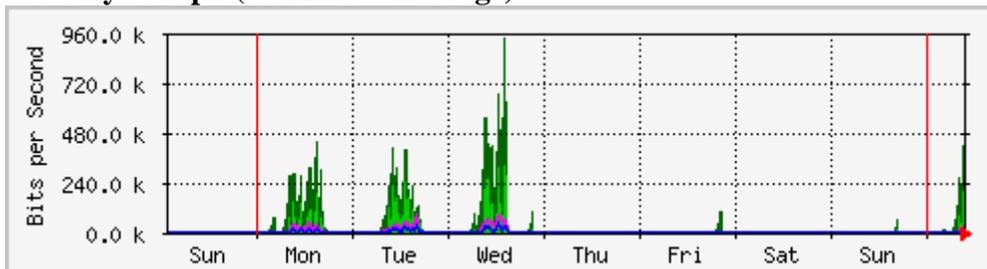
The statistics were last updated **Tuesday, 26 November 2002 at 9:59**, at which time '4-Kk-site xxxx had been up for **222 days, 16:39:54**.

`Daily' Graph (5 Minute Average)



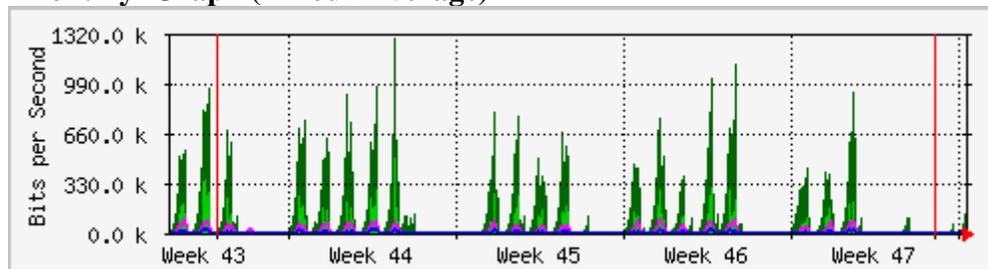
Max **In**:426.4 kb/s (27.6%) Average **In**: 29.8 kb/s (1.9%) Current **In**:328.1 kb/s (21.3%)
Max **Out**: 49.2 kb/s (3.2%) Average **Out**:4120.0 b/s (0.3%) Current **Out**: 27.7 kb/s (1.8%)

`Weekly' Graph (30 Minute Average)



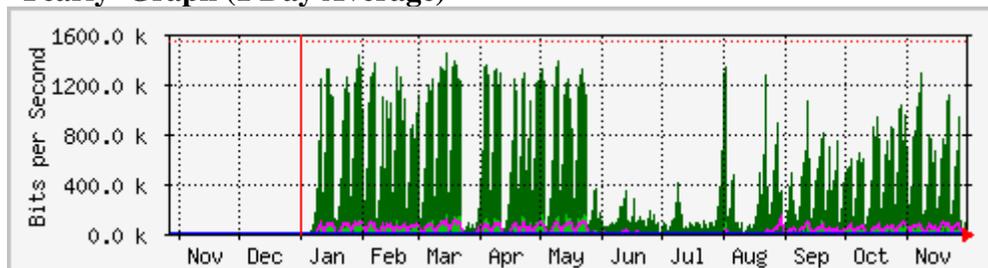
Max **In**:1133.4 kb/s (73.4%) Average **In**: 37.0 kb/s (2.4%) Current **In**: 71.3 kb/s (4.6%)
Max **Out**: 100.8 kb/s (6.5%) Average **Out**:4808.0 b/s (0.3%) Current **Out**:8240.0 b/s (0.5%)

`Monthly' Graph (2 Hour Average)



Max **In**:1296.4 kb/s (84.0%) Average **In**: 37.4 kb/s (2.4%) Current **In**:6856.0 b/s (0.4%)
Max **Out**: 108.6 kb/s (7.0%) Average **Out**:4576.0 b/s (0.3%) Current **Out**:1752.0 b/s (0.1%)

`Yearly' Graph (1 Day Average)



Max **In**:1466.4 kb/s (95.0%) Average **In**: 38.3 kb/s (2.5%) Current **In**: 32.1 kb/s (2.1%)
Max **Out**: 147.9 kb/s (9.6%) Average **Out**:3720.0 b/s (0.2%) Current **Out**:4512.0 b/s (0.3%)

GREEN ### Incoming Traffic in Bits per Second

BLUE ### Outgoing Traffic in Bits per Second

DARK GREEN### Maximal 5 Minute Incoming Traffic

MAGENTA### Maximal 5 Minute Outgoing Traffic

If you have multiple links and are utilizing per packet load balancing a change to per destination load balancing will be required. Per packet load balancing will cause packets to arrive out of sequence and result in poor video quality. RTC staff can advise you as to options you have in regard to load balancing.

A Quality of Service (**QoS**) policy is essential for successful H.323 video performance. It prioritizes traffic and provides appropriate bandwidth to ensure that latency and jitter are within acceptable levels. Latency refers to a slow or delayed signal stream while jitter results from digital communications being slightly out of synchronization – both are disruptive of high quality video. The ICN has deployed a differentiated services Internet Protocol (IP) QoS policy that will provide video bandwidth with equitable network resources.

These technical deployment rules or policies will accomplish three things:

- 1) Classify video packets at the network edge with access control lists (ACLs)
- 2) Mark video packets with IP Precedence information, and
- 3) Appropriately queue video packets with Low Latency Queuing (LLQ) to ensure quality video signal.

We recommend establishing QoS on your connection to the ICN to provide video traffic the priority it needs to function properly. This will guarantee the video application the bandwidth it needs only when it is active; allowing the bandwidth to be used by other applications when video is not in use. You can review the ICN QoS white paper at <http://www.illinois.net/reports/QoS.doc>.

Network parameters for successful H.323 video are shown in the figure below:

<i>Element</i>	<i>Value</i>
Jitter	Less than < 30ms
Packet Loss	Less than 1%
Latency	150 – 200ms one way

Source: Cisco AVVID Network Infrastructure Enterprise Quality of Service Design.

Router

QoS requires specific IOS, features, Flash and DRAM. Your router may require an upgrade. In general your router must support LLQ (Low Latency Queuing) and WFQ (Weighted Fair Queuing). ICN RTC <http://www.illinois.net/rtc/rtc.htm> staff can verify current router capabilities and provide quotes for upgrades for ICN managed routers.

Firewalls

A firewall most likely exists in your network as part of an overall security policy. Unfortunately firewalls can be a barrier to the implementation of H.323 applications. H.323 requires voice or video endpoints to establish data communication channels with each other using IP addresses and multiple data ports. Some ports are considered “well known” and therefore static while others are dynamically assigned. The table below describes the ports used by H.323.

<i>Port</i>	<i>Type</i>	<i>Purpose</i>
1718	Static UDP	Endpoint discovery of gatekeeper.
1719	Static UDP	Gatekeeper RAS, registration, admission and location requests between endpoints and gatekeepers.
1720	Static TCP	Endpoint-to-endpoint call setup requests.
1503	Static TCP	T.120 Collaboration
1024 – 65535	Dynamic TCP	H245 set up messaging between endpoints
1024 – 65535	Dynamic UDP	RTP/RTCP (Real Time Protocol/Real Time Control Protocol) audio and video data streams.

Firewalls typically allow users to request information from devices outside their own network but allow return responses only to that originating IP address and specific port and typically do not honor unsolicited incoming requests. IP video endpoints must “listen” on port 1720 for initial call setup messages (i.e. an incoming video call- which is unsolicited) and then be able to pass audio and video via ports dynamically assigned and agreed upon by the endpoints. Both of these actions are in conflict with firewall policies.

Network Address Translation (NAT)

NAT is a process that allows a local-area network (LAN) to use one set of IP addresses for internal traffic and a second address or set of addresses for traffic destined for external networks. NAT is used as a means of securing the LAN and to allow use of readily available internal addresses versus possibly scarce external globally routable addresses. NAT devices at the LAN edge make the translations between the internal network addresses and the external globally routable addresses enabling data transfer to occur. While this works for most applications it causes problems when using H.323 applications. H.323 embeds the originating IP address in the actual data packet payload and this IP address is the one used by the receiving end to establish communications. In networks using NAT this embedded IP address is not routable and as a result the call will fail.

Some Video Codecs provide a built in solution to the NAT problem including Polycom and Tandberg. If you are purchasing new endpoints and utilize NAT consider codecs that offer this feature.

Firewall and Network Address Translation Traversal

Multiple solutions for NAT/firewall traversal of H.323 exist; not all are viable for security and/or cost reasons and apply depending on network size etc. They include:

<i>Potential Solution</i>	<i>Issues</i>
Locate Video Systems outside the firewall	No access to internal network devices. Exposes systems to abuse. Limits control. Not recommended
Establish separate voice and video networks with separated security policies	Costly due to duplication of devices and resources. Not recommended.
Open ports on the firewall	Not secure. Not recommended.
Utilize H.323 “aware” Firewalls / Application Level Gateways (ALGs)	Some firewalls offer the capability to perform filtering at the application level and perform NAT proxy functions. Cisco, Checkpoint, Raptor, Netscreen, and Gauntlet offer ALG capability. Check with your firewall vendor to determine if this is a viable solution.
MCU in a DMZ	MCUs with a NIC facing both the internal network and external network (some with built-in NAT proxy capability) can offer a secure solution; this can be costly and is overkill for networks with few video endpoints.
Tunneling	Secure tunnels are created between networks wishing to pass H.323 between them. Not scalable. Not recommended.
Semi-Tunnels/Transparent Traversal	Client/server software is used to establish connections via well-known ports under control of a central server in a DMZ.

LAN

Typically if you have switched 10/100Mbps Ethernet to the desk- top there should be no issues with running video on the LAN. The key is that your network is a switched not a “shared” network (Hubs and even low capacity switches will result in poor video quality). Be sure that the speed and duplex settings on the video

device and the switch port match, mismatches will result in poor video quality. If problems persists check ports for errors, i.e. is the cable or the port actually bad and causing errors.

If no errors are detected and the switch ports and devices are matched and ports and cabling are functional there may be congestion on the LAN. If this is the case the options for QoS are:

- ◆ Set ports serving video endpoints as high priority on switches
- ◆ Establish a VLAN specific for video
- ◆ Utilize 802.1p Layer 2 QoS services to prioritize video traffic

Additional resources

H.323 tutorial:

<http://www.iec.org/online/tutorials/h323/topic01.html>

Firewall/NAT white papers:

<http://www.wainhouse.com/files/papers/WR-trans-firewalls-nats.pdf>

<http://www.radvision.com/NR/rdonlyres/162F9E89-5DB2-4F74-9A08-06E79B24944D/1015/RADVISIONFirewallCookbook.pdf>

http://www.polycom.com/common/pw_cmp_updateDocKeywords/0,1687,3026,00.pdf

ViDe cookbook

<http://www.videnet.gatech.edu/cookbook>

Manufacturers:

Polycom

<http://www.polycom.com>

Radvision

http://www.radvision.com/index_noflash.php3

Sony

http://bssc.sel.sony.com/Professional/markets/market_10010.html?m=10010

Tandberg

<http://www.tandberg.net/>

VCON

<http://www.vcon.com/>

Vtel

<http://www.vtel.com>

Zydacron

<http://www.zydacron.com/mainsite/products.htm>