New England Systems and Software Inc.
1100 Altamont Ave, Mitchell Drive
Schenectady, NY 12303
(518) 377-4057

Successful IP Video Conferencing White Paper

The success of an IP video conference is dependent on two things: c*onnection* to the remote system and *consistent* bandwidth during a call. Connection to a system is important for obvious reasons. Once connectivity is established, consistent bandwidth determines the overall quality of a call. A connection does not need to be fast, but it does need to be as reliable as possible. A consistent connection at 128-256Kbits/s using H.264 can be quite usable. A connection that peaks at 512Kbits/s but may drop to 64Kbits/s occasionally will generally be unacceptable. The SchoolStation/N-Station systems are state of the art video conference units and will produce the best quality conference as possible with the bandwidth available. However, the systems cannot overcome a poorly designed network or an oversubscribed Internet connection.

The methods below are have been tested by New England Systems. When properly implemented, these methods will generally provide a quality video conferencing experience.

ACCESS

- In a non-routed, non-firewalled LAN environment, there should be no access issue for any SchoolStation/N-Station video equipment. This is usually described as a *flat network*.
- In a routed LAN environment, access lists can limit connectivity between devices. All access lists must allow traffic between the networks and specifically the video conferencing endpoints. Configuration of router access lists is outside the scope of this document, but in most cases if the video conferencing units can communicate via ICMP (ping), video conferencing should work.
- In a firewall environment two things must be available: a suitable IP address and proper open ports. A Stateful Firewall should be required in any modern network installation. A Stateful Firewall is aware of an outbound connection to a remote device and the fact that this device may need to establish its own separate connection back to the calling system. The Cisco PIX is one such firewall. As the most common firewall implemented there are some standard configuration texts provided below. If a PIX is deployed in your network, be certain it is running version 6.3 or newer code. There are known video conferencing problems with previous revisions.

New England Systems and Software Inc.
1100 Altamont Ave, Mitchell Drive
Schenectady, NY 12303
(518) 377-4057

Suitable IP Address:
Each video conferencing endpoint MUST have a unique Internet IP address assigned to it if calls are to be made across the Internet. This IP address CANNOT be shared between devices; each video conferencing unit MUST have its own Internet IP address. The address can either be directly assigned to the VCU (video conferencing unit) or you may use NAT (Network Address Translation) to assign an Internet IP to a VCU with an internal address. PAT (Port Address Translation) is not sufficient or supported.

See the NAT example code for a Cisco PIX firewall at the end of this document.

Open Ports:
Across any firewall the appropriate ports must be opened. The ports required are defined as part of the H.323 (video conferencing over IP) standard. These ports are as follows:

389	TCP	ILS v2.0 Registration (LDAP)
1002	TCP	Win 2000 ILS Registration
1503	TCP	T.120
1718	TCP	Gatekeeper Discovery
1719	TCP	Gatekeeper RAS
1720	**TCP**	**H.323 Call Setup**
1731	TCP	Audio Call Setup
1024-65535	**TCP/UDP**	**Dynamically Assigned RTP AV Streams H.245, and RTCP ports**

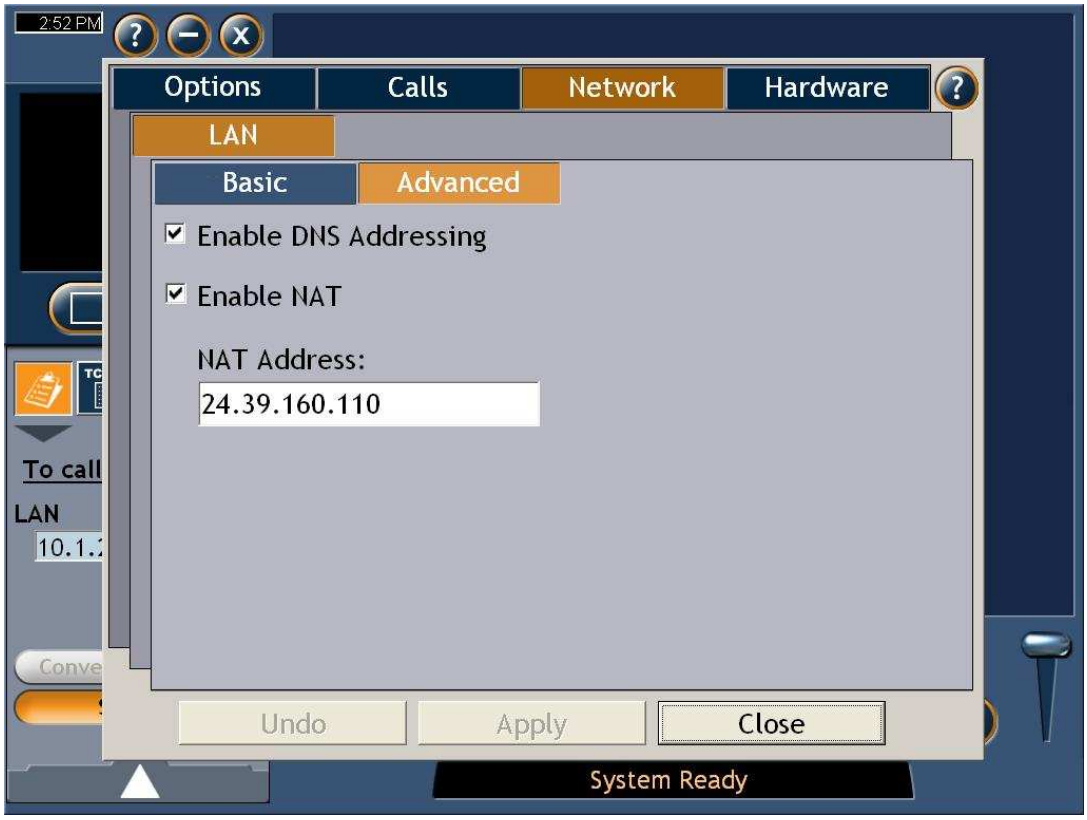
The ports in bold are the absolute minimum required for video conferencing, the remainder are used for enhanced features.

Cisco PIX H323 fixup:
This setting should generally be disabled.

See the NAT example at the end of this document for sample configuration.

SchoolStation/N-Station NAT:
The SchoolStation/N-Station may (or may not) require a NAT entry in the software to properly establish a connection to a unit outside your network. The address that would need to go in this field would be the EXTERNAL address assigned to the unit in your firewall. You should VERIFY the BOTH internal external calls still work after changing this entry. In rare instances, certain networks will require toggling of this field on/off to complete outside calls.

New England Systems and Software Inc.
1100 Altamont Ave, Mitchell Drive
Schenectady, NY 12303
(518) 377-4057



New England Systems and Software Inc.
1100 Altamont Ave, Mitchell Drive
Schenectady, NY 12303
(518) 377-4057

Bandwidth Considerations

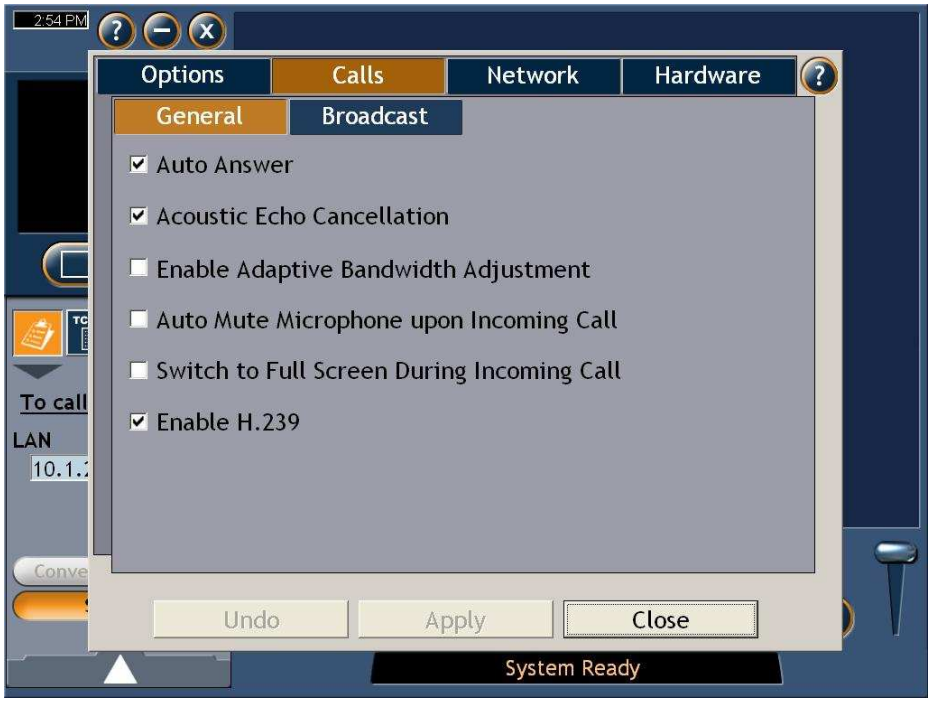
Having consistent bandwidth required by video conferencing can be a challenge. There are several factors that impact the availability of bandwidth to the system. In order to help alleviate this issue, our SchoolStation/N-Station Systems support both IP Precedence and DiffServ. The TCP/IP protocol was simply not designed to enforce strict QoS. Some network applications, specifically Peer to Peer file sharing programs, may cause network congestion regardless of the QoS methods deployed.

Ethernet Port Settings

Please make sure that the port settings are correct on your equipment all the way up the chain. In other words, you need to insure that if you have the SchoolStation/N-Station set for 100MB/Full Duplex, all the other devices upstream are set the same way. Allowing real time sensitive systems to "Auto-Negotiate" is a bad idea. Cisco networks particularly will have a habit of mis-matching ports under the Auto-Negotiate setting. Mismatched settings will portray themselves as poor quality calls that look like low bandwidth. Such things are not normally visible in a straight data network.

Dynamic Bandwidth Adjustment

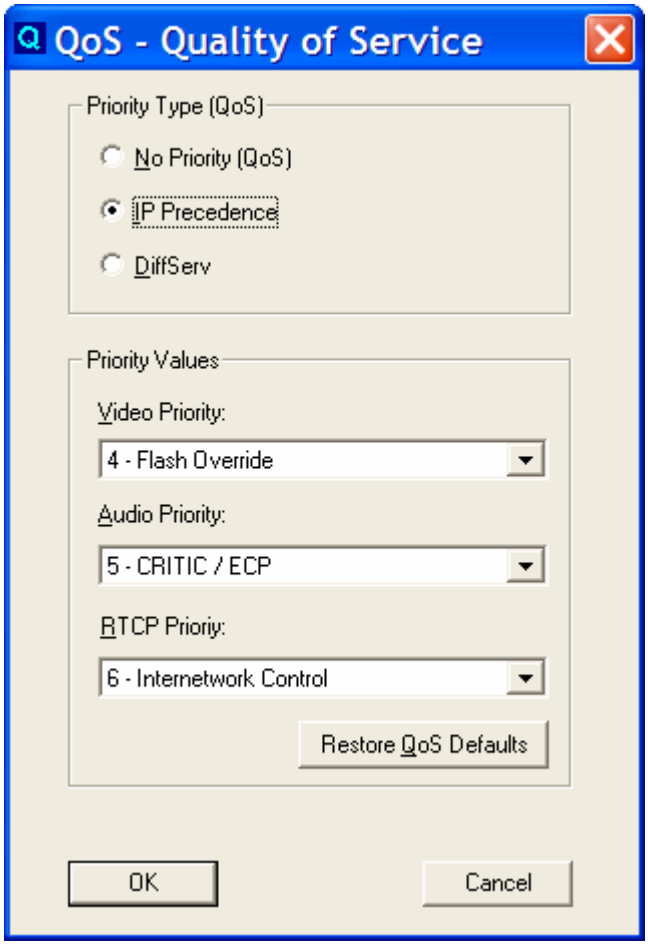
Every SchoolStation/N-Station system has a "Dynamic Bandwidth" adjustment. This setting forces the unit to slow down the video call should the network become congested. Unless there is a specific reason to turn this setting on, leave it OFF.



New England Systems and Software Inc.
1100 Altamont Ave, Mitchell Drive
Schenectady, NY 12303
(518) 377-4057

QOS

The settings for these QoS services can be made on a SchoolStation/N-Station by executing QOS.EXE found in C:\program files\hd4000.



Note that there are separate settings for Video, Voice and RTCP communication. Our recommendation is that you use the default settings for either IP Precedence or DiffServ whichever can be configured on your network devices. Note that Priority 5 is the highest setting allowed for normal data. Priority 6 and 7 are reserved for network control.

New England Systems and Software Inc.
1100 Altamont Ave, Mitchell Drive
Schenectady, NY 12303
(518) 377-4057

Configuring Your Network Devices for QOS

In most LAN environments, the default QoS settings are acceptable. Generally there is sufficient bandwidth and routing/switching performance in the LAN that the normal best effort method of IP connectivity will yield an acceptable video conference.

In a WAN environment, attention must be paid to the WAN link. In many environments, this link can easily be saturated by streaming media, peer to peer applications, or large email attachments. QoS may help the performance of videoconferencing in this type of situation.

Cisco IOS routers have a vast QoS feature set, explained here:

http://www.cisco.com/en/US/products/ps6558/products_ios_technology_home.html

For basic IP priority settings, see here:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800ca59a.html

In a small environment, in which no other QoS settings exist, you may enable QoS for your SchoolStation/N-Station as follows:

y.y.y.y = SchoolStation/N-Station IP address. In the example below, y.y.y.y would be attached to the LAN which accesses interface Ethernet0.

Define the list:
access-list 10 permit host y.y.y.y
priority-list 1 protocol ip high list 10

Apply it to an interface:
interface Ethernet0
priority-group 1

New England Systems and Software Inc.
1100 Altamont Ave, Mitchell Drive
Schenectady, NY 12303
(518) 377-4057

Advanced QOS

Care should be taken when configuring QoS, as these settings may have a detrimental effect to other real time network applications, such as VoIP or streaming video. DiffServ is not recommended due to its conflict with Windows Servers.

IP precedence guide is here:

http://www.cisco.com/en/US/tech/tk39/tk824/technologies_configuration_example09186a00080094ad1.shtml

Note that this guide is written for ATM interfaces, however the same commands will work for Ethernet or Serial interfaces.

A DiffServ guide is available here:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800bd9ed.html

Diffserv involves peering agreements between routers and networks. It is not generally used for Internet connections. The Cisco guide to Diffserv is available here:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800bd9ed.html

SAMPLE NAT CONFIG:

Inside IP address of VCU – x.x.x.x
Outside (public) address of VCU – y.y.y.y

static (inside,outside) X.X.X.X Y.Y.Y.Y netmask 255.255.255.255 0 0

Example:
Your ISP or network administrator has assigned you a public address of 64.24.1.8

The internal address of the VCU is 10.1.1.50

```
static (inside,outside)10.1.1.50 64.24.1.8  netmask 255.255.255.255
```

When Using Conduits:

conduit permit tcp host X.X.X.X eq h323 any

```
conduit permit tcp host 64.24.1.8 eq h323 any
```

New England Systems and Software Inc.
1100 Altamont Ave, Mitchell Drive
Schenectady, NY 12303
(518) 377-4057

When Using Access Lists:

access-list INBOUND permit tcp host X.X.X.X eq h323 any

```
access-list INBOUND permit tcp host 64.24.1.8 eq h323 any
```

To apply the access list to your outside interface

```
access-group outside_coming_in in interface outside
```

Turn off H323 fixup as follows:

```
No fixup protocol h323
```