

SchoolView

Technical Guide

In support of SchoolView Versions 9.1.x.

SchoolView

Table of Contents

Site Survey Considerations.....	1
Why perform a Site Walk/Survey?.....	1
Things to Consider	1
Existing “Common Zone” speakers.....	1
Existing clocks.....	1
Existing Displays.....	1
Technician / Installer Profile.....	2
AV Industry Training from AVIXA	3
About AVIXA.....	3
AVIXA Training.....	3
Recommended Applications / Tools	4
Software Applications	4
Other Tools.....	4
Training Resources	5
Recommended Equipment List	6
Why do we recommend specific equipment?	6
Security Cameras	6
Motion JPEG Cameras and Servers.....	7
Network Path Information.....	7
Axis.....	7
Panasonic	8
Vivotek	9
Displays (Projectors / Flat Panels).....	10
Video Encoders.....	11
Video Decoders	11
System Diagrams	12
Wiring Considerations.....	12
UTP Cable Recommendations	12
Button Labels.....	13
Speaker Cabling Considerations	15
Classrooms (typically 8-ohm speakers)	15
Common Zones (typically constant voltage, distributed, 25v or 70v systems).....	15
Speaker Choices.....	15
Network Requirements.....	16
Bandwidth Considerations	16
SchoolView specific network requirements	16
Unicast and Multicast Transmissions over the Network.....	16
Cisco IP Multicast Guidelines.....	16
Considerations for IGMP and MLD Snooping Switches.....	17
SV Mount	17
Classroom Equipment Trays.....	18
Tray Component Placement Layouts	18
Tray Parts List and Pin-out	19
Audio & Video Equipment Racks.....	20
Rack Wiring and Connection Considerations.....	20
Power Requirements	21

SchoolView

UPS Considerations.....	21
Example Rack Layouts.....	22
Unified Campus – Single Rack.....	22
Unified Campus – Dual Racks - Audio.....	23
Unified Campus – Dual Racks - Video.....	24
Bell & PA Audio Rack.....	25
SchoolView Hardware Configuration.....	26
Touch Panel Configuration.....	26
NetLinx Master Configuration.....	32
ATS Clocks Connection.....	38
Telephone Interface Configuration.....	39
Other Audio Device Connections.....	40
Head End Audio Sources.....	40
Common Zone Amplifiers.....	40
Barix Audio Encoder/Decoder Configuration.....	41
Barix Serial Rescue.....	43
Video Decoder Configuration.....	46
Enzo Configuration.....	46
SVSI Configuration.....	52
Spinetix HMP-350 Players.....	58
Classroom Touch Panel Configuration.....	58
Classroom Keypad (MET-7E) Configuration.....	58
Locating the IP Address of the Keypad.....	58
Modifying Keypad Connection and IP Settings.....	58
Simulating the ID Pushbutton.....	59
Toggling Between IP Addressing Modes: DHCP and Static IP.....	59
GL-300 Configuration.....	60
RF Receiver Configuration.....	60
Display Driver Creation.....	61
Overview.....	61
Acquiring XDD Driver Files.....	61
Importing XDD Driver Files.....	61
XDD Modifications for Schoolview.....	62
Removing Unused Input Sources.....	63
Adding an Input Source.....	64
Editing Signal Types.....	64
Ordering Input Sources.....	65
Adding Source Commands.....	65
Entering Source Commands.....	65
Creating a Driver File.....	66
Modifying Driver Files to Remove Command/Response Footer.....	66
Exporting an XDD file.....	68
Other Classroom Device Connections.....	69
Display Control.....	69
Classroom Audio.....	69
Two Way Classroom Microphones.....	69
Admin iPad Touch Panel Configuration (Optional).....	69
Site Readiness Checklist.....	74

SchoolView

Commissioning Task List	76
SchoolView Software Deployment	77
Loading Site Configuration Files.....	77
Loading Admin Touch Panel File and NetLinx Software.....	79
Loading and Configuring Other Software from the Admin TP	80
Loading Classroom Touch Panel Files	88
User Training Guidelines (Admin & Teacher)	89
Administration Training.....	89
Teacher Training	89
Appendix A: Cisco IP-Multicast.....	132
Appendix B: RFC 4541-Considerations for IGMP	149

SchoolView

Site Survey Considerations

Why perform a Site Walk/Survey?

The SchoolView solution is designed to work with many different products. Some product categories offer more choices and flexibility than others. A site walk can be useful to determine if there is any existing hardware that can be utilized as a part of the SchoolView solution. In addition, you will need to determine necessary quantities of certain hardware outside of the classroom that are variable based on the size and shape of the campus: digital signage locations, common zone loudspeakers and system clocks are all examples of this equipment.

Things to Consider

All of these things can / will affect your proposal:

Existing "Common Zone" speakers

- Cabling...home runs? Individual? Plenum rated / required?
- Amplifier(s)...25v? 70v? 100v? 4-8 ohm?
- Volume controls...existing? Desired?
- Speakers...all working? Any repairs / replacements **required**?
- Outdoor speakers – Coverage/location, condition, zones?

Existing clocks

- Power...110VAC? 12VDC? 24VAC? PoE? Other?
- Cabling...wireless? CAT5/6? Power / data?
- Master clock...make / model?
- Synchronization...none? Master clock? Network time server?
- Style...1-sided? 2-sided? Wall mounted? Ceiling mounted?

Existing Displays

- What types of inputs are available?
- Are they RS232 controllable?
- Are they IP/network controllable?

SchoolView

Technician / Installer Profile

The following skills are required to be successful:

- 1) Wiring diagram / rack elevation interpretation skills
- 2) General AV installation skills
 - a. Projector Installation
 - b. Speaker Installation
 - c. Input Wall Plate Installation
 - d. Audio and Video Rack Building & Wiring
 - e. General Cable Termination Skills
- 3) Basic networking skills
 - a. Physical network connectivity
 - i. Category / UTP Cabling
 - ii. Connectors
 - iii. Patch Panels
 - iv. Routers
 - v. Switches, etc.
 - b. Logical network connectivity
 - i. IP addresses and subnet masks
 - ii. Setting DHCP and Static IP addresses on your PC and other devices
 - iii. Familiarity with Command Prompt tools for configuration and troubleshooting
 - iv. Understanding VLANs
 - v. Multicast routing and IGMP snooping
- 4) Basic Troubleshooting Skills
 - a. Isolate problem : Clearly assess what works and what doesn't
 - b. Identify root problem(s), not just a symptom
 - c. Follow instructions when provided (don't skip steps)

SchoolView

AV Industry Training from AVIXA

About AVIXA

AVIXA™ is the Audiovisual and Integrated Experience Association, producer of InfoComm trade shows around the world, co-owner of Integrated Systems Europe, and the international trade association representing the audiovisual industry. Established in 1939, AVIXA has more than 5,400 members, including manufacturers, systems integrators, dealers and distributors, consultants, programmers, rental and staging companies, technology managers, IT professionals, content producers, and multimedia professionals from more than 80 countries. AVIXA members create integrated AV experiences that deliver outcomes. AVIXA is a hub for professional collaboration, information, and community, and the leading resource for AV standards, certification, training, market intelligence and thought leadership. <https://www.avixa.org/en>

AVIXA Training

A full list of AVIXA courses can be found at <https://avixa.netexam.com/newCatalogAvixa/>. AVIXA tracks that are useful for various roles in a SchoolView integration are listed below.

- Designer
- General Knowledge
- Installer
- Networking & Technology
- Project Manager

SchoolView

Recommended Applications / Tools

To complete an SchoolView deployment, several software applications & tools will be required or recommended.

Software Applications

- 1) NetLinx Studio
 - a) (free) <https://www.amx.com/en-US/software>
- 2) Web browser(s) – Chrome and/or Firefox
- 3) Terminal Emulator – SSH, telnet, and serial
 - a) PuTTY (free) <https://www.putty.org/>
 - b) shadeBlue Indigo (45 day free trial) <http://www.shadeblue.com/>
 - c) Windows Telnet client (free, included with all modern versions of Microsoft Windows)
 - d) Netlinx studio integrated telnet client (free, included with AMX Netlinx studio, see 1.a)
- 4) FTP Client (ex. Windows Explorer or Filezilla)
 - a) Filezilla (free) <https://filezilla-project.org/>
- 5) Angry IP Scanner
 - a) (free) <https://angryip.org>
- 6) VideoLAN.org VLC media player
 - a) (free) <https://www.videolan.org/vlc/index.html>
- 7) Barix discovery tool – A tool for finding Barix devices and setting IP addresses
 - a) (free, registration required to access) <https://www.barix.com/downloads/downloads-software/software-tools/>
- 8) Wireshark – Network packet capture and analysis
 - a) (free) <https://www.wireshark.org/>
- 9) AMX SVSI N-Able Software
 - a) PC <https://www.amx.com/en-US/products/n-able-pc>
 - b) MAC <https://www.amx.com/en-US/products/n-able-mac>
- 10) Text/XML Editing and Syntax Highlighting
 - a) Notepad++ (free) <https://notepad-plus-plus.org/>
 - b) EditPad Pro (free trial) <https://www.editpadpro.com/>
 - c) Microsoft Visual Studio (free) <https://visualstudio.microsoft.com>

Other Tools

- 1) Computer, preferably with a traditional 9-pin serial port. NOTE: This is useful for Barix and RS-232 displays.
 - a) If an on-board serial port is not an option, some USB adapters have been shown to work better than others.
 - i) One model that has been very reliable is the Micro Connectors E07-162 Dual Serial Adapter. <http://microconnectors.com/e07-162/>
 - ii) Another reliable model is the IOGEAR GUC232A. <https://www.iogear.com/product/GUC232A/>
- 2) Serial cables and adapters.
 - a) Female to Female DB9 cable
 - b) Male to Female DB9 cable
 - c) Male to Male DB9 adapter
 - d) DB9 Null modem adapter M-F
 - e) DB9 to screw terminals adapter

SchoolView

Training Resources

- Modero X | Wall Removal <https://www.youtube.com/watch?v=iie0hfSHJgA>
 - You will need to remove any wall mount touch panels from the back box before installing
- Modero X | Loading Firmware via USB <https://www.youtube.com/watch?v=hoD9IRwHI7U>
 - For updating touch panel firmware without a master
- SVSI Import and Export CSV <https://www.youtube.com/watch?v=g3ZFy3Mjp5I>
 - How to bulk configure SVSI devices
- NetLinx Control Systems | Locating the IP Address using the "Listen" Feature <https://www.youtube.com/watch?v=pJrrq3ToDHA>
- DGX & NX Series | Web Console - Main Overview & System Tab <https://www.youtube.com/watch?v=Vpz1hzB4pBM>
- DGX & NX Series | Web Console - Network Settings <https://www.youtube.com/watch?v=WOLTKIPUfdc>
- NX Series | Technical Overview - Part 1 <https://www.youtube.com/watch?v=rPFHZ2Cq5II>
- NX Series | Network Capabilities - Part 2 <https://www.youtube.com/watch?v=PqZfRtDm2qA>
- NX Series | USB Ports - Part 3 <https://www.youtube.com/watch?v=py7dkPYNhPo>
- NX Series | ID Button - Part 4 <https://www.youtube.com/watch?v=8L6PFFrf5XU>
- NetLinx Studio | Layout - Part 1 <https://www.youtube.com/watch?v=aPmYa4KydZU>
- NetLinx Studio | Workspace Wizard - Part 2 <https://www.youtube.com/watch?v=2ofJkMz8xo>
- NetLinx Studio | Importing Files - Part 3 <https://www.youtube.com/watch?v=9rNcFMMLxv8>
- NetLinx Studio | Exporting Workspaces - Part 4 <https://www.youtube.com/watch?v=XEsXclWeO9c>
- NetLinx Studio | Prep for File Transfer - Part 5 <https://www.youtube.com/watch?v=VINWhX57Xdg>
- NetLinx Studio | Build Active System - Part 6 <https://www.youtube.com/watch?v=MYLD0jpBMXO>
 - Note: SchoolView code is delivered as compiled TKN files. The second part of this video shows how to transfer files using Netlinx Studio and is useful for SchoolView systems.

SchoolView

Recommended Equipment List

Why do we recommend specific equipment?

The SchoolView solution is designed to work with many different products. Some product categories offer more choices and flexibility than others. This document is intended to identify products that are known to work with the Solution or alternately provide a generic specification that is required.

Security Cameras

The Admin touch panel is capable of displaying Motion-JPEG images from customer-provided security cameras, but only when the video feed is directly accessible without a browser plug-in. If a camera requires a plug-in, like Active-X, that camera is NOT a candidate for compatibility with the SchoolView solution.

The admin panel(s) need to access only the M-JPEG stream, not the entire HTML page served by the camera/server by default.

One way to work around this is connecting to your networked camera or video server using an Internet browser that captures the location or path to the stream. An example of such browser is Mozilla FireFox. Using the browser you can go to your network device's IP address, left click on the streaming image and Copy Image Location. Paste that image location into the address line of your browser. If the resulting page contains only the camera image / video, there is hope!

You can download a free version of FireFox at www.mozilla.org.

Here is more detail from AMX Tech Note 682:

SchoolView

Motion JPEG Cameras and Servers

A number of leading manufacturers are offering a variety of equipment that provides Motion JPEG streaming output. Below is a sample list of the most popular manufacturers and models:

Manufacturer	Network camera	Network video server
Axis	205 Network Camera 2100 Network Camera 2120 Network Camera 2420 Network Camera	241Q Video Server 4 Inputs 241S Video Server 1 Input
Panasonic	KX-HCM280 Color Pan Tilt Zoom KX-HCM10 Indoor Pan Tilt KX-HCM250 Wireless Pan Tilt KX-HCM230 Outdoor Pan Tilt	
Sony	SCN-RZ30N Pan/Tilt/25x Zoom	
Vivotek	IP2111 Network Camera IP2112 Network Camera	VS2402 Video Server

Network Path Information

While AMX is striving to bring to the market innovative features such as support for Motion JPEG, at points we have to work through the different ways manufacturers implement standards. In the case of streaming network cameras/servers, manufacturers are using somewhat different syntax for requesting Motion JPEG streams from their networked cameras and servers.

Case in point, many of the networked cameras/servers are accessed using a regular HTML browser, and the camera/server is serving up an HTML page with a video window being a part of the page. For DynaMo, however, the panel needs to access only the M-JPEG stream, not the entire HTML page served by the camera/server by default.

Depending on the camera/network video server type you are using, you may need to consult product documentation, or if necessary, contact manufacturer's technical support. In general, however, what is being sent to the camera/server in the path is a CGI call that may have additional parameters based on the feature set of the camera/server and the syntax the manufacturer requires. What follows are examples for some of most popular manufacturers.

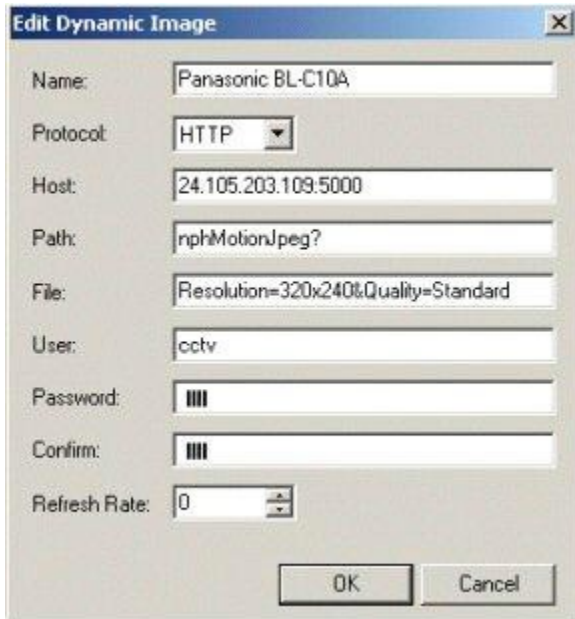
Axis

Model: **2100** (camera)

Path: **axis-cgi/mjpg/video.cgi?camera=&resolution=320x240**

Dynamic image settings:

SchoolView



Edit Dynamic Image

Name: Panasonic BL-C10A

Protocol: HTTP

Host: 24.105.203.109:5000

Path: nphMotionJpeg?

File: Resolution=320x240&Quality=Standard

User: cctv

Password: ■■■■

Confirm: ■■■■

Refresh Rate: 0

OK Cancel

Model: **2411** (video server)

Path: **axis-cgi/mjpg/video.cgi?resolution=704x480**

Note that Axis equipment supports a number of resolutions, and therefore requires that the target resolution be indicated. Each camera can also have a camera ID number but that is optional, just as a number of other features that can be indicated in the path.

Pana sonic

Model: **BL-C10A** (camera)

Path: **nphMotionJpeg?resolution=320x240&Quality=Standard**

Dynamic image settings:

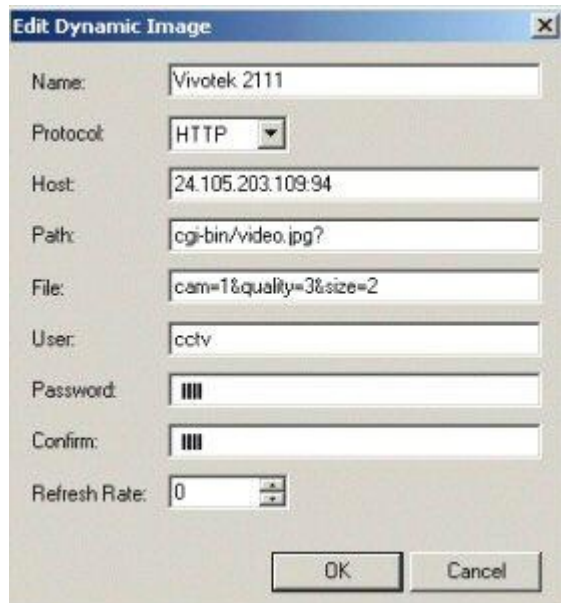
SchoolView

Vivotek

Model: 2111 (camera)

Path: [cgi-bin/video.jpg?cam=1&quality=3&size=2](http://24.105.203.109:94/cgi-bin/video.jpg?cam=1&quality=3&size=2)

Dynamic image settings:



The screenshot shows a dialog box titled "Edit Dynamic Image" with the following fields and values:

- Name: Vivotek 2111
- Protocol: HTTP
- Host: 24.105.203.109:94
- Path: cgi-bin/video.jpg?
- File: cam=1&quality=3&size=2
- User: cctv
- Password: |||
- Confirm: |||
- Refresh Rate: 0

Buttons: OK, Cancel

HINT: Like with any other type of equipment AMX controls, manufacturer's documentation and customer support are the most reliable ways of obtaining information on the device's communication protocol/syntax. This can also help you fully utilize optional features available on that specific device. However, at times it can be difficult to get the needed information with respect to the protocol/syntax of a particular camera/server. One way to work around this is connecting to your networked camera or video server using an Internet browser that captures the location or path to the stream. An example of such browser is Mozilla Firefox. Using the browser you can go to your network device's IP address, left click on the streaming image and Copy Image Location.

You can download a free version of Firefox at www.mozilla.org.

SchoolView

Displays (Projectors / Flat Panels)

The SchoolView solution requires RS232 or IP for control of video displays throughout the campus. Some displays have a serial port that is non-functioning or reserved for support purposes only, although this is becoming less common as time goes by. If a display has a published protocol for control via serial / RS232 / IP, it is probably compatible with the SchoolView solution. Specifically, the protocol must support the following commands and [responses]:

- 1) Power ON
 - a) Discreet Command and Query
- 2) Power OFF
 - a) Discreet Command and Query (query must be supported in standby mode)
- 3) Discreet Input Select (cycle command is not compatible):
 - a) VGA 1/2
 - b) Component
 - c) Composite/Video
 - d) HDMI 1/2/3/4
- 4) Video Mute (discreet or toggle) (optional)
- 5) Video Freeze (discreet or toggle) (optional)
- 6) Auto PC Adjust (optional)
- 7) [Power Status Query] - Projector must respond when in standby mode.
- 8) [Input Query]
- 9) [Lamp Time Query] (optional)
- 10) [Filter Time Query] (optional)

Following is a list of displays that have been successfully deployed and controlled by SchoolView:

- Epson PowerLite 980W, 6x5W(i), G7xxx, L1xxx
- Promethean PRM-25, 30 and 35 (various models have had issues with off/on cycles being too quick while warm)
- Sanyo (various models)
- Panasonic (various models)
- Hitachi / Dukane (use caution; rebranded from multiple OEMs, not all use the same control protocol)
- Boxlight (use caution; some models have issues with reliably responding to RS-232 commands)
- Newline (use caution; some models have trouble reliably switching sources when only a single active signal is present)
- LG Flat Panel Displays (various models)
- Samsung Flat Panel Displays (various models)

The SchoolView team has encountered a few display models with specific issues that are problematic for deployment with our solution. This highlights the need to thoroughly evaluate the capabilities of any given model before deployment. Examples of these models and the problem with each:

- Dell 1209s projector – no discreet power OFF command, only ON and toggle, causing unreliable control.
- LG 52LG50DC – does not respond to RS232 commands while in standby mode, causing communication errors.

SchoolView

Video Encoders

While existing H.264 video encoders may be used with the SchoolView solution, products from AMX SVSI N3xxx series are recommended.

RECOMMENDED

- 1) AMX SVSI NMX-ENC-N3132 Encoder
 - a) NMX-ACC-N9102 – 1RU rack shelf for two SVSI N-Series products
 - b) NMX-ACC-N9101 – Mounting wings for SVSI N-Series products
- 2) AMX SVSI NMX-ENC-N3132-C Encoder Card
 - a) NMX-ACC-N9206 – 2RU rack mount cage with power for six SVSI N-series card units

REQUIRED:

- Multicast stream
- Always on, no user intervention required
- H.264
- No HDCP/encryption

Video Decoders

The SchoolView solution uses either AMX ENZO or AMX SVSI N3232 Decoders. No exceptions / substitutions are allowed.

SchoolView

System Diagrams

The SchoolView solution is available in multiple configurations. The system diagrams provide a generic illustration of the significant elements of the solution and may be incorporated into your specific project as needed. Please refer to the current system diagrams; provided separately.

Wiring Considerations

UTP Cable Recommendations

Some basic recommendations for installing UTP cable are provided below. Note that these are generally network cabling-related concepts.

- Avoid installing UTP cabling in close proximity to electrical conduit or other high-voltage electrical sources.
- Allow at least 18" (45.72 cm) of separation between electrical and data lines.
- Always check local codes and other applicable regulations.
- Avoid installing UTP cabling in any area that is likely to see sustained temperatures lower than -4°F (-20°C), or higher than 150°F (65°C).
- Install cable with gradual bends at corners. Kinks or sharp bends can create line interference.
- Only use staples or fasteners that conform to the cable's shape. When using staples or fasteners, be careful not to crimp the wires inside.

SchoolView

Button Labels

MET-7E buttons must be ordered separately. The following list shows the typical button layout and part numbers for the white keypads.

Part #	Model	Description
FG5794-03-WH	MET-7-WH	White Metreau 7-Button Keypad
MA5794-03WH-CUSTOM	MA5794-03WH-CUSTOM	Double Button, WHITE, CUSTOM, "POWER"
MA5794-03WH-CUSTOM	MA5794-03WH-CUSTOM	Double Button, WHITE, CUSTOM, "PTT / PTC"
MA5794-03WH-CUSTOM	MA5794-03WH-CUSTOM	Double Button, WHITE, CUSTOM, "CHANNEL UP"
MA5794-03WH-CUSTOM	MA5794-03WH-CUSTOM	Double Button, WHITE, CUSTOM, "CHANNEL DOWN"
MA5794-03WH-CUSTOM	MA5794-03WH-CUSTOM	Double Button, WHITE, CUSTOM, "INPUT"
MA5794-03WH-CUSTOM	MA5794-03WH-CUSTOM	Double Button, WHITE, CUSTOM, "AUDIO MUTE"
MA5794-03WH-+-	MA5794-03WH-+-	Double Button, White, +/-



SchoolView

MET-7E buttons must be ordered separately. The following list shows the typical button layout and part numbers for the black keypads.

Part #	Model	Description
FG5794-03-BL	MET-7-BL	Black Metreau 7-Button Keypad
MA5794-03BL-CUSTOM	MA5794-03BL-CUSTOM	Double Button, Black, CUSTOM, "POWER"
MA5794-03BL -CUSTOM	MA5794-03BL-CUSTOM	Double Button, Black, CUSTOM, "PTT / PTC"
MA5794-03BL -CUSTOM	MA5794-03BL-CUSTOM	Double Button, Black, CUSTOM, "CHANNEL UP"
MA5794-03BL-CUSTOM	MA5794-03BL-CUSTOM	Double Button, Black, CUSTOM, "CHANNEL DOWN"
MA5794-03BL-CUSTOM	MA5794-03BL-CUSTOM	Double Button, Black, CUSTOM, "INPUT"
MA5794-03BL-CUSTOM	MA5794-03BL-CUSTOM	Double Button, Black, CUSTOM, "AUDIO MUTE"
MA5794-03BL-+-	MA5794-03BL-+-	Double Button, Black, +/-



Speaker Cabling Considerations

Speaker cable should be 2-conductor stranded, but the wire gauge should be selected based on distance between the amplifier and speaker. As a rough guideline please see the chart below based on 0.5 dB loss (11%).

AWG	4 Ohm Speaker	8 Ohm Speaker	70V Speaker
12	69 ft	138 ft	3376 ft
14	43 ft	87 ft	2127 ft
16	27 ft	53 ft	1305 ft
18	17 ft	34 ft	823 ft
20	11 ft	21 ft	518 ft

If using two 8 Ohm speakers with the GL-300 amplifier the impedance will be 8 Ohms / channel.

If using four 8 Ohm speakers with the GL-300 amplifier (2 in parallel per output) the impedance will be 4 Ohms / channel.

Classrooms (typically 8-ohm speakers)

In a typical SchoolView classroom, 16 AWG speaker cable is perfectly acceptable. Because the distance is typically so short in the classroom, even 18 AWG speaker cable may be adequate. When planning the audio-only option in a classroom, it is permissible to consolidate the audio decoder/amplifiers in one or more central location(s) such as an IDF or MDF. While that is convenient and efficient, it does present a potential challenge for speaker cabling. For two-way classrooms it is recommended to install the Barix device in the classroom to minimize the distance of the cabling between the Barix and the microphone. Barix Annunicom devices are plenum rated and POE powered making them easy to conceal above accessible ceilings for bell and PA applications. In unified installations they should be installed inside the plenum enclosure with the rest of the classroom hardware.

Refer to the current system diagrams and tray layouts for examples.

Common Zones (typically constant voltage, distributed, 25v or 70v systems)

For large groups of speakers or long distances, the typical solution consists of an amplifier with 70V output connected to speaker(s) with input transformers. The systems are most commonly 70v. This system design is supported by smaller gauge wire than a traditional 8-ohm design, typically 16 gauge wire is sufficient.

Speaker Choices

Speaker choices are almost endless with a wide price range. The most commonly used JBL speakers are listed below.

1. JBL LCT 81 C/T 2 x 2 Layin Speaker 8ohm/70V
 - a. Most common speaker for classrooms and hallways with drop tile ceilings.
2. JBL Control 26CT 6.5" Ceiling Loudspeaker Transducer Assembly
 - a. Typically used for hard ceiling common areas, includes 70V transformer.
3. JBL Control 24CT Background/ Foreground Ceiling Loudspeaker
 - a. Typically used for smaller hard ceiling areas, offices, bathrooms, etc.
4. JBL Control 67 P/T Extended Range Full-Range Pendant Speaker
 - a. Typically used in open ceiling areas that require suspended speakers, hallways, gyms, etc.
5. JBL Control 67 HC/T Narrow 75° Coverage High Ceiling Pendant Speaker
 - a. Typically used in tall open ceiling areas that require suspended speakers, hallways, gyms, etc.
6. JBL CSS-H30 30 Watt Paging Horn
 - a. Typically used in outdoor areas and gyms, good for voice/paging applications.
7. JBL Control 23-1 Ultra-Compact Indoor/Outdoor Background/Foreground Speaker, Surface Mount
 - a. Typically used in classrooms that require wall mount speakers. Note: the 23-1L model does not include a 70V transformer. For use in a 70V distributed audio system the 23-1 must be used,

SchoolView

typical classrooms may use either model.

8. JBL Control 25AV Compact Indoor/Outdoor Background/Foreground Loudspeaker, Surface Mount
 - a. Typically used in common areas that require a wall mount solution.
9. JBL Control 126WT Premium In-Wall Loudspeaker
 - a. Typically used in common areas that require an in-wall solution.

Network Requirements

Bandwidth Considerations

For each audio stream, we use 400Kbps. Generally, there are no more than 1 or possibly 2 active audio streams at any one time. You might have background music and a bell or PA announcement. The bell or page is a very short event, but music might be streaming longer.

Control packets are very small (under 500 bytes) and are sent only as needed (very short burst) when an event starts or stops.

Video is the real bandwidth user and that depends on how many sources or channels are used. Each video stream is typically 3 – 6 Mbps (depends on encoder configuration). Because we use multicast streaming, each end point (Enzo, SVSI or teacher PC) will only receive the one stream that they are watching. So worst case to each drop will only be 6 Mbps at any one time. Further, if all classrooms are watching the same stream, such as during an emergency alert or the president's inaugural address, the total network bandwidth used for that one stream is only 6 Mbps. Note that all encoders will be streaming to the switch port they are attached to all of the time. A properly configured network will not carry the stream on the backbone unless one or more viewers join the multicast group.

With most schools having a gigabit or better backbone and usually gigabit drops to each end-point, we don't require a large percentage of the backbone capacity.

SchoolView specific network requirements

1. IGMP multicast snooping.
2. We use multicast addresses above 224.1.1.1.
3. For the best performance, all network switches should be able to perform IGMP snooping. This allows multicast traffic to be switched intelligently at layer 2 in order to reduce unnecessary traffic.
4. Multicast routing between networks can be handled through PIM-DM (Dense mode) or PIM-SM (Sparse mode).
5. 100Mbps drops to each device or 1000Mbps (1Gbps) drop to a classroom, if a local switch will be used in the room. A switch in the room still must meet all of the requirements of a core switch regarding multicast.
6. Switches having 16, 24, or 48 ports, need to have a backbone capacity to handle the overall traffic. This means capacities of: 32Gbps for 16 ports or 140 Gbps for 48 ports.
7. NOTE: This is not intended to be a complete list but does cover the highlights.

Unicast and Multicast Transmissions over the Network

If you are unfamiliar with the difference between unicast and multicast the following resources offer detailed information on the topic.

- <https://en.wikipedia.org/wiki/Unicast>
- https://en.wikipedia.org/wiki/IP_multicast
- https://en.wikipedia.org/wiki/IGMP_snooping
- https://en.wikipedia.org/wiki/Multicast_address
- https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html

Cisco IP Multicast Guidelines

SchoolView

See Appendix A.

Considerations for IGMP and MLD Snooping Switches

See Appendix B.

SV Mount

The SV Mount is an integral component in the SchoolView solution, especially in the classrooms. This 2'x2' ceiling enclosure is designed to safely and securely house the classroom electronics while supporting a uniform deployment from one school to another. The removable tray is designed to be configured with the electronics offsite and installed into the plenum box after the building is secure and dust free. The separate plenum box can be installed as soon as ceiling grid is present, allowing electrical and network to be installed prior to the electronics tray. The recommended practice for new construction sites is to keep the plenum enclosure doors in a safe location and install them at the same time or after the trays are installed and wired.

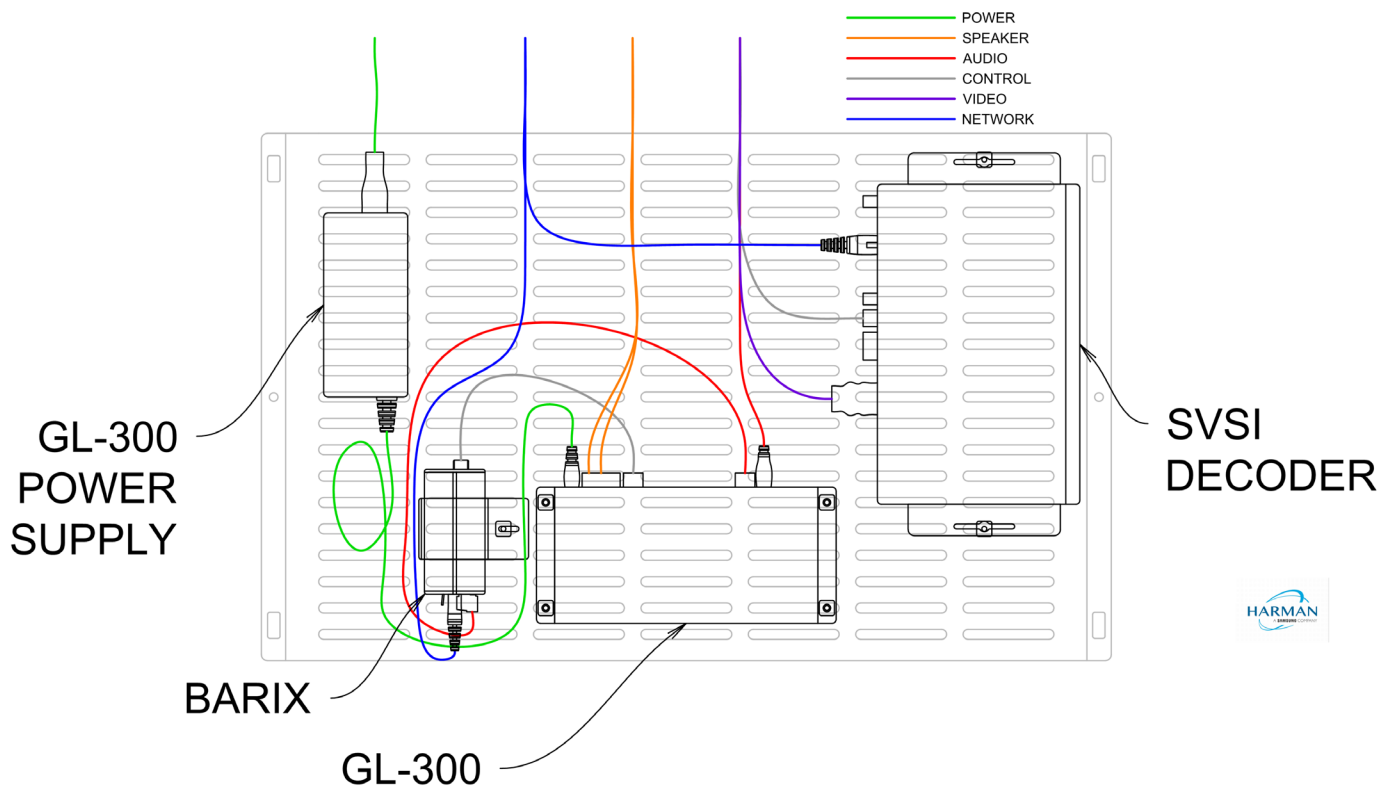
SchoolView

Classroom Equipment Trays

Tray Component Placement Layouts

The figures below provide for standardized placement of the equipment that resides in the SchoolView ceiling enclosure. Consistency between all systems will aid in troubleshooting and future hardware upgrades (if necessary). Different cable lengths and placements are required due to connector positions on each device. The video decoder may be either a SVSI N3000 series decoder (shown) or AMX Enzo depending on what was specified/ordered for the job. The layout below may be constructed as the mirror image of what is shown. The layout below works best when the electrical outlet is above the top left portion of the tray (double gang knockout closest to the edge of the enclosure) and the shortest possible AC power cord(s) are used. The network outlet should be placed near the location of the blue wiring (typically the single gang knockout next to the second double gang knockout). One of the remaining single gang knockouts can then be fitted with a cable pass through plate to accommodate the speaker, audio, control, and video cabling.

Figure 1: SchoolView standard audio encoder/decoder, GL-300 and SVSI (or Enzo) video decoder.



SchoolView

Tray Parts List and Pin-out

Enzo Classroom Tray Parts List			
Qty.	Source	P/N	Description
1	SchoolView	FG1702-21	Audio Decoder/Encoder/Amp Control
1	SchoolView	FG3211-01	AMX Enzo Video Decoder/Display Control
1	SchoolView	FG1702-22	GL-300 Amplifier
1	SchoolView	MA1702-01	Power supply for GL-300 amplifier
1	SchoolView	FG1700-01T	Equipment Tray
12	SchoolView	Included with Tray	Nylon Grommet Nut
12	SchoolView	Included with Tray	6-32 x 3/8" Pan Head Phillips Screws
12	SchoolView	Included with Tray	Zip Tie
2	Dealer	N/A	CAT 6 patch cable
1	Dealer	N/A	DB9 to bare wire
1	Dealer	N/A	22/2 Audio Cable

SVSI Classroom Tray Parts List			
Qty.	Source	P/N	Description
1	SchoolView	FG1702-21	Audio Decoder/Encoder/Amp Control
1	AMX	NMX-DEC-N3232	AMX SVSI Video Decoder/Display Control
1	AMX	FGN9101	Mounting wings for video decoder
1	SchoolView	FG1702-22	GL-300 Amplifier
1	SchoolView	MA1702-01	Power supply for GL-300 amplifier
1	SchoolView	FG1700-01T	Equipment Tray
12	SchoolView	Included with Tray	Nylon Grommet Nut
12	SchoolView	Included with Tray	6-32 x 3/8" Pan Head Phillips Screws
12	SchoolView	Included with Tray	Zip Tie
2	Dealer	N/A	CAT 6 patch cable
1	Dealer	N/A	DB9 to bare wire
1	Dealer	N/A	22/2 Audio Cable

Barix to GL-300 Serial Cable Pin Out			
Barix (DB9 Male)		GL-300 (Captive Screw)	
Pin	Signal	Pin	Signal
2	RX	1(TXD)	TX
3	TX	2(RXD)	RX
5	GND	3(GND)	GND

Barix to GL-300 Audio Cable Pin Out			
Barix (Captive Screw)		GL-300 (Captive Screw)	
Pin	Signal	Pin	Signal
3(Line Out -)	GND	2(Signal -)	GND
4(Line Out +)	AUDIO +	1(Signal +)	AUDIO +
		3(Shield)	GND

SchoolView

Audio & Video Equipment Racks

A typical SchoolView system will have one or two equipment racks. The typical Bell & PA system consist of one rack. Unified systems may consist of two racks. If a Unified system does consist of two equipment racks the video rack will typically be in a location accessible to the school librarian or other personnel for the purpose of swapping physical media or other tasks associated with the video sources. The audio rack is typically located in the MDF. These racks(s) will house all of the required equipment outside of the administration area and classrooms, except network hardware (by others), clocks, and common zone speakers/amplifiers.

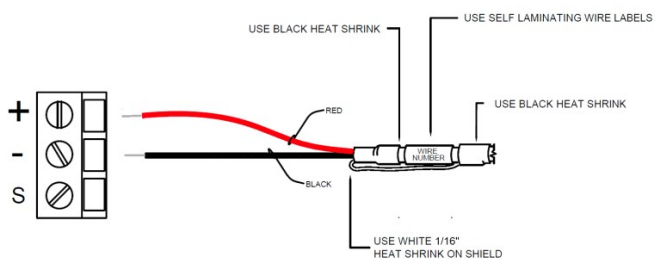
Rack Wiring and Connection Considerations

Follow all manufacturers' guidelines regarding installation of cables. These might include guidelines such as: minimum bend radius, recommended cable support methods and other special considerations per cable type. When wiring an audio or video equipment rack, it is advisable to separate cabling by relative signal or power level. Below is an excerpt from a typical consultant specification document regarding cable separation:

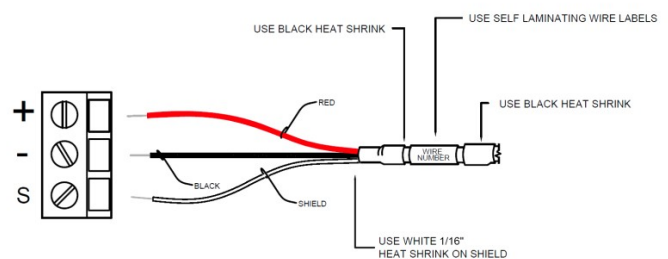
- All cables shall be separated into like groups according to signal or power levels and routed separately to eliminate signal contamination and cross-talk, this includes both in equipment racks and outside of equipment racks.
- All power cables, control cables, and high level cables shall be grouped to one side of the equipment rack while low level cables shall be grouped to the other side.

Many of the device connections in the equipment racks of an SchoolView system can be made using pre-manufactured patch cables, such as network and many video connections. Some specialty cables may be included with the hardware. In the case of other connections which don't fall into these categories, you may be required to custom terminate cables, such as most of the audio connections in the audio rack and some RS232 connections. When custom terminating cables, be sure to keep the following best practices in mind:

- Be careful not to score the individual conductors' insulation while stripping away the outer jacket.
- Dress each termination with heat-shrink tubing, including a boot at the end of the outer jacket as well as insulation for any bare shield conductors. See typical example figures below:



06 FOR CAPTIVE SCREW TERMINATION SHIELD LIFTED



07 FOR CAPTIVE SCREW TERMINATION SHIELD TIED

- When preparing cable for termination into captive screw connectors, DO NOT apply solder to the conductors. Doing so can result in connections becoming loose over time.
- Make certain you understand the function of, and install, all of the necessary parts that are provided with each connector type. A good example of one that gets discarded all too often is the insulating sleeve that should be included with tip, ring, sleeve (such as typical 3.5mm and 1/4" audio) connectors that use metal back shells.
- Follow all manufacturers' guidelines regarding installation of each connector type.

SchoolView

Power Requirements

Generally, the audio equipment rack requires one or two 120V, 20A circuits and the video equipment rack requires one 120V, 20A circuit. These are general guidelines which assume a typical system. Increasing the quantities of additional equipment, especially high power equipment such as audio amplifiers, may increase the necessary number and /or size of these circuits. A good practice might be to have one (or more) circuit(s) in the audio rack for the amplifier(s) and one for the rest of the system electronics. Be sure to consider the requirements of all devices in the system when coordinating power requirements with consultants or electrical contractors.

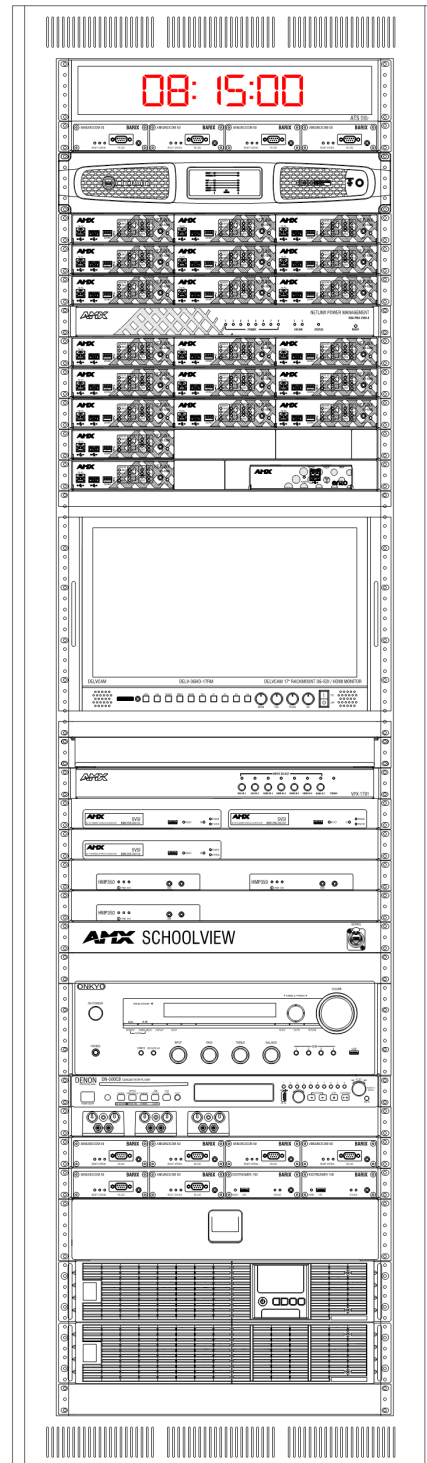
UPS Considerations

A typical Uninterruptible Power Supply such as the APC Smart-UPS SC 1500VA would run the audio (excluding amplifiers) or video rack in a typical SchoolView system for about thirty minutes. The current draw of typical audio amplifiers used for common zone speakers varies greatly depending on the load and output power level. One example of a typical amplifier's specifications states current draw varying from less than one ampere at idle, to nearly ten amperes with typical program material. Using the same typical UPS example as above, this translates to over an hour of runtime at idle, but only a few minutes at maximum current draw. If you need common zone speakers to remain available for paging during a power outage, be sure to determine the appropriate size and type of UPS necessary to run the amplifiers that are required by your specific project.

SchoolView

Example Rack Layouts Unified Campus - Single Rack

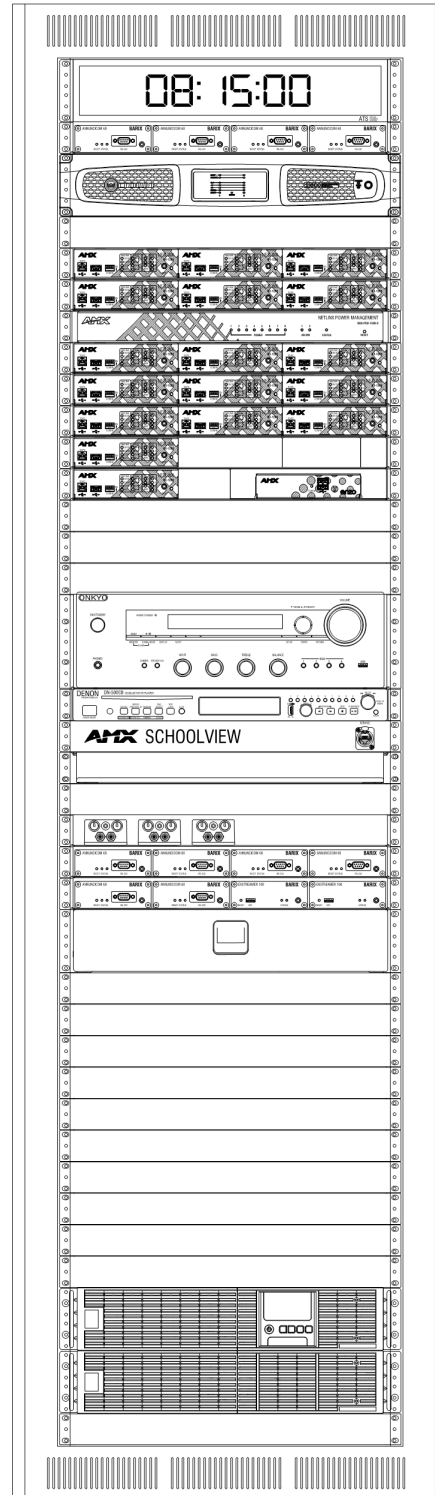
System Clock	44
4 x Barix Annunicom 60	42
Common Zone Amplifier	41
3 x NX1200	39
3 x NX1200	38
3 x NX1200	37
Power Supply	36
3 x NX1200	35
3 x NX1200	34
3 x NX1200	33
NX1200	32
NX1200 + ENZO	31
EB1/2 Blank	30
	29
	28
Preview Video Monitor	27
	26
	25
	24
EB1/2 Blank	23
Sliding Shelf	22
Preview Video Switcher	21
2 x Video Encoders	20
Video Encoder	19
2 x Digital Signage Players	18
Digital Signage Player	17
Logo Panel + Network	16
	15
Internet Radio	14
	13
	12
CD Player	11
3 x PodDI	10
4 x Annunicom 60	9
2 x Annunicom 60 + 2 x Extreamer 100	8
	7
2U Rack Drawer	6
	5
UPS	4
	3
Extended Runtime UPS Battery	2
EB1 Blank Panel	1



SchoolView

Unified Campus – Dual Racks - Audio

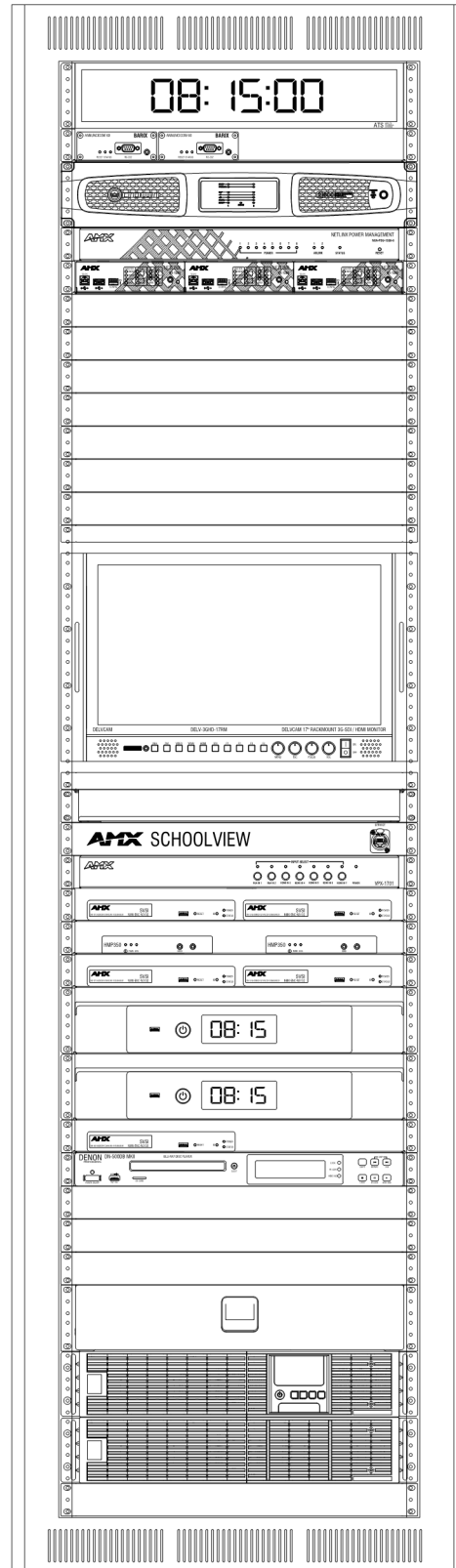
	44
System Clock	43
4 x Barix Annunicom 60	42
Common Zone Amplifier	41
EB1 Blank	40
EB1 Blank	39
3 x NX1200	38
3 x NX1200	37
Power Supply	36
3 x NX1200	35
3 x NX1200	34
3 x NX1200	33
NX1200	32
NX1200 + ENZO	31
EB1 Blank	30
EB1 Blank	29
FEB1 Blank	28
Internet Radio	27
EB1 Blank	26
EB1 Blank	25
CD Player	24
Logo Panel + Network	23
Sliding Shelf	22
EB1 Blank	21
3 x PodDI	20
4 x Annunicom 60	19
2 x Annunicom 60 + 2 x Exstreamer 100	18
2U Rack Drawer	17
EB1 Blank	16
EB1 Blank	15
EB1 Blank	14
EB1 Blank	13
EB1 Blank	12
EB1 Blank	11
EB1 Blank	10
EB1 Blank	9
EB1 Blank	8
EB1 Blank	7
EB1 Blank	6
EB1 Blank	5
UPS	4
EB1 Blank	3
Extended Runtime UPS Battery	2
EB1 Blank	1



SchoolView

Unified Campus - Dual Racks - Video

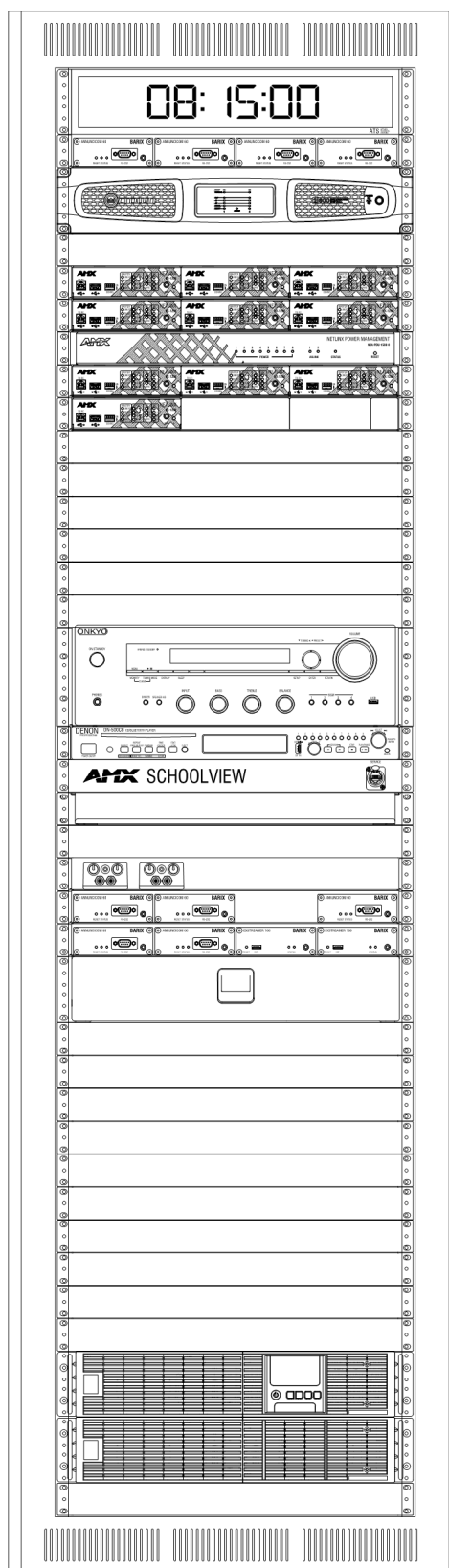
	44
System Clock	43
2 x Barix Annunicom 60	42
Common Zone Amplifier	41
	40
Power Supply	39
3 x NX1200	38
EB1 Blank	37
EB1 Blank	36
EB1 Blank	35
EB1 Blank	34
EB1 Blank	33
EB1 Blank	32
EB1 Blank	31
EB1/2 Blank	30
	29
	28
	27
Preview Video Monitor	26
	25
	24
EB1/2 Blank	23
Sliding Shelf	22
Logo Panel + Network	21
Preview Video Switcher	20
2 x Video Encoder	19
2 x Digital Signage Players	18
2 x Video Encoder	17
	16
Cable DVR	15
	14
Cable DVR	13
	12
Video Encoder	12
Blu-Ray Player	11
EB1 Blank	10
EB1 Blank	9
EB1 Blank	8
	7
2U Rack Drawer	6
	5
UPS	4
	3
Extended Runtime UPS Battery	3
	2
EB1 Blank	1



SchoolView

Bell & PA Audio Rack

	44
System Clock	43
4 x Barix Annunicom 60	42
Common Zone Amplifier	41
EB1 Blank	40
EB1 Blank	39
3 x NX1200	38
3 x NX1200	37
Power Supply	36
3 x NX1200	35
NX1200	34
EB1 Blank	33
EB1 Blank	32
EB1 Blank	31
EB1 Blank	30
EB1 Blank	29
FEB1 Blank	28
Internet Radio	27
EB1 Blank	26
EB1 Blank	25
CD Player	24
Logo Panel + Network	23
Sliding Shelf	22
EB1 Blank	21
2 x PodDI	20
3 x Annunicom 60	19
2 x Annunicom 60 + 2 x Exstreamer 100	18
2U Rack Drawer	17
EB1 Blank	16
EB1 Blank	15
EB1 Blank	14
EB1 Blank	13
EB1 Blank	12
EB1 Blank	11
EB1 Blank	10
EB1 Blank	9
EB1 Blank	8
EB1 Blank	7
EB1 Blank	6
EB1 Blank	5
UPS	4
EB1 Blank	3
Extended Runtime UPS Battery	2
EB1 Blank	1



SchoolView

SchoolView Hardware Configuration

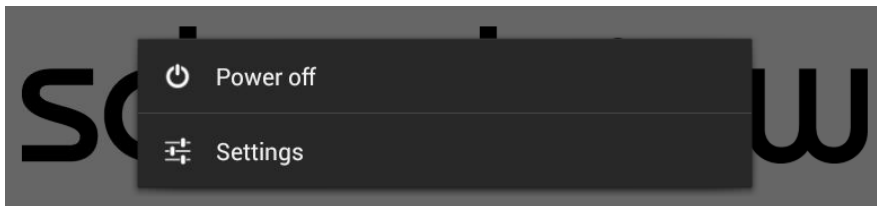
The following sections will explain how to configure necessary connections and settings on each type of device in an

SchoolView system. Network settings shown throughout are examples only, and should be replaced by the actual values assigned to be used on your particular project.

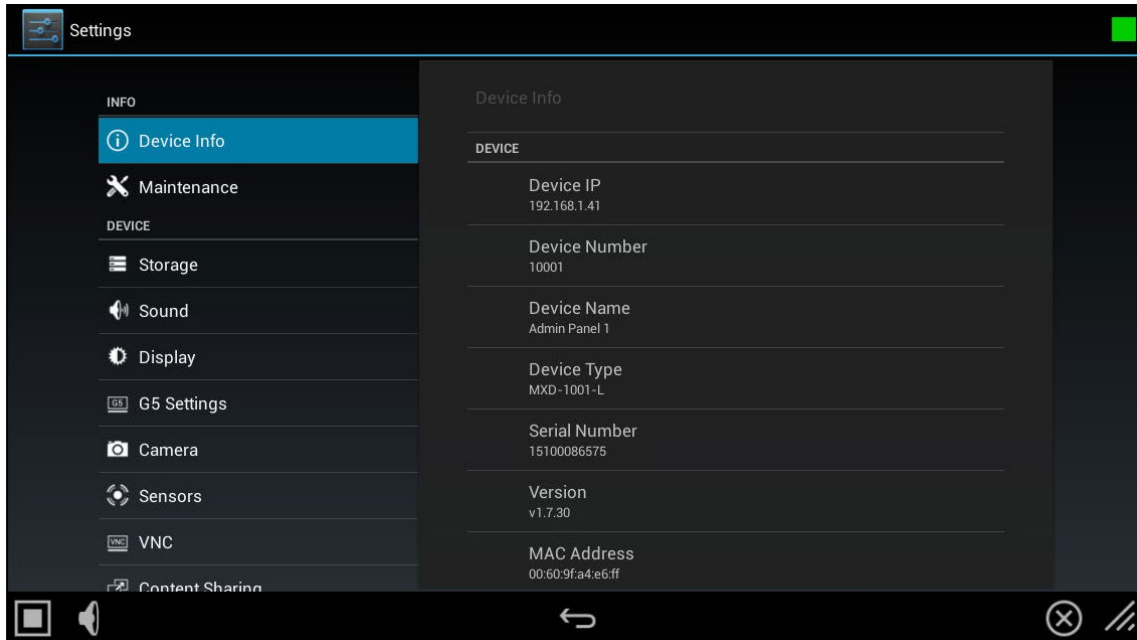
Touch Panel Configuration

The Admin touch panel (and classroom touch panels, if present) will need to be configured with network and master connection settings.

A brand new AMX touch panel will boot up to the Setup page. If a project file has already been loaded, you can access the Setup page by pressing and holding the bezel button (table top panels) or using a ball point pen to press the setup button located on the top left of the panel (wall mount panels). Select Settings from the menu.



You should now see the full menu.

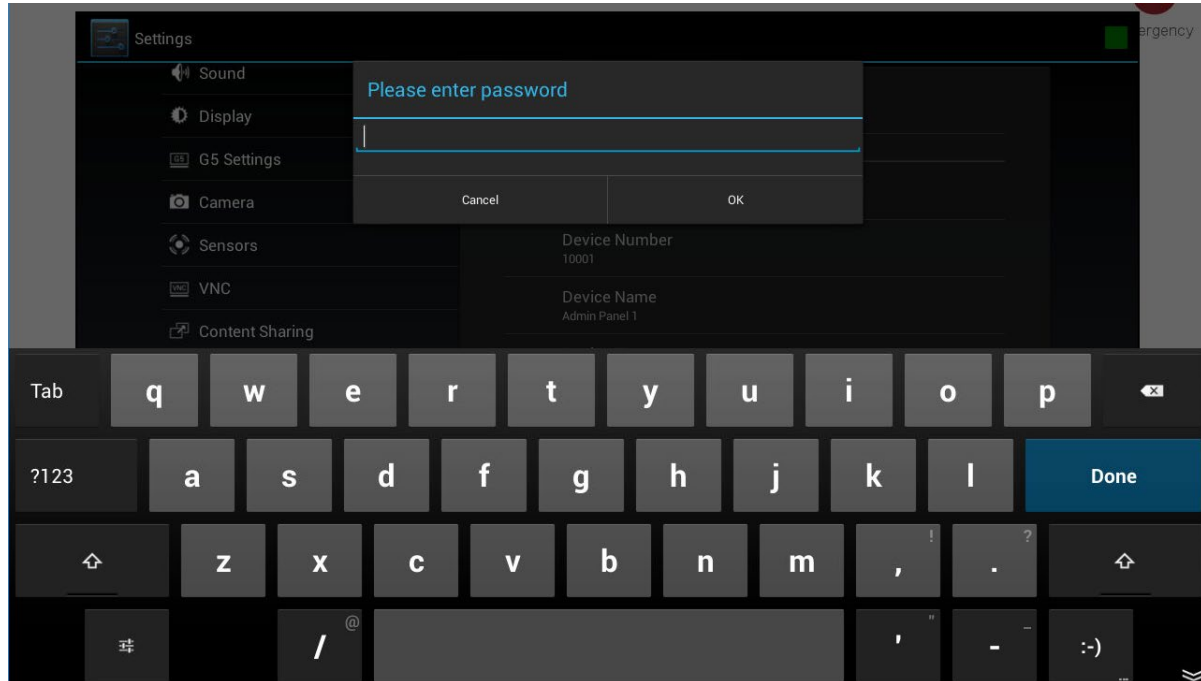


Enter exact contents of quotes as shown, except replace example values as necessary.

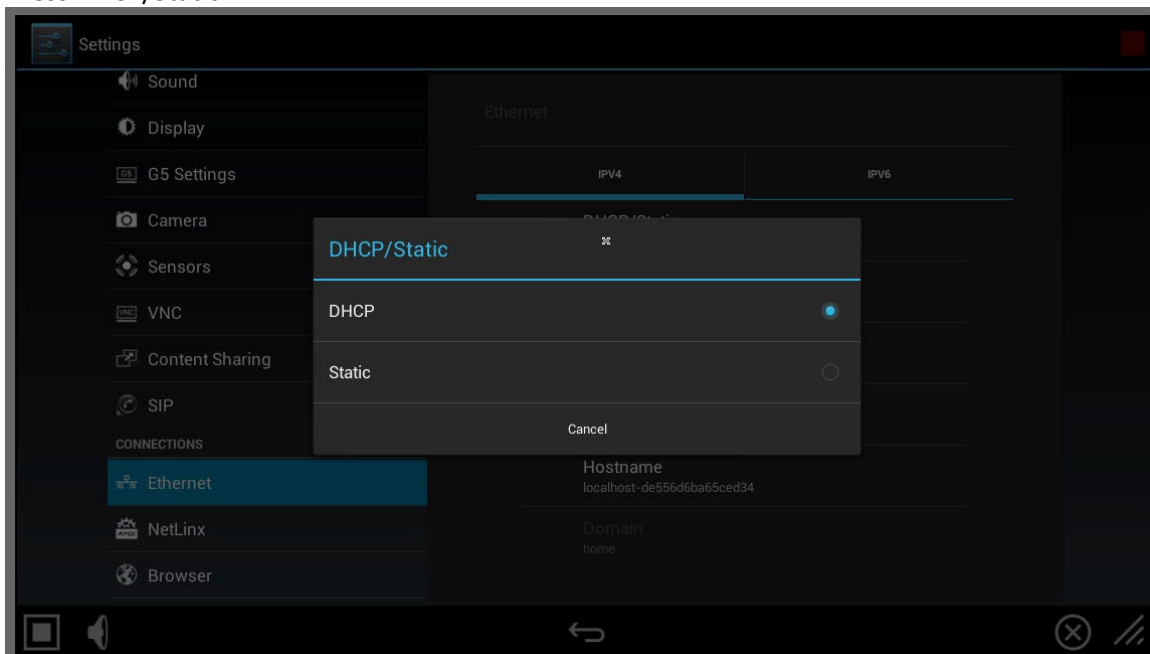
To configure the touch panel network and master connection settings, follow these steps:

- 1) Scroll down on the settings menu and select Ethernet.

SchoolView



- 2) Enter the default password: "1988".
- 3) Press OK
- 4) Press DHCP/Static



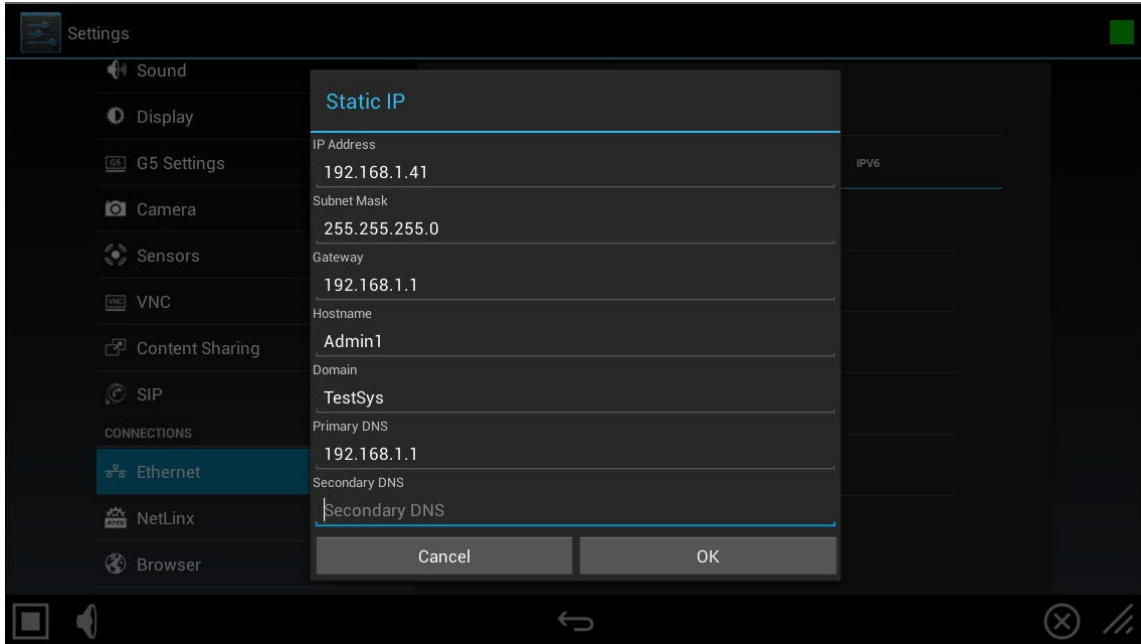
- 5) Select Static

SchoolView

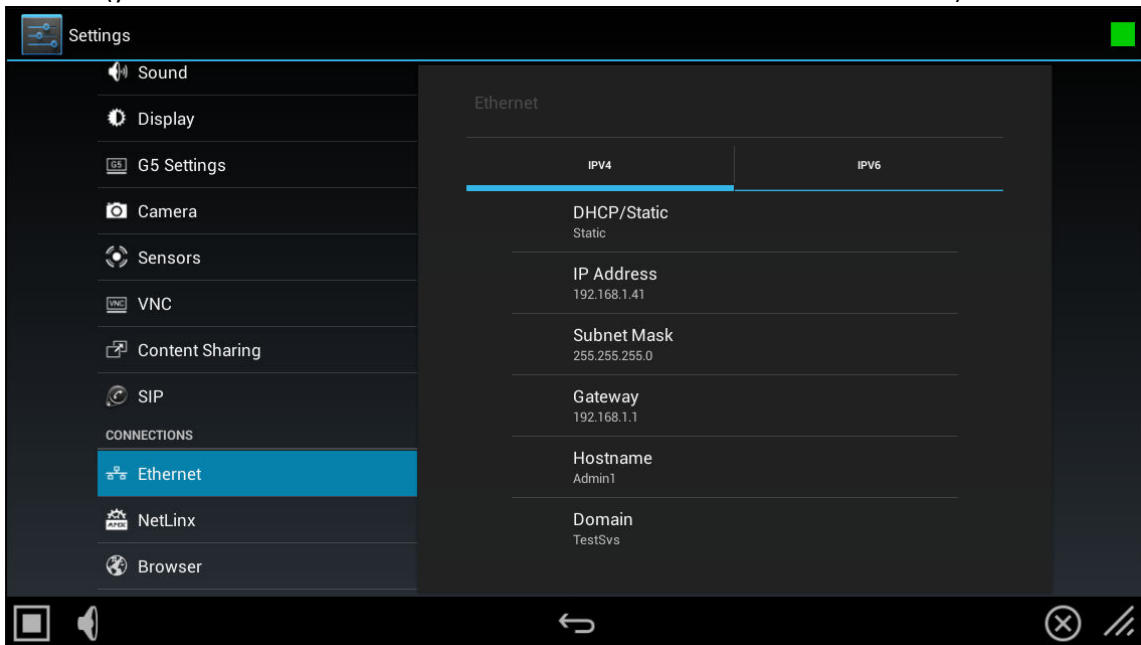


- 6) Press IP Address.
- 7) Enter IP Address: "192.168.1.41"
- 8) Press Next
- 9) Enter Subnet Mask: "255.255.255.0".
- 10) Press Next
- 11) Enter Gateway: "192.168.1.1".
- 12) Press Next
- 13) Enter Hostname: "Admin1"
- 14) Press Next
- 15) Enter Domain (optional)
- 16) Press Next
- 17) Enter the Primary DNS address: "192.168.1.1"
- 18) Press Next
- 19) Enter the Secondary DNS address: (optional)
- 20) Press Done

SchoolView

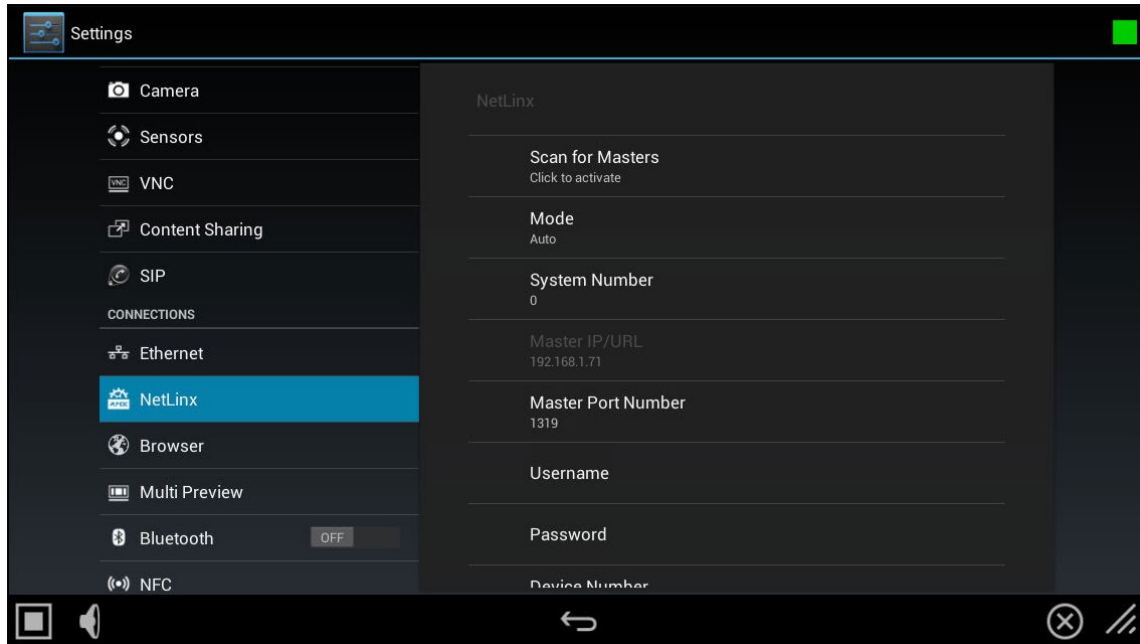


21) Press OK (you should now see the values entered reflected in the Ethernet menu)

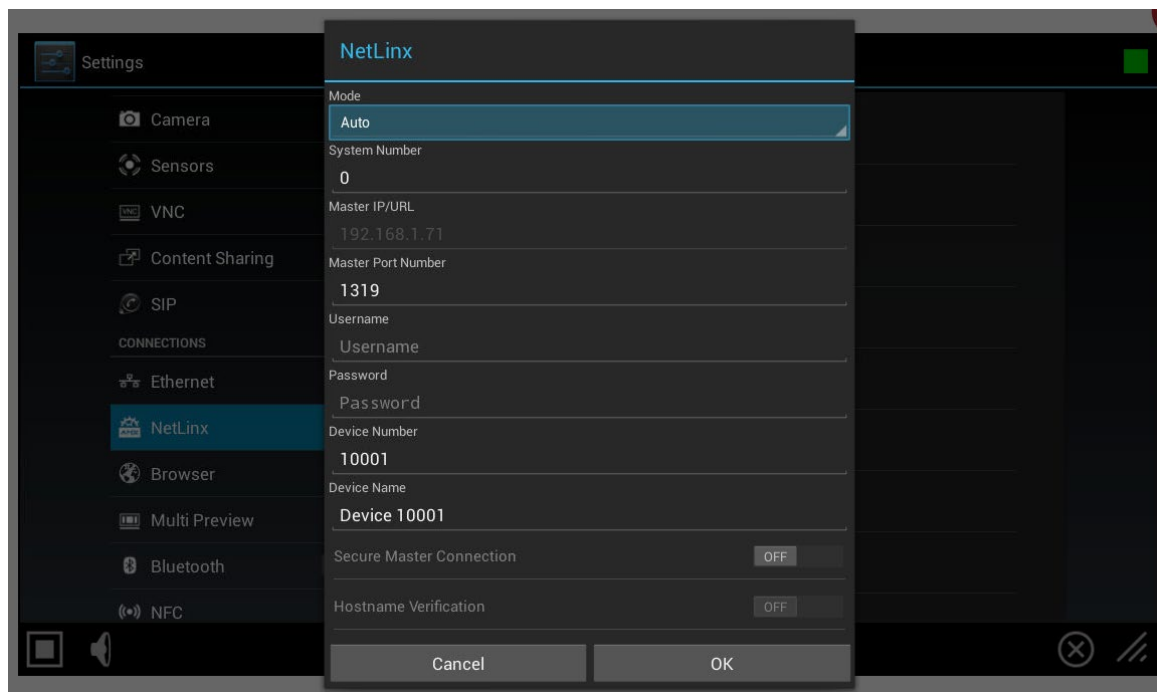


22) Select NetLinx from the main settings menu on the left

SchoolView



23) Press the Mode field



24) Press the Mode dropdown menu and select URL.

25) Press the Master IP/URL field

26) For admin panels enter the IP address of the primary master:
"192.168.1.71"

For classroom panels enter the IP address of the assigned classroom master.

27) Press Next

SchoolView

- 28) Enter Master Port Number: "1319" (default).
- 29) Press Next
- 30) Leave Username blank (default)
- 31) Press Next
- 32) Leave Password blank (default)
- 33) Press Next
- 34) Enter assigned Device Number: "10001" (Note: Admin panels are device numbers 10001 – 10004, classroom panels are device numbers 11001 – 11254 the last octet of the panel IP address typically matches the last three digits of the device number)
- 35) Press Next
- 36) Enter Device Name: "Admin Panel 1"
- 37) Press Done
- 38) Press OK
- 39) Close the menu (X in the lower right hand corner)

SchoolView

NetLinx Master Configuration

The SchoolView solution utilizes multiple AMX NetLinx masters, and each NetLinx master in the system must be configured with IP Address settings. This includes the primary master (in the audio rack) and classroom masters (various locations depending on configuration).

To configure the NetLinx master network settings you have multiple options.

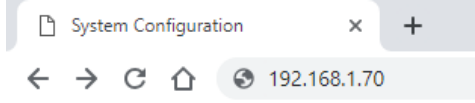
1. Use Netlinx Studio (Ethernet or USB)
2. Use the web interface
3. Use Telnet commands

Only the web interface option will be shown in detail below. For more information about the other options please consult the product information available at amx.com for both the [NX-1200](#) and [Netlinx Studio](#).

Enter exact contents of quotes as shown, except replace example values as necessary.

Follow these steps:

1. Open a web browser and type the IP address of the master into the address bar.



2. Press enter and you should see the following page

192.168.1.70/web/http/nxmaster/login.html?path=/web/http/nxmaster/default.html#/network-ipv4

System Configuration

A screenshot of the "System Configuration" login page. The page has a dark header with the title "System Configuration". Below the header is a "Login" form with two input fields: "Username:" and "Password:". A "Login" button is located at the bottom right of the form.

3. Enter the username "administrator" and the password "password". Select the Login button. If the login attempt is successful you should see the home page of the master.



System Configuration



SchoolView

4. Select the Network menu -> IPv4 Setup

IPv4 Setup IPv6 Setup Date / Time

IPv4 Network Settings for the System.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

IP Address	DNS Address
<p>IP Hostname: AMX22100</p> <p>DHCP Specific IP Address</p> <p>IP Address: 192.168.1.70</p> <p>Subnet Mask: 255.255.255.0</p> <p>Gateway: 192.168.1.1</p>	<p>Domain: </p> <p>DNS IP 1: 192.168.1.1</p> <p>DNS IP 2: </p> <p>DNS IP 3: </p>
<p>Zero-Config Networking</p> <p>Off On</p>	<p>NetLinx Discovery Protocol (NDP)</p> <p>Off On</p>

5. Select Specific IP Address and enter the correct information for your site into the following fields.
- IP Address
 - Subnet Mask
 - Gateway
 - Domain
 - DNS IP 1
 - DNS IP 2 (optional)
 - DNS IP 3 (optional)
 - Leave Zero-Config Networking set to ON
 - Leave NetLinx Discovery Protocol (NDP) set to ON

SchoolView

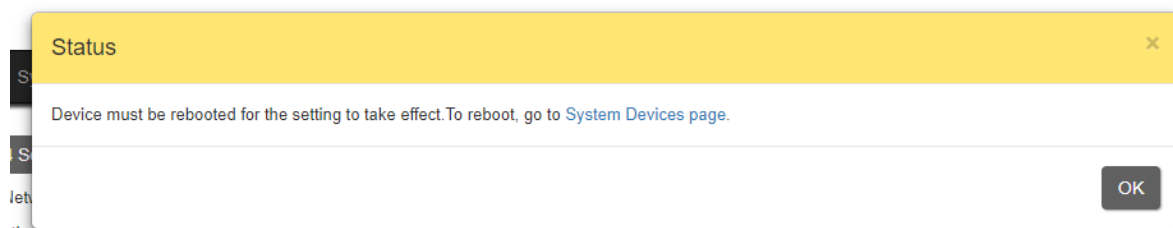
IPv4 Setup IPv6 Setup Date / Time

IPv4 Network Settings for the System.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

IP Address IP Hostname: <input type="text" value="PrimaryMaster"/> DHCP: <input checked="" type="radio"/> Specific IP Address IP Address: <input type="text" value="192.168.1.70"/> Subnet Mask: <input type="text" value="255.255.255.0"/> Gateway: <input type="text" value="192.168.1.1"/>	DNS Address Domain: <input type="text" value="ExampleSD.com"/> DNS IP 1: <input type="text" value="192.168.1.1"/> DNS IP 2: <input type="text"/> DNS IP 3: <input type="text"/>
Zero-Config Networking <input type="radio"/> Off <input checked="" type="radio"/> On	NetLinx Discovery Protocol (NDP) <input type="radio"/> Off <input checked="" type="radio"/> On

- j. Select the Accept button to confirm the new IP address settings.
- k. A message pop-up will inform you the system needs to be rebooted for the changes to take effect. Use the link in the message to go to the System Devices Page.



- l. At the system devices page select Reboot

SchoolView

Info **Devices**

Select a device in the list to view its details.

Press the Accept button to save changes. Press the Cancel button to revert values from the System. Press the Reboot button for Device changes.

The screenshot shows the 'Devices' section of the SchoolView interface. On the left is a 'Device List' with a scrollable list of devices, including '00000 NX-1200 Master' (highlighted) and various 'Virtual' devices. On the right are two panels: 'System Information' and 'Device Information'. The 'System Information' panel has a 'System Number' field with the value '25001' and a 'Reset to Factory Defaults' button. The 'Device Information' panel displays details for device '0', including 'Device Name: NX-1200 Master', 'Port Count: 62', 'Firmware ID: 1116', 'Manufacturer: AMX LLC', and 'Version: v1.5.78'. At the bottom, there are 'Reboot', 'Cancel', and 'Accept' buttons.

m. You will see the message below. Select Yes.

A yellow warning dialog box with the title 'Warning' and a close button. The text inside asks, 'Are you sure you want to reboot device 0?'. At the bottom right, there are 'No' and 'Yes' buttons.

n. Wait for the master to reboot and repeat steps 1 – 3 to login using the new IP address.

6. After the master has been rebooted follow the additional steps below for the primary master to configure a network time server (NTP server).

a. After logging in select Network -> Date / Time from the menu bar at the top of the screen.

The screenshot shows the 'Date / Time' configuration screen in the SchoolView interface. At the top, there are tabs for 'IPV4 Setup', 'IPV6 Setup', and 'Date / Time'. Below the tabs, it says 'Clock Settings for the System.' and 'Press the Accept button to save changes. Press the Cancel button to revert values from the System.' The main area is titled 'Clock Manager' and contains several settings: 'Timezone:' set to 'GMT-06:00 Central Time (US & Canada), AMX HQ'; 'Time Sync:' with 'Network Time' and 'Stand Alone' buttons; 'Date:' set to '03/25/2019'; and 'System Clock:' showing '13:17:32' and '03/25/2019'. At the bottom, there are 'Hours:', 'Minutes:', and 'Seconds' dropdown menus with values '13', '15', and '37' respectively. At the bottom right, there are 'Cancel' and 'Accept' buttons.

SchoolView

- b. Use the Timezone drop down to select the correct time zone for your location.
- c. Select Network Time under the Time Sync settings. This will show additional fields.

IPv4 Setup IPv6 Setup **Date / Time**

Clock Settings for the System.
Press the Accept button to save changes. Press the Cancel button to revert values from the System.

Clock Manager
Timezone: GMT-06:00 Central Time (US & Canada), AMX HQ
Time Sync: **Network Time** Stand Alone
Re-Sync Period: 1 hour
System Clock: 13:19:14
03/25/2019

Daylight Savings Time Manager
Daylight Savings: **Off** On

NIST Server Manager

Select	Server Name	IP	Location	Remove
<input checked="" type="radio"/>	time-a.timefreq.bldrdoc.gov	132.163.4.101	NIST, Boulder, Colorado	
<input type="radio"/>	time-b.timefreq.bldrdoc.gov	132.163.4.102	NIST, Boulder, Colorado	
<input type="radio"/>	time-c.timefreq.bldrdoc.gov	132.163.4.103	NIST, Boulder, Colorado	

+ Add Server

- d. Select the Add Server button
- e. Fill in the dialog box with the information for the school districts NTP server and select Accept when finished.

Add New Server
New Server URL: *
time.example.edu
New IP: *
192.168.1.1
New Location: *
Texas

- f. The new time server should now appear in the NIST Server Management list. Use the radio button to select the new server you added as the server to use.

SchoolView

NIST Server Manager

Select	Server Name	IP	Location	Remove
<input type="radio"/>	time-a.timefreq.blrdoc.gov	132.163.4.101	NIST, Boulder, Colorado	
<input type="radio"/>	time-b.timefreq.blrdoc.gov	132.163.4.102	NIST, Boulder, Colorado	
<input type="radio"/>	time-c.timefreq.blrdoc.gov	132.163.4.103	NIST, Boulder, Colorado	
<input checked="" type="radio"/>	time.example.edu	192.168.1.1	Texas	<input type="checkbox"/>

- g. Click the Accept button. The system clock should now display the time supplied by the time server. If the building has a clock system the same NTP server should be configured as the time source for the clocks.

SchoolView

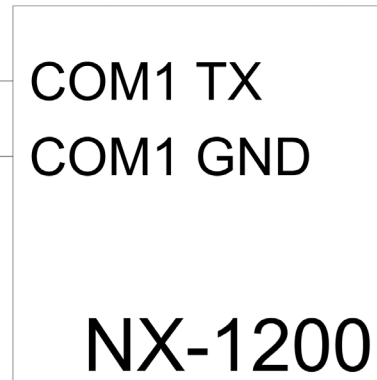
ATS Clocks Connection

The SchoolView solution utilizes ATS RS232 clocks, such as the CC2002 and similar models (different mounting and display styles available, as required by your particular project). We provide time (and emergency alert data depending on model) updates via an RS232 connection from any of the NetLinx masters or specially configured Barix. You can get the clocks running independently before SchoolView software deployment by applying power at exactly 12:00.

ATS



AMX



WHT/ORG

BLK/RED

COM1 TX

COM1 GND

NX-1200

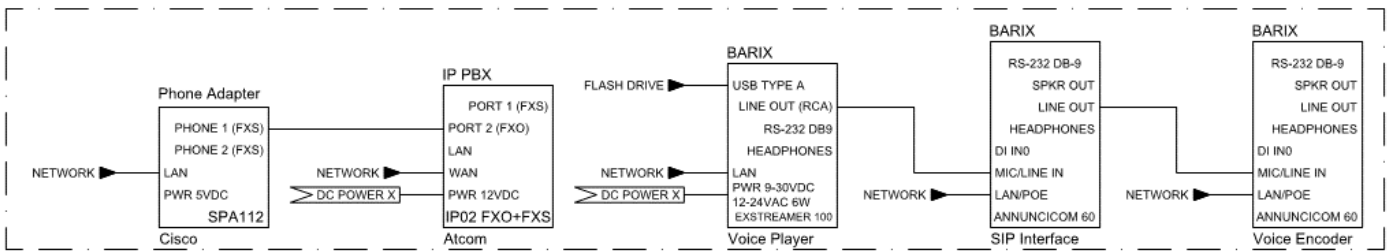
SchoolView

Telephone Interface Configuration

If using the enhanced phone interface option please follow the steps below to configure the hardware. Older sites may have a legacy telephone interface option known as the basic phone interface, this can be identified by the presence of a JK Audio AutoHybrid box connected to an analog phone line. The basic phone interface is not compatible with SchoolView versions running on NX hardware. For further information on configuration options for a basic phone interface please consult version 7.5.2 of this guide or contact tech support.

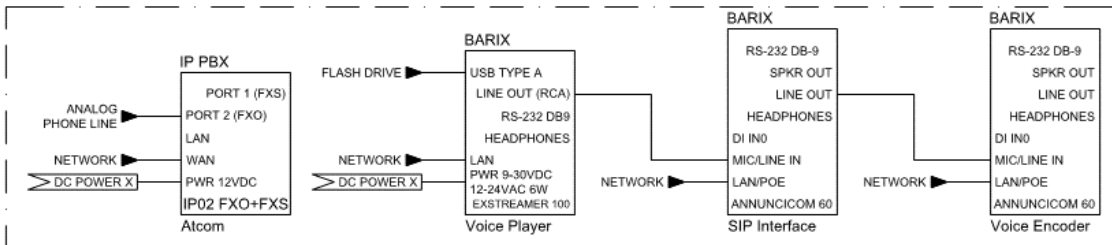
The Enhanced Phone Interface has three options depending on the type of phone service. Those three options are shown in the diagrams below.

OPTIONAL - 1 ONLY



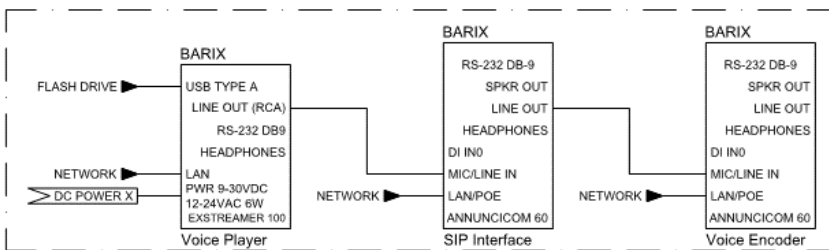
Enhanced Phone Interface - VOIP Interface (Non Cisco Call Manager)

OPTIONAL - 1 ONLY



Enhanced Phone Interface - POTS Line Interface

OPTIONAL - 1 ONLY



Enhanced Phone Interface - Cisco Call Manager Integration

All options require two Annunicom 60 boxes and one Exstreamer 100 box. The flash drive with voice prompts is no longer included with the package. The integrator must supply a flash drive with a copy of the voice prompts audio files. The audio files can be found in the Schoolview release \MP3 Files\ folder. Copy the voice folder to the flash drive and insert it into the Exstreamer 100.

If an analog phone line interface is needed an Atcom IP02 FXO+FXS box can act as the interface between the SIP Barix and VOIP system. If a VOIP system other than Cisco Call Manager is employed at the site than a Cisco SPA112 and Atcom IP02 FXO+FXS are both required to complete the interface with the SIP Barix.

SchoolView

Other Audio Device Connections

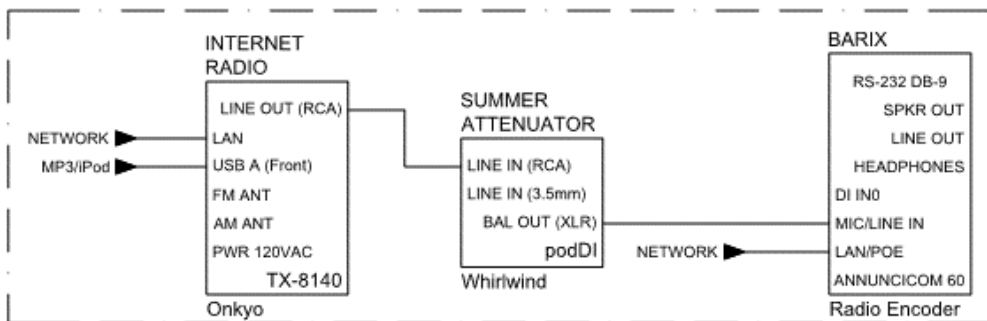
Head End Audio Sources

When connecting stereo sources such as CD players and AM/FM tuners to the system, they will have to be attenuated and summed to interface with the audio inputs on an Annunicom 60 or 100. In order to make these connections correctly, you will need to employ passive line level audio combiners/attenuators, such as the Whirlwind PodDI (shown below).



The connections between the Onkyo TX-8140, PodDI and Annunicom 60 are shown below as an example.

OPTIONAL - CONTROLLED



Background Music Source - Onkyo Internet Radio

When using the PodDI for audio summing/attenuation either the 3.5mm or RCA inputs may be used.

Common Zone Amplifiers

Typical common zone speakers will be driven by 70v amplifiers and may or may not employ the use of attenuators (wall mounted volume knobs) in the speaker lines. The audio to the common zone amplifiers will be connected from the output of a Barix (typically an Annunicom 60 but can be an Annunicom 100 in special situations). Be sure to install these high-power audio devices per the manufacturer's instructions and recommendations. State and local codes may require special care regarding the installation of these devices in your area.

SchoolView

Barix Audio Encoder/Decoder Configuration

The SchoolView solution uses Barix audio and control devices in several different roles throughout the system. They will each need to have network settings configured regardless of their role. Each one will have software loaded and be configured appropriately later.

To configure the Barix network settings, follow these steps:

- 1) Connect the Barix to a DHCP enabled network.
- 2) Apply power to the Barix.
- 3) Identify the leased IP address (router's attached devices, IP scan, headphones or other).
 - a) If the Barix doesn't find a DHCP server, it should default to x.y.z.168 (or the next available higher address) where x.y.z matches other devices on the same local network segment that are generating traffic (like your PC).
- 4) Connect to the Barix using a web browser
 - a) If the Barix is running SchoolView firmware open a web browser to http://<BARIX_IP>/config.html
 - i) If the Barix is running SchoolView firmware go directly to step 8.
 - b) If the Barix is not running a SchoolView firmware image open a web browser to http://<BARIX_IP>/
 - i) The steps shown below are for a Barix running default firmware.
- 5) When you see this homepage click Configuration

The screenshot shows a web browser window with the address bar displaying "192.168.1.91/index.html". The page title is "Full-duplex Intercom" and the BARIX logo is visible in the top right corner. The interface is divided into several sections:

- Navigation Menu:** HOME, CONFIGURATION, STATUS, DEFAULTS, UPDATE, REBOOT. A red status bar at the top right shows "Annunicom 50 OEM MAC: 00:08:E1:02:CC:03 FW V01.21".
- APPLICATION STATUS:**
 - Streaming Mode: Send Always
 - Remote Party: No Stream
- AUDIO STATUS:**
 - Current Volume: 0 %
 - Input Peak Level: -61 dB
 - Output Peak Level: -90 dB
- Help:**
 - Home page: Gives an overview of the most important settings of the unit.
 - APPLICATION STATUS
 - Streaming Mode: Shows the current streaming mode of the application, and may take the following values:
 - Send Always: In this mode the application is always sending a stream to the configured destination IP and

SchoolView

- 6) You should then see the main configuration page. Click Advanced Settings in the menu on the left

The screenshot shows the BARIX IP Intercom configuration page. The browser address bar shows "192.168.1.91". The page has a navigation menu with "HOME", "CONFIGURATION", "STATUS", "DEFAULTS", "UPDATE", and "REBOOT". The "CONFIGURATION" tab is active. The page title is "Full-duplex Intercom". The "Streaming Mode" is set to "Send Always". The "BASIC SETTINGS" section is active, showing fields for "Destination IP:Port", "Source IP", and "Local Listen Port". The "Help" section on the right provides detailed instructions for each field.

BASIC SETTINGS

Destination IP:Port: 0 . 0 . 0 . 0 : 0

Source IP: 0 . 0 . 0 . 0

Local Listen Port: 0

Help

BASIC SETTINGS

Destination IP:Port
Destination address and port where the audio stream will be sent to. Enter your peer's UDP address and port here. Default port: "3030"

Source IP
Enter IP address of your source here. The annunicom will receive audio stream only from this address. This address can be 0.0.0.0 to accept any stream coming to the receiving port; a **multicast address** to subscribe to a specific multicast group; or a **unicast address** to receive stream from a specific source only. Default: "0.0.0.0"

Local Listen Port
Local UDP stream receive port. Set to a value between 0 (disabled) and 65535. Default port is "3030".

- 7) You should then see the configuration page shown below.

The screenshot shows the BARIX IP Intercom configuration page. The browser address bar shows "192.168.1.91". The page has a navigation menu with "HOME", "CONFIGURATION", "STATUS", "DEFAULTS", "UPDATE", and "REBOOT". The "CONFIGURATION" tab is active. The page title is "Full-duplex Intercom". The "Streaming Mode" is set to "Send Always". The "NETWORK SETTINGS" section is active, showing fields for "Use SonicIP", "IP Address", "Netmask", "Gateway IP Address", "Primary DNS", "Alternative DNS", "Syslog Address", "DHCP Host Name", "Web Server Port", "SNMP System Name", "SNMP System Location", and "SNMP System Contact". The "Help" section on the right provides detailed instructions for each field.

NETWORK SETTINGS

Use SonicIP®: Yes No

IP Address: 0 . 0 . 0 . 0

Netmask: 0 . 0 . 0 . 0

Gateway IP Address: 0 . 0 . 0 . 0

Primary DNS: 0 . 0 . 0 . 0

Alternative DNS: 0 . 0 . 0 . 0

Syslog Address: 0 . 0 . 0 . 0

DHCP Host Name: []

Web Server Port: 80

SNMP System Name: []

SNMP System Location: []

SNMP System Contact: []

Help

NETWORK SETTINGS

Use SonicIP
If set to "yes", the device will announce its IP address over the audio output during device startup. Default: "yes"

IP Address
Enter the 4 values of the desired device IP address e.g.: "0.0.0.0" for automatic discovery (DHCP/BOOTP, IPzator, AutoIP) "192.168.0.12" for an internal LAN Default: "0.0.0.0"

Netmask
Enter the 4 values of the desired Static IP e.g.: "0.0.0.0" for a default Netmask depending on the used IP Address. "255.255.255.0" for a C class network Default: "255.255.255.0"

Gateway IP Address
Enter the 4 values of the desired Gateway IP address e.g.: "0.0.0.0" for no Gateway "192.168.0.1" for a Gateway in a LAN

- 8) Fill in the following fields with the information for the Barix you are configuring
- Leave SonicIP set to "yes"
 - IP Address
 - Netmask
 - Gateway IP Address
 - Primary DNS (optional)
 - Secondary DNS (optional)
 - Syslog Address – Leave as 0.0.0.0 (this field is not present if the Barix is running SV firmware)
 - DHCP Host Name – ex. "Brx Rm 103" (max. 15 characters)
- 9) When all network settings have been entered click the Apply button to save the settings and reboot the Barix. If speakers or headphones are connected to the Barix you should hear the new IP address announced when the Barix

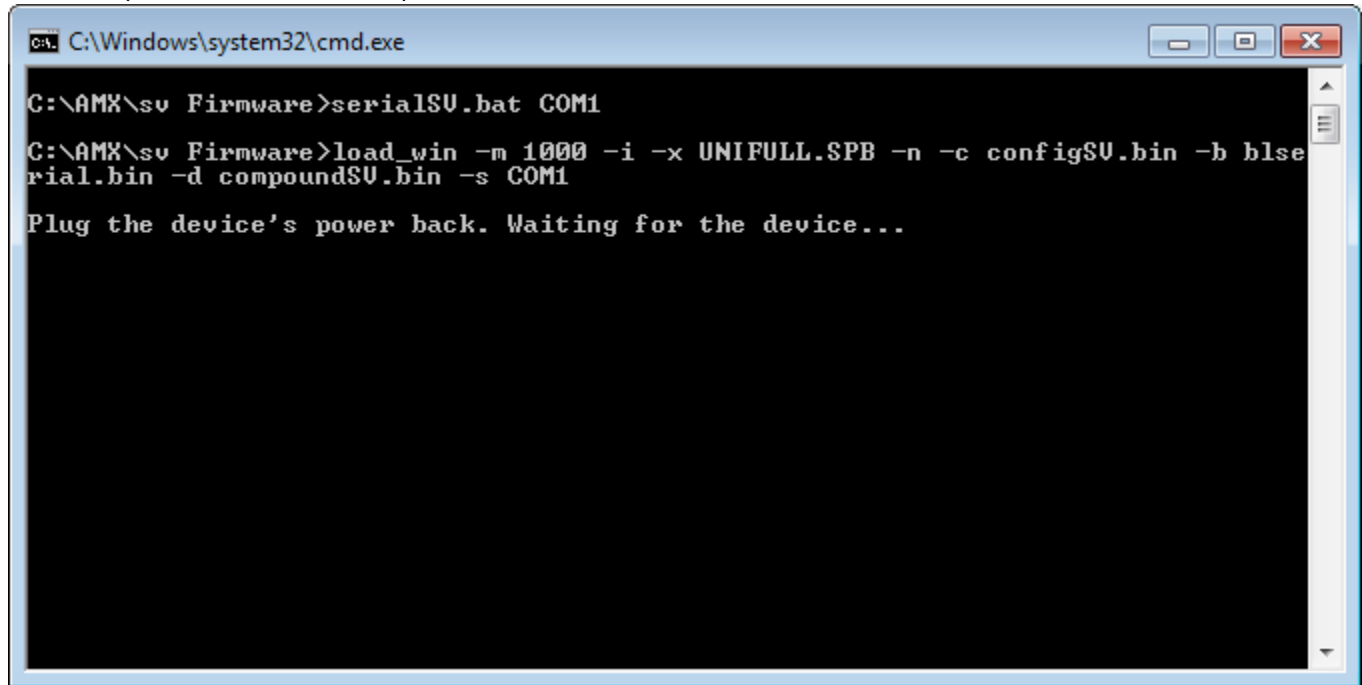
SchoolView

reboots.

Barix Serial Rescue

If the Barix cannot be reached via IP (unusual), or the boot loader needs to be updated, you must re-load the firmware via a serial (RS232) connection. To do so, follow these steps:

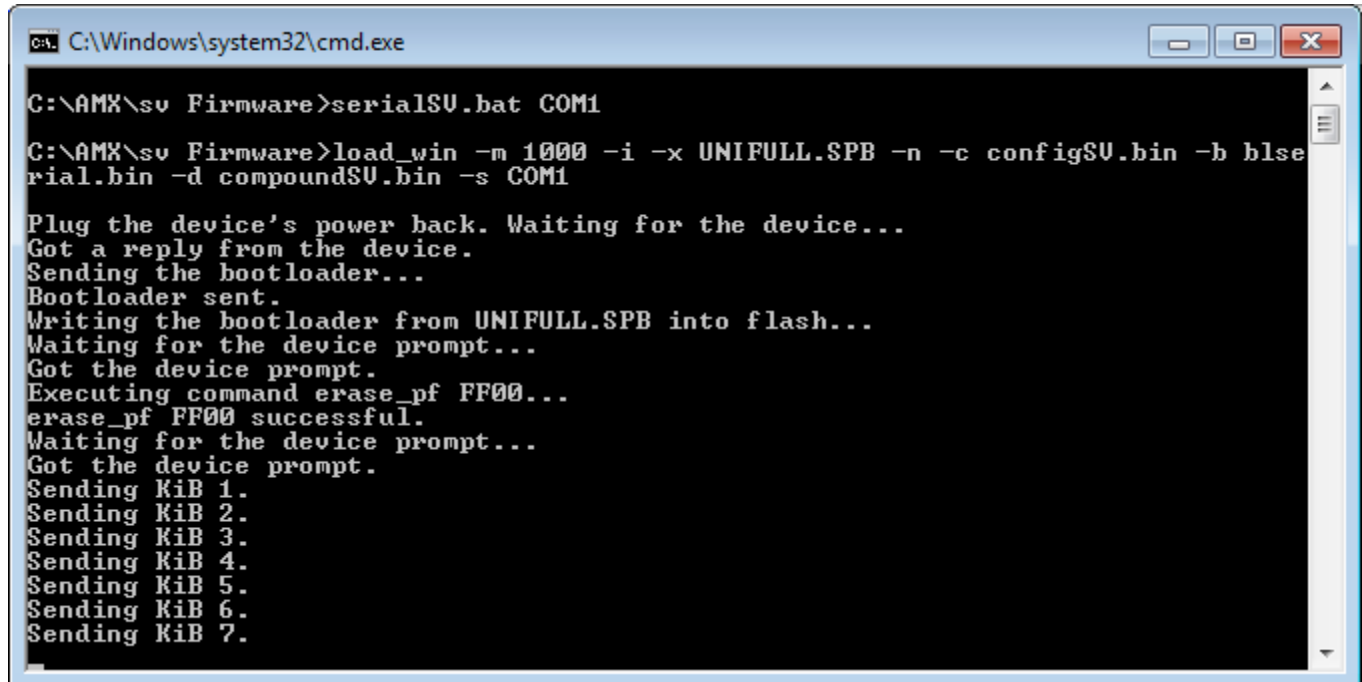
- 1) Connect a DB9 F-F null modem serial cable between the Barix and a PC serial port.
- 2) Locate and run the SchoolView provided serial1SV.bat file, assuming you are using COM1. If you are using COM2, 3 or 4, use serial2SV.bat, etc.
- 3) When you see the message "Plug the device's power back. Waiting for the device..." apply power to the Barix (See screenshots below).

A screenshot of a Windows command prompt window titled "C:\Windows\system32\cmd.exe". The window has a black background with white text. The text shows the following commands and output:

```
C:\AMX\sv Firmware>serialSU.bat COM1
C:\AMX\sv Firmware>load_win -m 1000 -i -x UNIFULL.SPB -n -c configSU.bin -b blse
rial.bin -d compoundSU.bin -s COM1
Plug the device's power back. Waiting for the device...
```

- 4) You should see the following confirmations and the first file transfer will begin. If a failure occurs before the file transfer, remove power from the Barix and press <Ctrl>-c to abort the process. You will be asked to press y to confirm. Return to step 2 and try again.

SchoolView



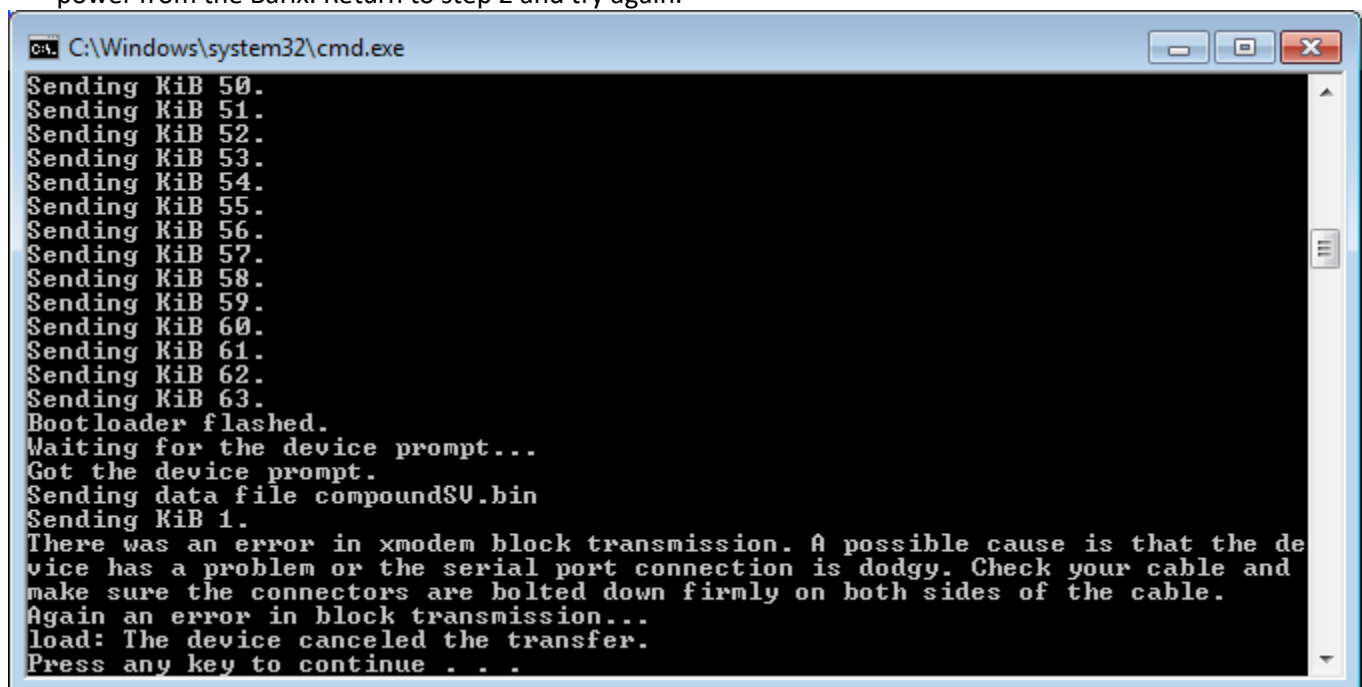
```
C:\Windows\system32\cmd.exe

C:\AMX\sv Firmware>serialSU.bat COM1

C:\AMX\sv Firmware>load_win -m 1000 -i -x UNIFULL.SPB -n -c configSU.bin -b blserial.bin -d compoundSU.bin -s COM1

Plug the device's power back. Waiting for the device...
Got a reply from the device.
Sending the bootloader...
Bootloader sent.
Writing the bootloader from UNIFULL.SPB into flash...
Waiting for the device prompt...
Got the device prompt.
Executing command erase_pf FF00...
erase_pf FF00 successful.
Waiting for the device prompt...
Got the device prompt.
Sending KiB 1.
Sending KiB 2.
Sending KiB 3.
Sending KiB 4.
Sending KiB 5.
Sending KiB 6.
Sending KiB 7.
```

- 5) The most common place for the process to fail is after the boot loader is completely written, during the first KB of the second file transfer. If this occurs, press any key to continue, this will terminate the process. Remove power from the Barix. Return to step 2 and try again.

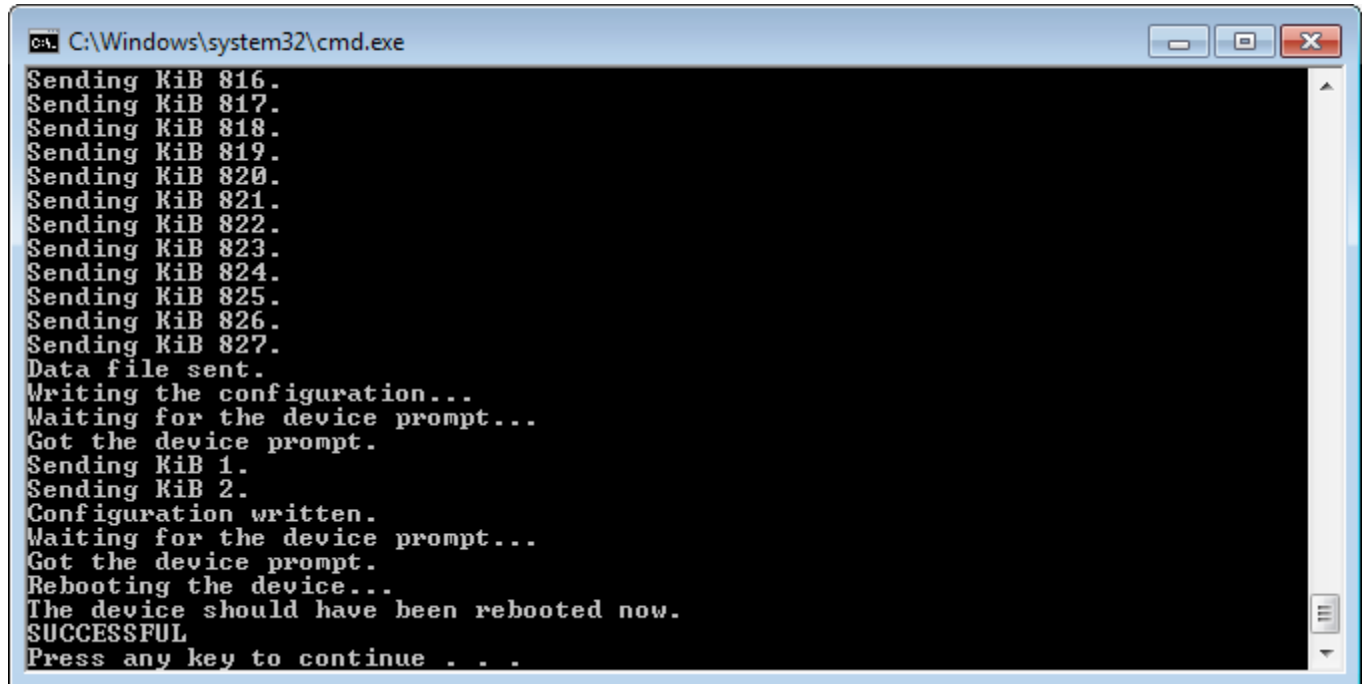


```
C:\Windows\system32\cmd.exe

Sending KiB 50.
Sending KiB 51.
Sending KiB 52.
Sending KiB 53.
Sending KiB 54.
Sending KiB 55.
Sending KiB 56.
Sending KiB 57.
Sending KiB 58.
Sending KiB 59.
Sending KiB 60.
Sending KiB 61.
Sending KiB 62.
Sending KiB 63.
Bootloader flashed.
Waiting for the device prompt...
Got the device prompt.
Sending data file compoundSU.bin
Sending KiB 1.
There was an error in xmodem block transmission. A possible cause is that the device has a problem or the serial port connection is dodgy. Check your cable and make sure the connectors are bolted down firmly on both sides of the cable.
Again an error in block transmission...
load: The device canceled the transfer.
Press any key to continue . . .
```

- 6) If the second file transfer proceeds beyond the first KB, it will typically finish unless something becomes unplugged. In this case, you should see a confirmation, followed by a prompt to press any key to continue. This will end the process.

SchoolView



```
C:\Windows\system32\cmd.exe
Sending KiB 816.
Sending KiB 817.
Sending KiB 818.
Sending KiB 819.
Sending KiB 820.
Sending KiB 821.
Sending KiB 822.
Sending KiB 823.
Sending KiB 824.
Sending KiB 825.
Sending KiB 826.
Sending KiB 827.
Data file sent.
Writing the configuration...
Waiting for the device prompt...
Got the device prompt.
Sending KiB 1.
Sending KiB 2.
Configuration written.
Waiting for the device prompt...
Got the device prompt.
Rebooting the device...
The device should have been rebooted now.
SUCCESSFUL
Press any key to continue . . .
```

7) You may now proceed with the normal Barix configuration process as described above.

SchoolView

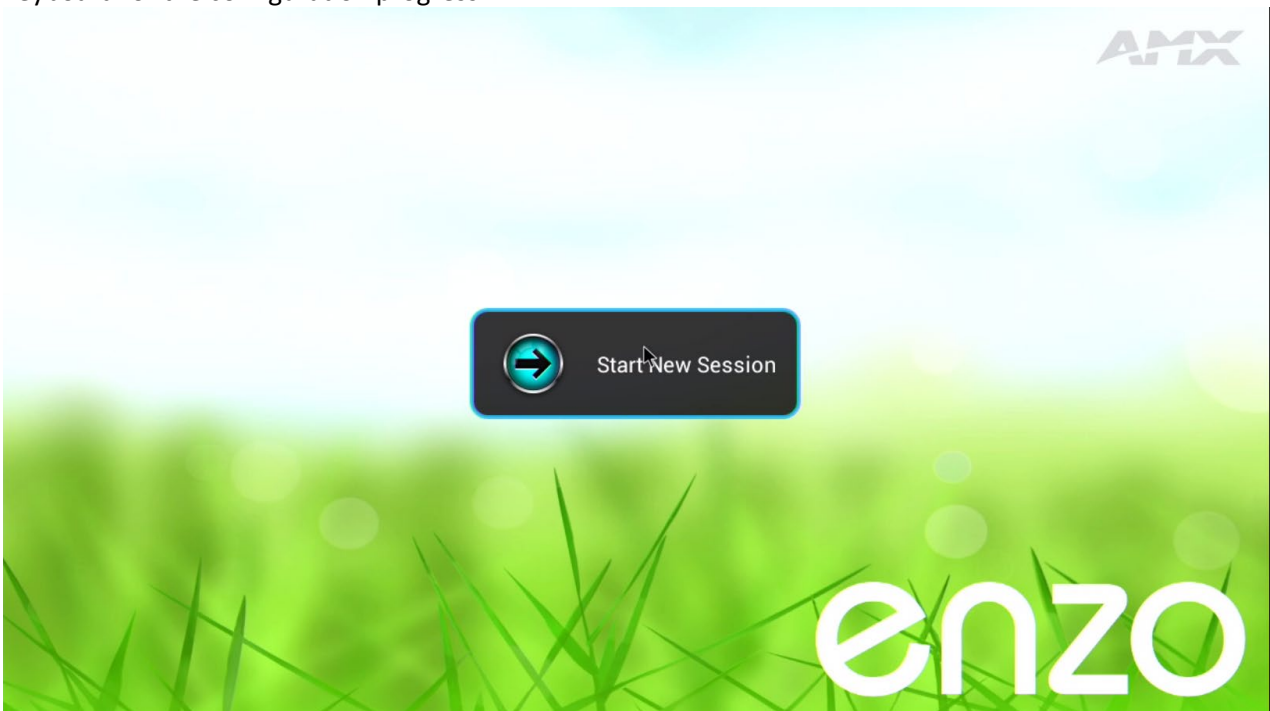
Video Decoder Configuration

Currently there are two supported video decoders for unified classrooms. One is the AMX Enzo and the other is the AMX SVSI N3xxx decoder. Instructions for configuring both are below.

Enzo Configuration

Enzo video decoders are used to decode video streams in classrooms as well as the head end (for common zone audio from video streams). In addition to configuring the Enzo with a keyboard it is also possible to use SSH for configuration. For more information download the “Programmers Guide - NMX-MM-1000 Enzo Meeting Presentation System” from the AMX website. The SSH commands “ip” and “netlinx” allow for setting all of the same options you would set using a keyboard.

- 1) Connect the Enzo to a display and POE network connection. You will also need a wireless or wired keyboard for the configuration progress.

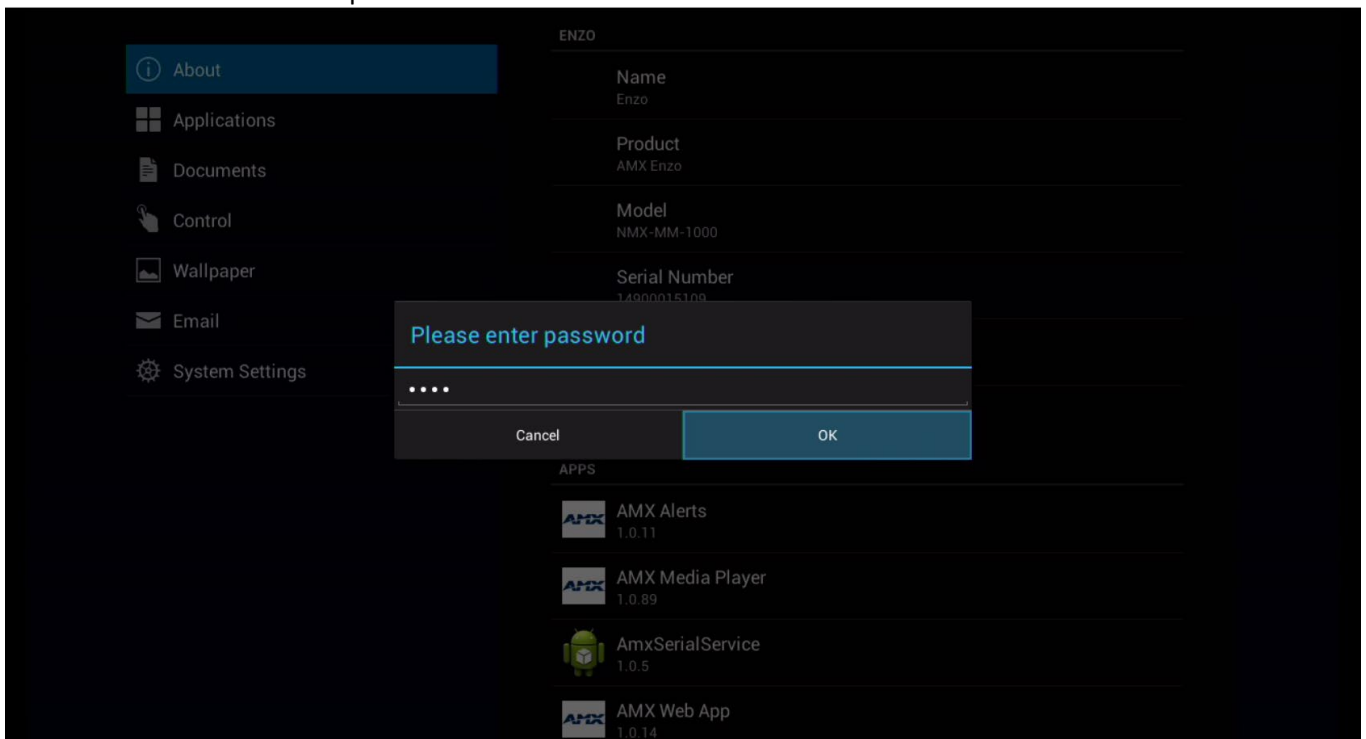


- 2) At the start screen select Start New Session

SchoolView

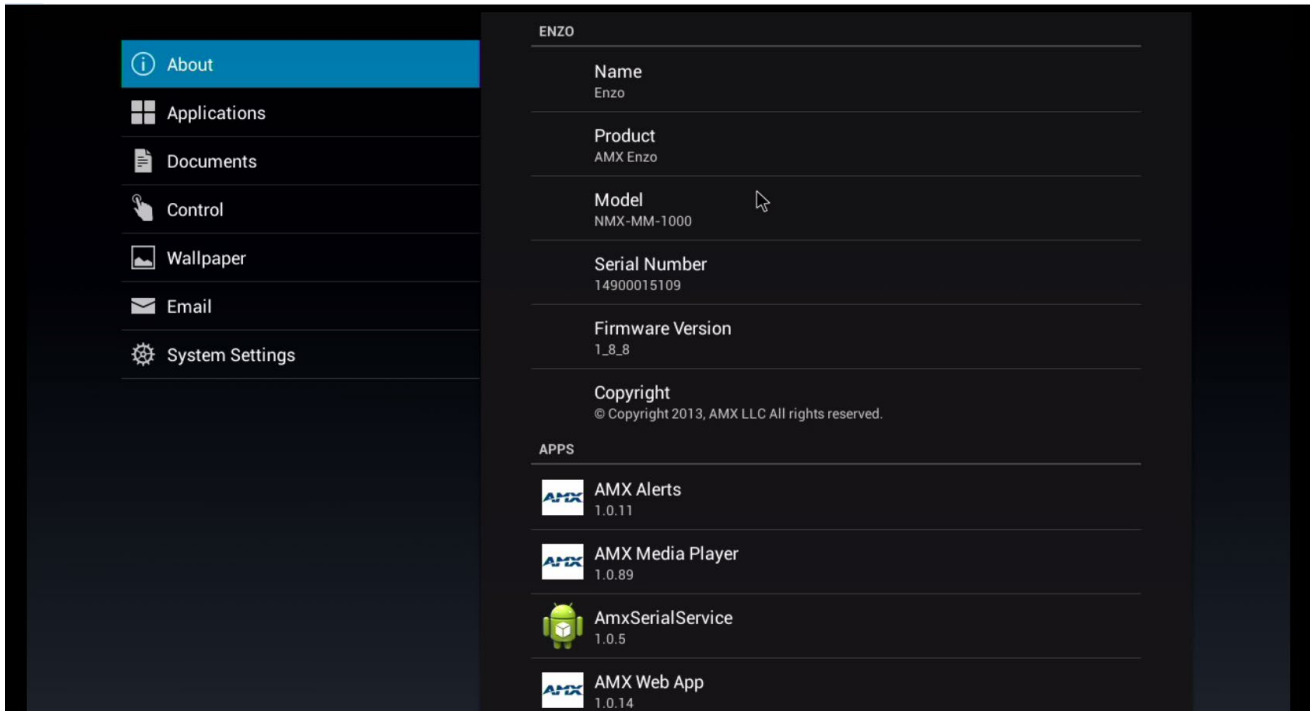


3) Once the session has loaded press F12 to access the menu.

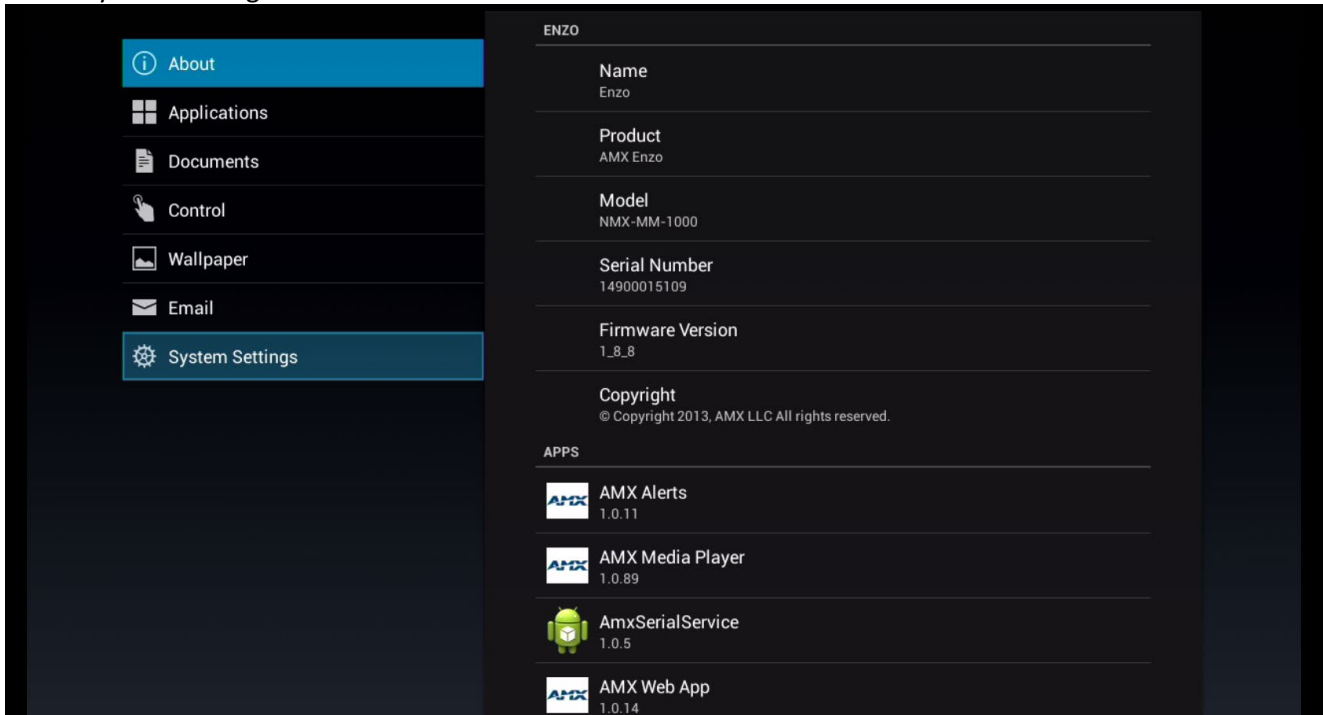


4) Enter the default password: 1988
Select OK to access the menu

SchoolView

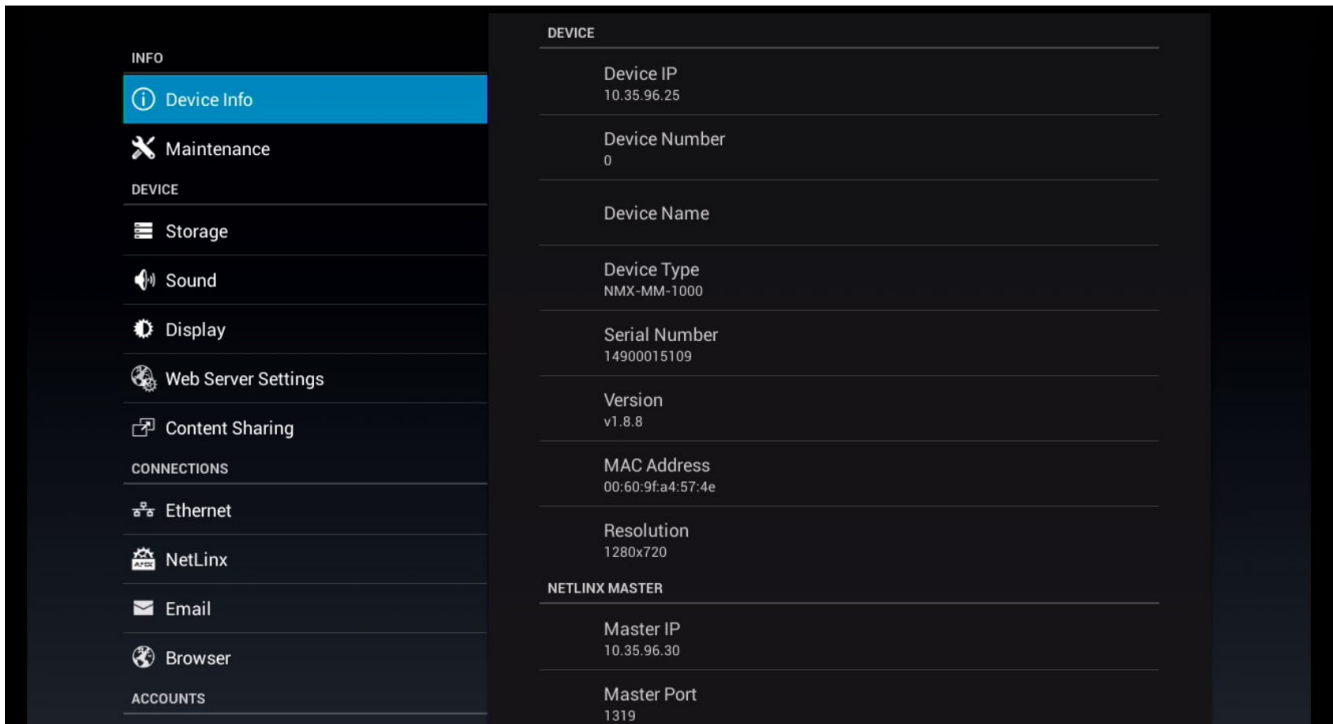


5) Select System Settings

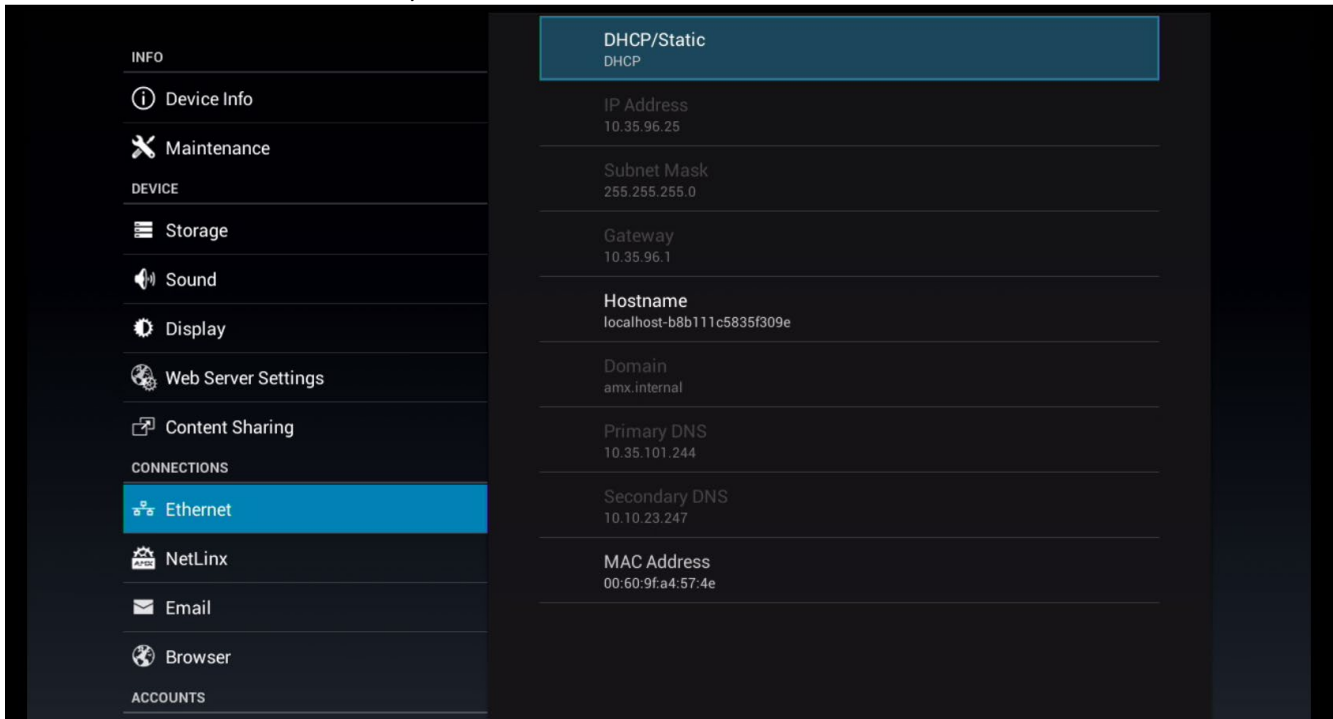


6) In the settings menu select Ethernet

SchoolView

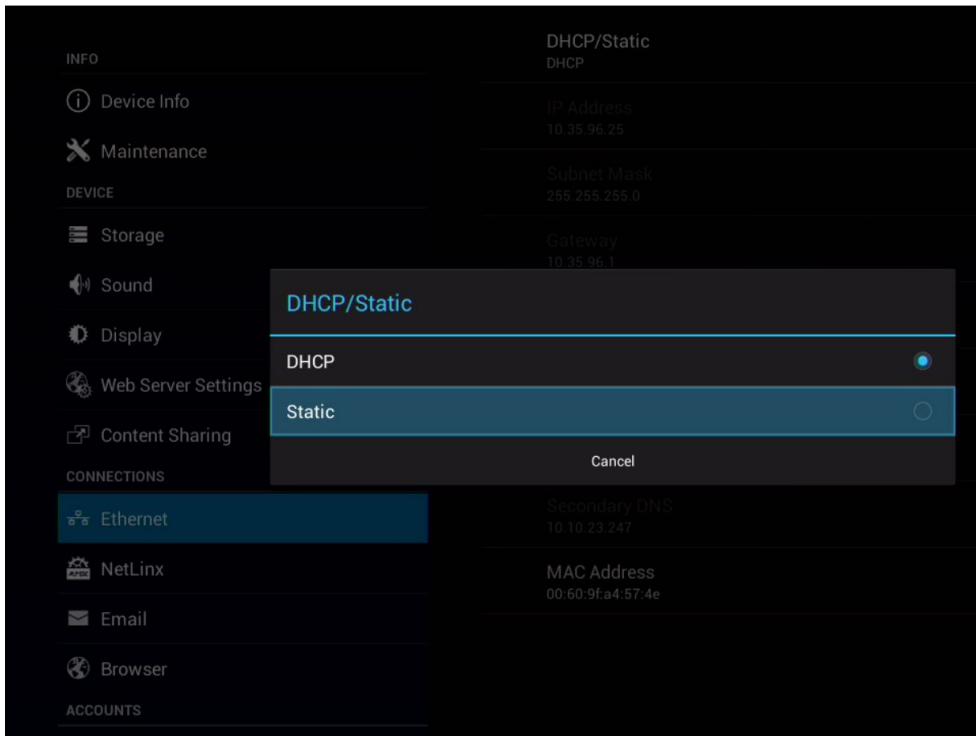


7) In the Ethernet menu select DHCP/Static

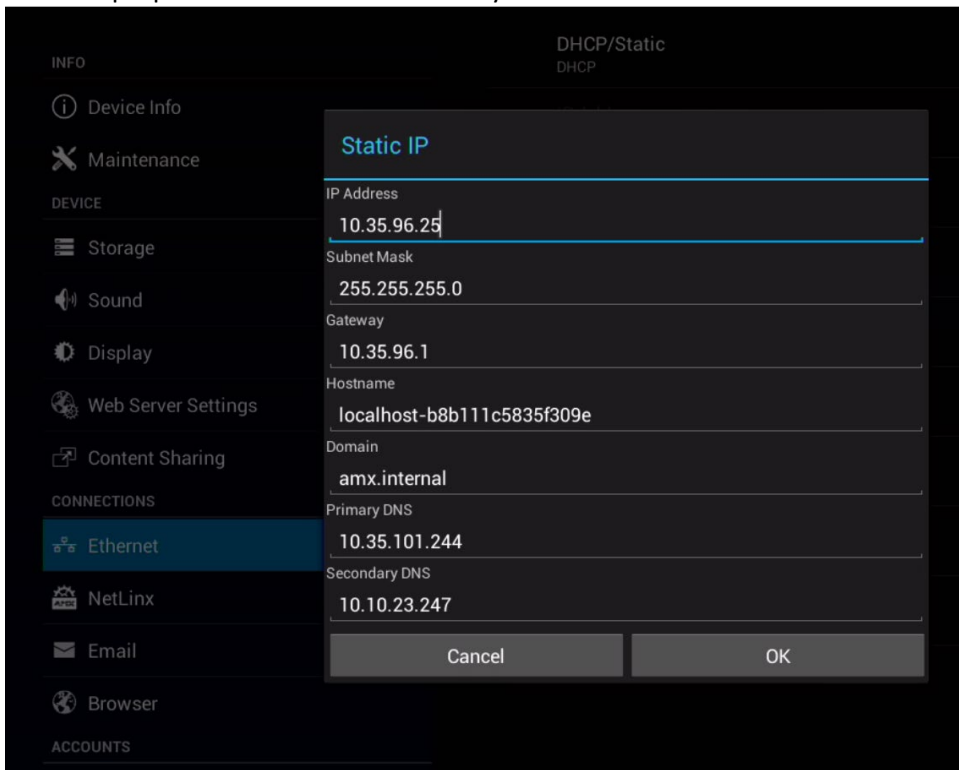


8) In the DHCP/Static menu select Static

SchoolView

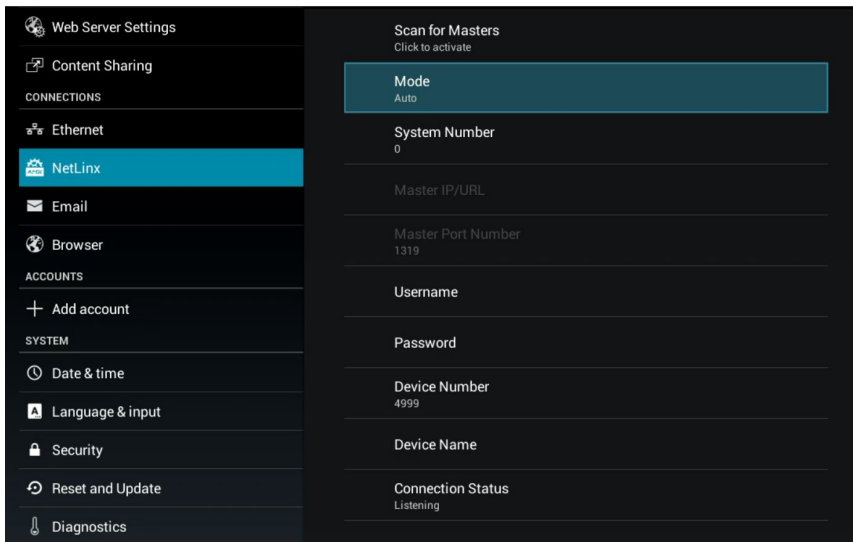


- 9) After selecting Static in the DHCP/Static options the dialog shown below will allow for setting all of the network properties. Enter the values for your site and select OK when finished.

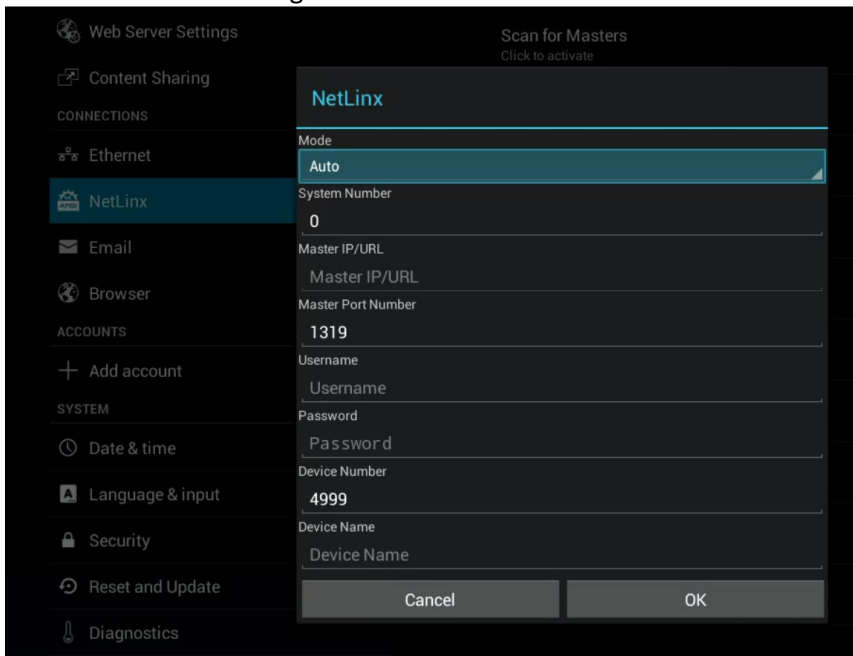


- 10) After configuring the network connections you will need to select OK to save your changes.

SchoolView



11) Select the Netlinx settings from the main menu on the left. Once in Netlinx settings select Mode.



12) Make the following changes

- a) Mode – Change to URL
- b) Master IP/URL – Enter the IP address of the appropriate master.
- c) Master Port Number – Leave at the default of 1319
- d) Device Number – For classroom/digital signage Enzo devices use range 1001 – 1999. Standard convention is for the last three digits to match the last octet of the device IP address, zero padded to three places if necessary. For the audio extract Enzo the device number may be outside this range, typically 4999.
- e) When all settings have been entered select OK to save your changes.

13) Press ESC twice to exit the menu and return to the main Enzo screen.

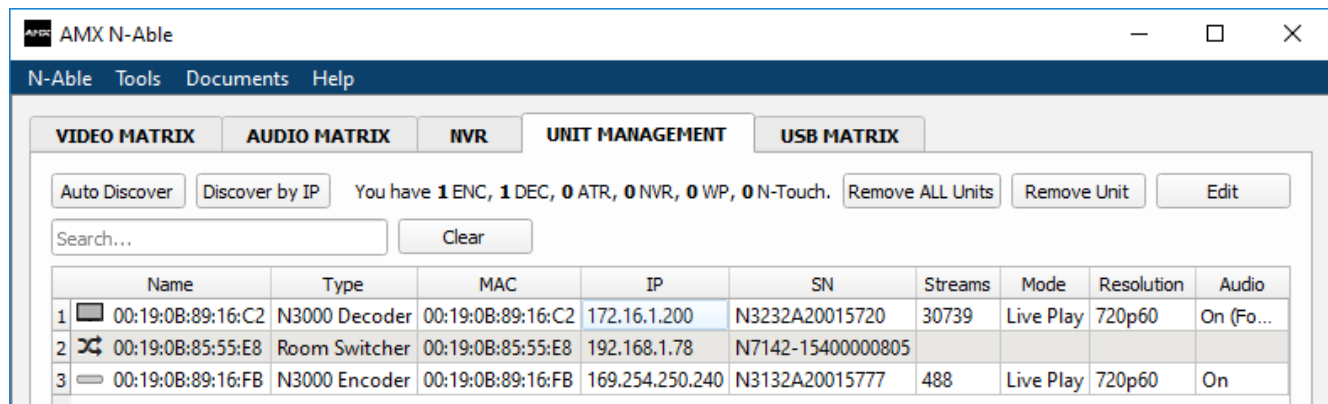
SchoolView

SVSI Configuration

For configuring SVSI encoders and decoders the N-able software is required. If you do not already have the N-able software installed you will need to download the latest version from the AMX website. Both [MAC](#) and [PC](#) versions are available. The steps below will show how to configure a single SVSI device. There are several methods for batch configuring multiple devices, please consult the help documentation in the N-Able application as well as the documentation available on <https://www.amx.com/> for further information.

To configure SVSI encoders and decoders you will need to connect the SVSI devices and your computer to the same network. SVSI encoders and decoders will need to be powered by either external 12V DC power or POE on port P0. Port P1 does not support POE.

After launching the N-Able software all encoders and decoders should be automatically discovered and displayed in the list shown under the Unit Management tab. If the SVI units are not automatically discovered the Discover by IP button allows for a specific address range to be used for the discovery process.



The screenshot shows the AMX N-Able software interface. The 'UNIT MANAGEMENT' tab is selected. The interface includes a menu bar (N-Able, Tools, Documents, Help), a toolbar with buttons for 'Auto Discover', 'Discover by IP', 'Remove ALL Units', 'Remove Unit', and 'Edit'. A status bar indicates 'You have 1 ENC, 1 DEC, 0 ATR, 0 NVR, 0 WP, 0 N-Touch.' Below the toolbar is a search bar and a 'Clear' button. The main area contains a table with the following data:

	Name	Type	MAC	IP	SN	Streams	Mode	Resolution	Audio
1	00:19:0B:89:16:C2	N3000 Decoder	00:19:0B:89:16:C2	172.16.1.200	N3232A20015720	30739	Live Play	720p60	On (Fo...
2	00:19:0B:85:55:E8	Room Switcher	00:19:0B:85:55:E8	192.168.1.78	N7142-15400000805				
3	00:19:0B:89:16:FB	N3000 Encoder	00:19:0B:89:16:FB	169.254.250.240	N3132A20015777	488	Live Play	720p60	On

Double clicking on any line will initiate a connection to the device. The most likely reason for an unsuccessful connection attempt is for the SVSI device to have an IP address outside the subnet configured for your network adapter.

SchoolView

Upon successfully connecting to a SVSI device the Settings page as shown below will open.

Decoders must use a static IP address. Encoders are not controlled by the masters and all network settings may be configured as needed.

For decoders set IP Mode: STATIC and fill in all information in the Network Setup section (shown in the red rectangle below).

The screenshot shows the settings interface for an N-Series 3232 Decoder. The 'Network Setup' section is highlighted with a red rectangle. It contains the following fields and values:

Field	Value
IP Mode	STATIC
IP address	172.16.1.200
Netmask	255.255.254.0
Gateway address	172.16.0.1
Manual DNS	<input type="checkbox"/> Enable
DNS #1	192.168.20.5
DNS #2	192.168.20.6
Ping Test	172.16.0.1

Below the Network Setup section, there is a 'Trial Save' button. The 'Status' section shows HDMI Status as disconnected, Source Resolution as 1920x1080, and three source IP addresses (Port 50001, Port 50002, and Serial Source IP) all as disconnected, each with a 'Flush' button. At the bottom, there is a 'Change Password' section with a 'Change Password' button.

After entering all of the settings select the Trial Save button. The dialog box below will be shown.

The dialog box is titled "JavaScript Alert - 172.16.1.220". The text inside the dialog box reads:

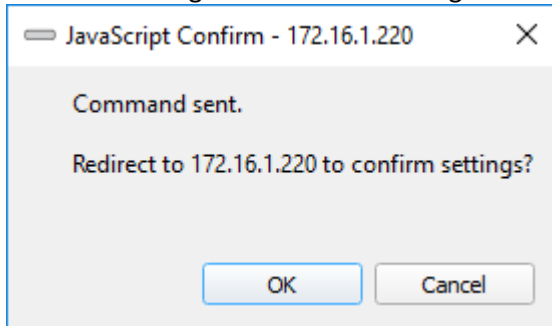
Settings will be in trial until confirmed.
If there is a problem, reboot board to reset IP.

There is an "OK" button at the bottom right of the dialog box.

Select OK to confirm the trial save.

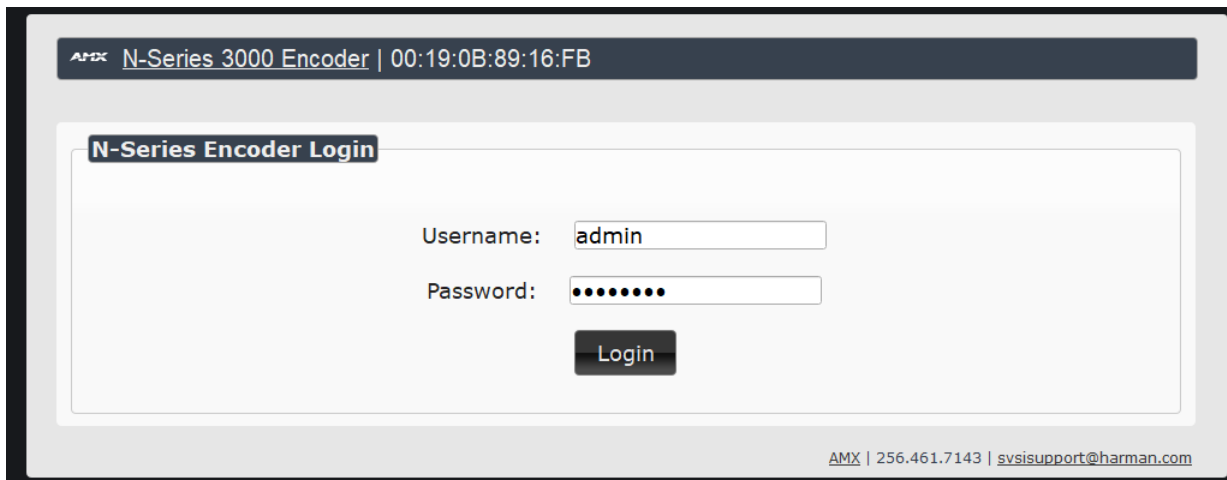
SchoolView

After confirming a trial save the dialog box shown below will be displayed.



Select OK to reconnect to the unit.

Upon reconnecting to the unit a username and password may be required. The default username is "admin" and the default password is "password".



After entering the username and password select the Login button.


A successful connection to the device with the network settings in trial save will confirm the network settings.

SchoolView

After confirming the network settings the Decoder/Encoder settings should be configured. Decoders should be able to use the default settings in most cases but Scaler and Output Mode can be adjusted if necessary.

The screenshot displays the web interface for an AMX N-Series 3232 Decoder. The page title is "N-Series 3232 Decoder | 00:19:0B:89:16:C2". The navigation menu includes Settings, LocalPlay, IR, N-Act, Serial, Security, Overlay, EDID, Logs, LLDP, and NetLinX.

Decoder Setup

Device Name: 00:19:0B:89:16:C2
Stream: 30739
Preview: 
Unicast Mode: Enable
Audio Stream: 0
Audio Follows Video: Follows
Scaler: Auto
Output Mode: auto
Live/Local: Live
Audio Mute: Mute
Lineout Volume: Set Left/Right
Enable HDMI Audio: Auto

Network Setup

IP Mode: STATIC (STATIC dropdown)
IP address: 172.16.1.200 (172.16.1.200 input)
Netmask: 255.255.254.0 (255.255.254.0 input)
Gateway address: 172.16.0.1 (172.16.0.1 input)
Manual DNS: Enable
DNS #1: 192.168.20.5 (8.8.8.8 input)
DNS #2: 192.168.20.6 (8.8.4.4 input)
Ping Test: 172.16.0.1 (input)

Status

HDMI Status: disconnected
Source Resolution: 1920x1080
Status:
Port 50001 Source IP: Disconnected
Port 50002 Source IP: Disconnected
Serial Source IP: Disconnected

Change Password

[Change Password](#)

Stream Settings

Stream Source: SVSI encoder
Stream URL:
Support B-Frames: Enable
Multicast Address Override: Enable
Multicast Address: 239.255.0.0

Software

Serial: N3232A20015720
MAC address: 00:19:0B:89:16:C2
Firmware Version: v2.12.11 (5/7/2018)
Web Version: 5/7/2018

SchoolView

Encoder setup is similar to decoder setup except the following stream setting options must be configured.

- Encoder Output Mode: SVSI decoder
- Transport Stream – Select Enable
- Generate Multicast Stream – Select Always
- Multicast Address Override – Select Enable
- Multicast Address – Enter the multicast address as defined in the Schoolview configuration for the corresponding channel/stream.
- UDP Port Number – Enter the port number as defined in the Schoolview configuration for the corresponding channel/stream.

Stream Settings

Encoder Output Mode	SVSI decoder ▾
Transport Stream	<input checked="" type="checkbox"/> Enable
Generate Multicast Stream	<input checked="" type="checkbox"/> Always
RTP Encapsulation	<input type="checkbox"/> Enable
HTTP File Duration (sec):	10 ▾
RTMP URL:	rtmp: <input type="text"/>
RTMP Stream:	none <input type="text"/>
PCM audio	<input type="checkbox"/> Enable
I-Frame Frequency	90 ▾
Multicast Address Override	<input checked="" type="checkbox"/> Enable
Multicast Address	<input type="text" value="239.255.37.251"/>
UDP Port Number	<input type="text" value="18888"/>
RTSP Port Number	<input type="text" value="8554"/>
RTCP Port Number	<input type="text" value="50011"/>

When finished entering all values select Save.

For encoders the video stream may be previewed using VLC media player. Open VLC media player and select Media -> Open Network Stream. In the dialog box copy paste the Stream URL shown in the top right of the Encoder Setup page.

SchoolView

For decoders it is required to enter Netlinx connection settings. Netlinx connection does not need to be enabled for encoders. When selecting the Netlinx tab the screen below will be shown.

The screenshot shows the 'Netlinx Setup' configuration page. At the top, there is a header bar with the AMX logo, the device name 'N-Series 3232 Decoder', and the MAC address '00:19:0B:89:16:C2'. Below the header is a navigation menu with tabs for Settings, LocalPlay, IR, N-Act, Serial, Security, Overlay, EDID, Logs, LLDP, and NetLinx. The 'Netlinx Setup' section contains the following fields: 'Enable' (checked), 'Device Status' (Unknown), 'Master Mode' (URL), 'IP/URL' (172.16.1.6), 'Port' (1319), 'Device Number' (1102), 'System Number' (0), 'Username' (empty), and 'Password' (empty). A 'Save' button is located at the bottom of the form. At the bottom right of the page, there is a footer with the text 'AMX | 256.461.7143 | svsupport@harman.com'.

- Enable – Select
- Master Mode: URL
- IP/URL – Enter the IP address of the classroom master.
- Port – Leave at the default value of 1319
- Device number: 1001 – 1999. Must match device number assigned in the configuration of the Schoolview system. Recommended convention is to use a 1 followed by the last octet of the IP address padded to three places. For the example above with an IP address ending in .6 the device number would be 1006. Audio extract devices should use a device number outside of this range, the standard convention is to use 4999 for audio extract.
- After entering all of the Netlinx settings select Save.

SchoolView

Spinetix HMP-350 Players

This section will explain how to configure the Spinetix HMP-350 as the emergency alerts player.

The [Spinetix HMP-350](#) uses the [Elementi](#) software for configuration and uploading of project files. A free trial is available if you do not have a license.

If you need information about the installation or setup of the HMP-350 or elementi software please visit the [Spinetix information](#) page. The Elementi quick guide and HMP-350 Getting started guide will be referenced in the following instructions.

Classroom Touch Panel Configuration

See the touch panel configuration section, the process is identical for configuring admin and classroom touch panels.

Classroom Keypad (MET-7E) Configuration

To configure the keypad, you must have it powered by PoE.

Locating the IP Address of the Keypad

Metreau Keypads with Ethernet are configured for DHCP addressing by default. The keypads use link local addressing as a backup in case the DHCP server is inaccessible. See the ***toggling Between IP Addressing Modes: DHCP and Static IP*** section for information on setting a static IP address. Verify there is an active LAN connection between your computer and the keypad you wish to configure before beginning the procedure below.

Modifying Keypad Connection and IP Settings

1. Establish a telnet connection with the keypad using either the DHCP address or by toggling the keypad to static IP mode.
 - a. Upon successfully connecting to the keypad it should respond with the message “Welcome to MET-7E v1.2.14 Copyright AMX LLC”
 - b. If you need to confirm which keypad you are connected to there are two options:
 - i. To see the MAC address of the keypad issue the command “get ip”. One of the values returned will be the MAC address.
 - ii. To see the serial number of the keypad issue the command “get sn”. The keypad will respond with the serial number.
2. Issue the command “set connection”. This command will set several properties in an interactive manner.
 - a. The first parameter to set is the mode. Type “t” (for TCP/URL mode) and press enter.
 - b. The second parameter to set is the master IP. Enter the IP address of the correct room master ex. “192.168.1.10” and press enter.
 - c. The third parameter is the master port and it should already be set to 1319, press enter to keep the default master port.
 - d. The fourth parameter is the master user and by default will be blank. Press enter to keep the default.
 - e. The fifth parameter is the master password and by default will be blank. Press enter to keep the default.

SchoolView

- f. The sixth parameter is a confirmation of the master password. Press enter to keep the default.
 - g. At the end you should see a summary of the information you have entered. If the mode is set to "TCP/URL" and the master IP is the correct room master type "Y" to confirm the changes. The keypad should respond with "Settings Written" to confirm success.
3. Issue the command "set device xxxx"
 - a. Replace the xxxx in the above command with the desired device number, ex. "6005". Note that while valid device numbers are between 0 to 31999 for Schoolview keypads must use device numbers between 6001 and 6999. The standard convention is to use the last octet of the device IP address padded with zeros as necessary to three digits and prefix with a 6 to create the 6xxx device number. Example 1: Keypad has IP address 192.168.1.20, device number will be 6020. Example 2: Keypad has IP address 192.168.1.121, device number will be 6121.
 - b. The keypad should respond with "The new device number is: xxxx".
 4. Issue the command "set ip". This command will set several properties in an interactive manner.
 - a. The first parameter is the host name. Either enter your desired host name or press enter to keep the default. Ex. "MET-7E-RM-101"
 - b. The second parameter is the mode. Type "S" for static IP and press enter.
 - c. The third parameter is the IP address. Enter the desired IP address. Ex. "192.168.3.120"
 - d. The fourth parameter is the subnet mask. If the subnet mask displayed is correct press enter otherwise enter the desired subnet mask. Ex. "255.255.252.0"
 - e. The fifth parameter is the gateway address. Enter the correct gateway address, ex. "192.168.1.1" and press enter.
 - f. At the end you should see a summary of the information you have entered. If all of the information is correct enter "Y" to save your changes.
 5. Issue the command "reboot" to reboot the keypad and have all of the settings changes take effect.

Simulating the ID Pushbutton

You can press buttons 1 and 2 (on the MET-7E this is the top two buttons) simultaneously on the keypad to simulate the functions of a NetLinx device's ID pushbutton.

Toggling Between IP Addressing Modes: DHCP and Static IP

Metreau Keypads with Ethernet support both DHCP and static IP addresses. You can use a static IP address which you can set via a Telnet command (SET IP), or you can use the factory default static IP address (192.168.1.2). With the keypad powered and booted up (or in ID Mode), you can toggle between the DHCP and Static IP modes by pressing and holding buttons 1 and 2. The LEDs on buttons 1 and 2 blink while you keep them pressed. Hold them until the LEDs begin blinking at double the rate (approximately 10 seconds), then release the buttons. When you release the buttons, the keypad toggles either from static to dynamic (DHCP) IP addressing or vice versa and remains in that mode until you use the buttons to toggle the IP mode again or you perform a factory reset. The keypad automatically reboots to complete the process.

NOTE: You must wait until the keypad is finished booting before toggling the IP address. Pressing the buttons while booting will cause the keypad to restore its factory default settings.

SchoolView

GL-300 Configuration

The amplifier does not require any special configuration. If you encounter control issues with a GL-300 follow the troubleshooting steps below.

- Check the serial cable between the Barix and GL-300
- Reboot the GL-300 and Barix
- Try moving the serial cable connection to the other GL-300 serial port and rebooting both the Barix and GL-300.
 - Note: For older sites any GL-300 amplifier with firmware older than 2018-04-27_2100 should be updated to the latest the latest available firmware from the [Audio Enhancement](#) website.

RF Receiver Configuration

The RF receiver does not require any configuration. It must be connected to the GL-300 amplifier using a category cable. If implementing SAFE the serial port of the receiver should be connected to the serial port of the SAFE Barix.

SchoolView

Display Driver Creation

Overview

This section is a guide intended for use by integrators who are installing or modifying a Schoolview 9.1.x system and need to create or modify a display driver. The AMX Design Suite / Driver Design software, available from the AMX website, is required. The Driver Design Instruction manual, available as a PDF download, is also helpful and this guide will reference the product manual.

Acquiring XDD Driver Files

XDD driver files can be downloaded from AMX.com website. Only logged in users can download driver files. From the main page of the AMX website go to Support -> Downloads -> Search Device Modules to begin your search. Fill in as much information as possible. Both IP and serial drivers may be used with Schoolview, IR display drivers are not supported.

From the list of search results download the appropriate DD (Driver Design) driver file. Duet Module (DM) drivers are not compatible with Schoolview. If a DD driver is not available for the exact model you are searching for it is likely the DD file from a similar model by the same manufacturer can be used. If no driver design file is found using the Device Database it is possible to create a driver file using communication protocol information provided by the manufacturer.

Importing XDD Driver Files

Once an XDD file is downloaded it must be imported into a project. To import an XDD file select File -> Import..., you should see the import window shown in Figure 1.

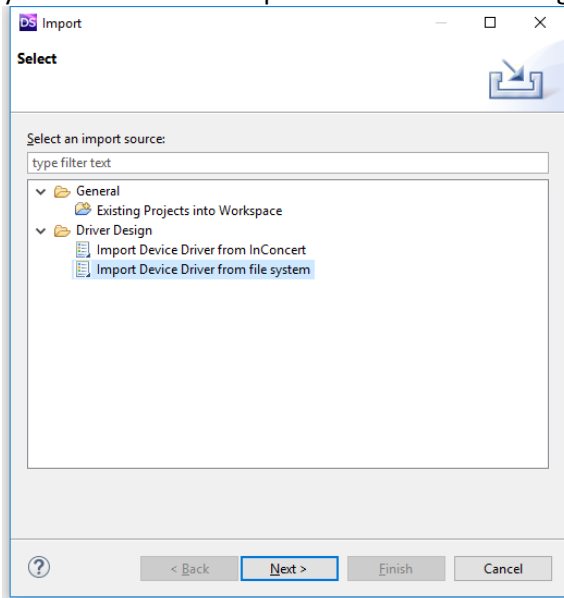


Figure 1

Select Import Device Driver from file system and Next.

SchoolView

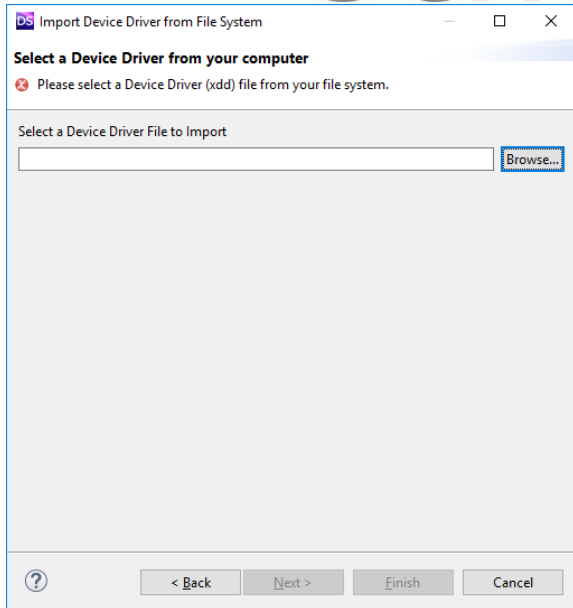


Figure 2

Use the Browse button to choose an XDD file then select Next.

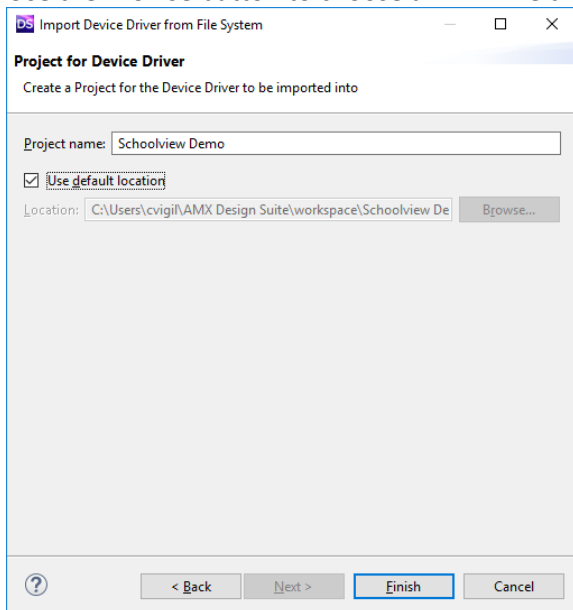


Figure 3

Enter a project name and select Finish.

The project should now be available in the project explorer window.

XDD Modifications for Schoolview

Before modifying a driver file you will need to know which display inputs will be used. If the driver file will be used with a keypad the order in which the inputs will cycle will also need to be known. If a touch panel will be present than the cycle order will not matter but as a rule it is best to follow the same convention as with a keypad file. Typically the order is classroom inputs than classroom video. In the example shown in this guide HDMI 1 and HDMI 2 are local inputs and HDMI 3 is the Enzo/Campus Video input.

Open the project file and select the Control tab.

Next expand the Input Source section (1) as shown in Figure 4 and open the Edit Input Sources window (2).

SchoolView

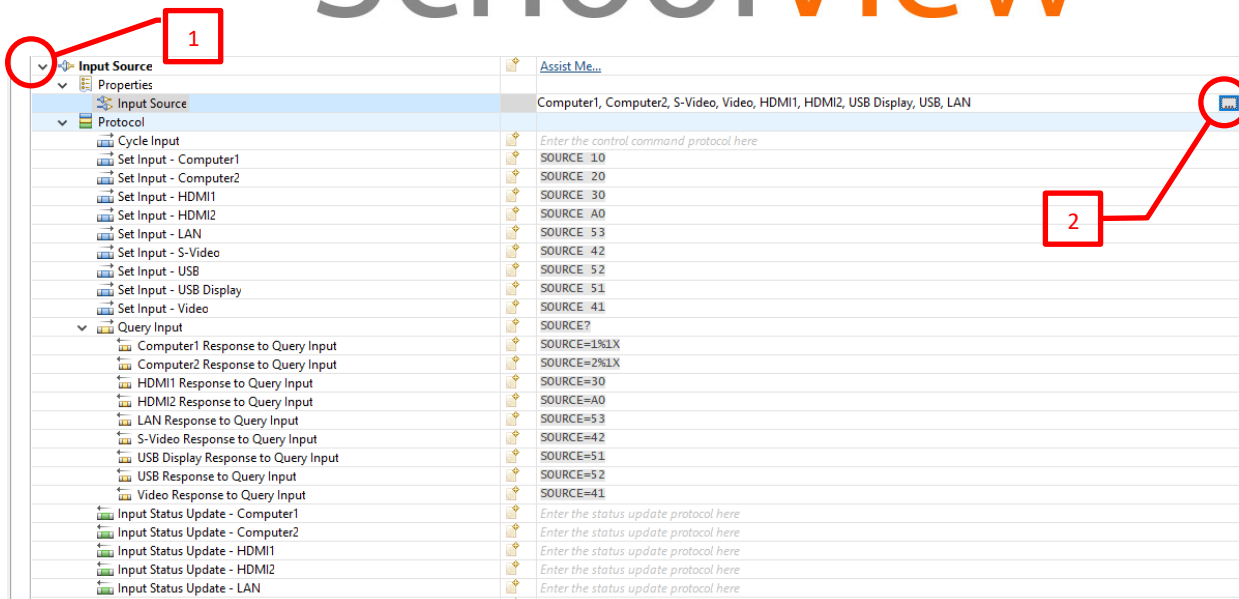


Figure 4

Removing Unused Input Sources

The first step is to remove any input sources that will not be used. Select the line and use the Delete button to remove all sources not needed for the room type the driver will be used with.

In our example we only need HDMI 1, HDMI 2, and HDMI 3. Since HDMI 3 is not present in the list we will add it after removing the unnecessary input commands.

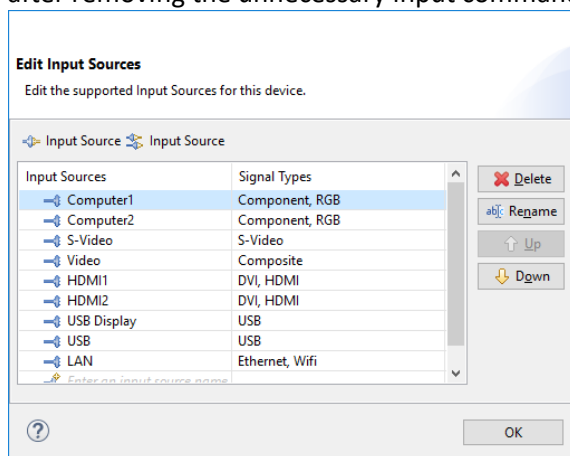


Figure 5

After removing the unneeded input commands the sources window should look similar to Figure 6.

SchoolView

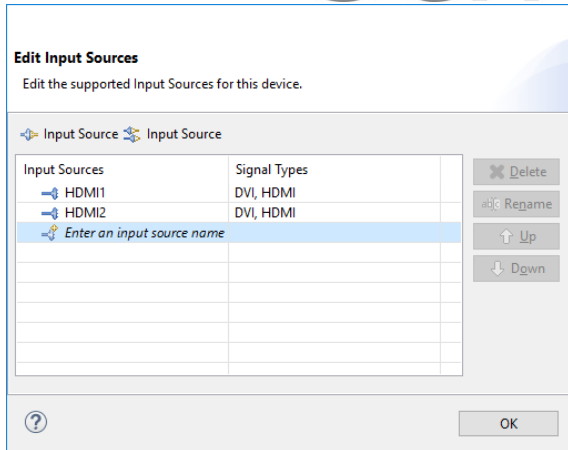


Figure 6

Adding an Input Source

A name and signal type for the new source (HDMI 3) will need to be entered. It is important that each source only have one signal type for Schoolview compatibility. After adding the new source the existing sources will be edited to have only one signal type.

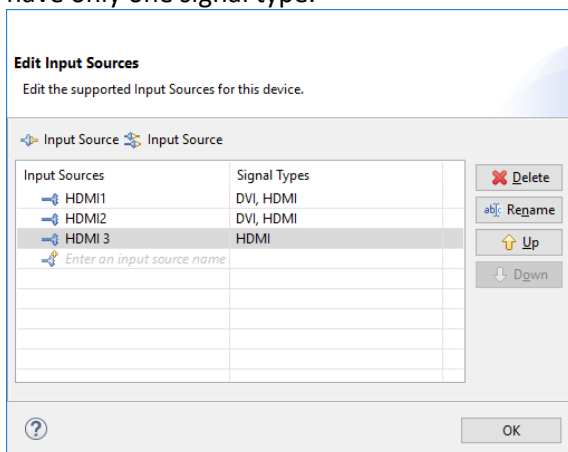


Figure 7

Editing Signal Types

The new source has been added. Now the existing sources will be edited to remove the DVI signal type and leave them with only one signal type, in this case the HDMI signal type will be the one remaining.

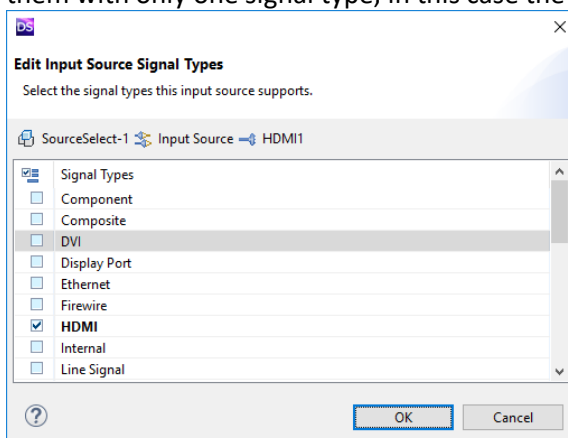


Figure 8

SchoolView

The DVI signal type has been unchecked for the selected source. Edit each source so that there is only one signal type associated with each input.

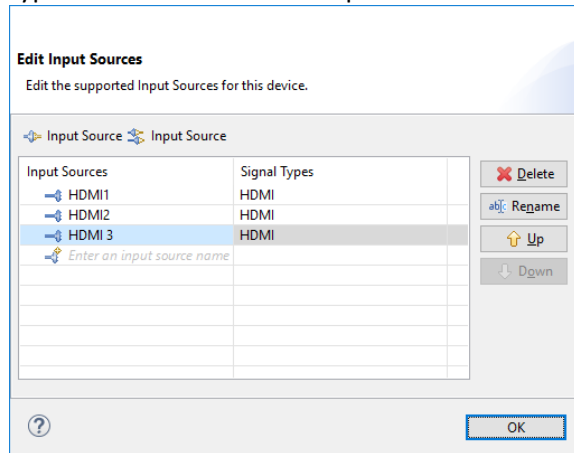


Figure 9

Ordering Input Sources

Once all unnecessary sources have been removed and all remaining sources have only one signal type assigned use the Up and Down buttons to arrange the sources in the desired order. If the site only has touch panels this order is not important but it is best practice to put the Enzo/Campus Video input last.

Once all sources have the correct order and only one signal type is assigned to each, select OK to close the window. This is also a good time to save the project.

Adding Source Commands

Because we added a source that was not in the list it is necessary to enter the Set and Response to Query commands. If you did not add any input types you can skip the section below and go to the section on exporting your driver to a XDD file.

Entering Source Commands

Input Source	Assist Me...
Properties	
Input Source	HDMI1, HDMI2, HDMI 3
Protocol	
Cycle Input	Enter the control command protocol here
Set Input - HDMI 3	Enter the control command protocol here
Set Input - HDMI1	SOURCE 30
Set Input - HDMI2	SOURCE A0
Query Input	SOURCE?
HDMI 3 Response to Query Input	Enter the response protocol here
HDMI1 Response to Query Input	SOURCE=30
HDMI2 Response to Query Input	SOURCE=A0
Input Status Update - HDMI 3	Enter the status update protocol here
Input Status Update - HDMI1	Enter the status update protocol here
Input Status Update - HDMI2	Enter the status update protocol here

Figure 10

Fill in the Set and Response to Query Input commands. Please refer to the documentation included with the display to determine the proper strings to enter. When selecting the Set Input command buttons appear on the far right of the line for HEX and ASCII data. You will need to refer to the manufacturer's product information to determine the correct string to enter.

When selecting the Response to Query Input field there are three options that appear to the right. HEX, ASCII and REGEX (Regular Expression). In cases where the display response to an input query requires string processing to be interpreted a REGEX can be used. How to write a REGEX is out of the scope of this document and further information can be found in the Driver Design manual.

SchoolView

Creating a Driver File

When creating a driver instead of modifying an existing one the following list of items will provide a guide for the required functionality. For commands which have toggle and discreet options it is always best to use the discrete commands if available.

- Freeze Commands – Optional but recommended if supported by display
 - Enter Cycle or Set commands
 - Enter Query command
 - Enter Response to Query strings or REGEX
- Picture Mute – Optional but recommended if supported by display
 - Enter Cycle or Set commands
 - Enter Query command
 - Enter Response to Query strings or REGEX
- Lamp History – Optional but recommended – Will allow lamp time to be displayed on the admin touch panel(s)
 - Enter Query command
 - Enter Response command (Reference the Driver Design manual for more information on REGEX and PARAM options for this field)
- Device and lamp power state – Power state query must be supported for the display to function properly with Schoolview
 - Cooling and Warming times are entered into the Schoolview config tool. The values contained in the driver file are not used.
 - Power Set commands – Must be entered for proper functionality
 - Power Query and Responses – Must be entered for proper functionality
- Input Source – Input sources must be correctly defined for proper functionality
 - Enter only the input sources that will be used
 - Configure each input source for only ONE signal type
 - Enter set commands for each input source
 - Enter Query and Response commands for each input source

Modifying Driver Files to Remove Command/Response Footer

This section is for those that need to create a driver file for a protocol that does not use a footer (terminating character string at the end of each command/response to/from the display). If you are not creating a custom driver and having issues with needing to remove a command/response footer than you can skip this section.

Steps to remove footer information from a driver file.

1. Create or modify a driver using Design Suite
 - a. With Design Suite version 1.2.12 the footer for sending commands is optional and you can simply uncheck the footer option in the Transport Configuration window. If you have an XDD file created with an earlier version of DS you can either use the latest version of DS to remove the command footer or follow the steps below to manually remove the command footer.
 - b. The footer for Response Format is not optional and you must enter a footer to proceed when creating a driver. Enter any value for the footer so you can finish creating your custom driver. The following steps will remove this footer.
2. Finish creating your custom driver and export it to create an XDD file.
 - a. The Export step is explained in more detail in the following section of this document.
3. Change the file extension on the XDD file from .xdd to .zip.

SchoolView

4. Open the .zip archive and extract the driver.xml file.
5. Open the driver.xml file with any text editor. The screenshots below are from Notepad++.
6. Remove the unnecessary characters from the end of the <MsgFormat value= lines.
 - a. In Figure 11 the lines that will be edited are 50, 57, 69 and 76.
 - i. Line 50 is the IP transmit string, \x0D\x0A will be removed.
 - ii. Line 57 is the IP receive string, \x0D\x0A will be removed.
 - iii. Line 69 is the RS-232 transmit string, \xCF will be removed.
 - iv. Line 76 is the RS-232 receive string, \xCF will be removed.
 - b. Figure 12 shows the driver file with the edits applied.
7. Save your changes to driver.xml.
8. Insert the driver.xml file back into the zip archive.
9. Change the file extension from .zip back to .xdd.
10. It is possible to open the modified driver in Design Suite and make changes to any section except the Transport Configuration settings. If you change the Transport Configuration settings in Design Suite it will be necessary to redo the footer customization.

```
46 <Provisioning>
47 <Ip ip-address="0.0.0.0" port="3073">
48 <Transport manufacturer="*Custom">
49 <Transmit minMsgInterval="100">
50 <MsgFormat value="\x02\x03\x30%s\x0D\x0A">
51 <Segment type="Header" value="02 03 30" editorPattern="HH HH HH" />
52 <Segment type="Message" value="%s" />
53 <Segment type="Footer" value="0D 0A" editorPattern="HH HH" />
54 </MsgFormat>
55 </Transmit>
56 <Receive onlineTimeout="60">
57 <MsgFormat value="\x02\x03\x31(.+?)\x0D\x0A">
58 <Segment type="Header" value="02 03 31" editorPattern="HH HH HH" />
59 <Segment type="Message" value="(.+)" />
60 <Segment type="Footer" value="0D 0A" editorPattern="HH HH" />
61 </MsgFormat>
62 </Receive>
63 <Info>User Customizable Transport.</Info>
64 </Transport>
65 </Ip>
66 <Serial phy-layer="RS-232" baudrate="19200" databits="8" stopbits="1" parity="None" flowcontrol="None">
67 <Transport manufacturer="*Custom">
68 <Transmit minMsgInterval="100">
69 <MsgFormat value="\x7F\x08\x99\xA2\xB3\xC4\x02\xFF%s\xCF">
70 <Segment type="Header" value="7F 08 99 A2 B3 C4 02 FF" editorPattern="HH HH HH HH HH HH HH HH" />
71 <Segment type="Message" value="%s" />
72 <Segment type="Footer" value="CF" editorPattern="HH" />
73 </MsgFormat>
74 </Transmit>
75 <Receive onlineTimeout="120">
76 <MsgFormat value="\x7F\x09\x99\xA2\xB3\xC4\x02\xFF(.+?)\xCF">
77 <Segment type="Header" value="7F 09 99 A2 B3 C4 02 FF" editorPattern="HH HH HH HH HH HH HH HH" />
78 <Segment type="Message" value="(.+)" />
79 <Segment type="Footer" value="CF" editorPattern="HH" />
80 </MsgFormat>
81 </Receive>
```

Figure 11

SchoolView

```
46 <Provisioning>
47   <Ip ip-address="0.0.0.0" port="3073">
48     <Transport manufacturer="+Custom">
49       <Transmit minMsgInterval="100">
50         <MsgFormat value="\x02\x03\x30%s">
51           <Segment type="Header" value="02 03 30" editorPattern="HH HH HH" />
52           <Segment type="Message" value="%s" />
53           <Segment type="Footer" value="0D 0A" editorPattern="HH HH" />
54         </MsgFormat>
55       </Transmit>
56       <Receive onlineTimeout="60">
57         <MsgFormat value="\x02\x03\x31(.+?)">
58           <Segment type="Header" value="02 03 31" editorPattern="HH HH HH" />
59           <Segment type="Message" value="(.+?)" />
60           <Segment type="Footer" value="0D 0A" editorPattern="HH HH" />
61         </MsgFormat>
62       </Receive>
63       <Info>User Customizable Transport.</Info>
64     </Transport>
65   </Ip>
66   <Serial phy-layer="RS-232" baudrate="19200" databits="8" stopbits="1" parity="None" flowcontrol="None">
67     <Transport manufacturer="+Custom">
68       <Transmit minMsgInterval="100">
69         <MsgFormat value="\x7F\x08\x99\xA2\xB3\xC4\x02\xFF%s">
70           <Segment type="Header" value="7F 08 99 A2 B3 C4 02 FF" editorPattern="HH HH HH HH HH HH HH HH" />
71           <Segment type="Message" value="%s" />
72           <Segment type="Footer" value="CF" editorPattern="HH" />
73         </MsgFormat>
74       </Transmit>
75       <Receive onlineTimeout="120">
76         <MsgFormat value="\x7F\x09\x99\xA2\xB3\xC4\x02\xFF(.+?)">
77           <Segment type="Header" value="7F 09 99 A2 B3 C4 02 FF" editorPattern="HH HH HH HH HH HH HH HH" />
78           <Segment type="Message" value="(.+?)" />
79           <Segment type="Footer" value="CF" editorPattern="HH" />
80         </MsgFormat>
81       </Receive>

```

Figure 12

Exporting an XDD file

After you have modified or created the driver project it must be exported to create the XDD file you will transfer to the primary master.

From the main window select File -> Export...

In the Export window select Export Device Driver and Next

SchoolView

Other Classroom Device Connections

This section will provide guidelines regarding the connection of other classroom hardware that requires either custom cable terminations or different cables depending on third-party devices.

Display Control

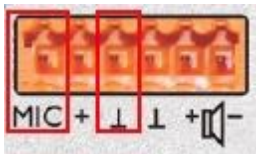
There are two possible display control scenarios in Unified Campus. Either a serial port or IP control of the display. The serial port can be either an Enzo or SVSI decoder. The Enzo uses a DB9 connector and the SVSI decoder uses a captive screw connector.

Classroom Audio

It is important to maintain the polarity of audio signals throughout the system. When connecting to the GL-300 captive screw terminals, be sure to connect external audio devices (e.g. audio decoder & classroom speakers) using the correct polarity. The cable required between the audio decoder and GL-300 LINE IN is described in the Tray Parts List and Pin-out section. Typically speakers are marked with positive (+) and negative (-) terminals, just like the GL300 AUDIO OUTPUTS terminals. If your speakers are not marked in this way, verify correct connection polarity with the manufacturer of the speakers.

Two Way Classroom Microphones

When using a typical dynamic intercom microphone with the audio decoder/encoder in a two-way classroom, be sure to only connect the necessary terminals on the audio decoder/encoder as indicated below. The necessary terminals of this connector are as follows: Pin 1 (mic audio) and pin 3 (signal ground). Pin 2 provides bias power, which is unused with a typical dynamic microphone.



Admin iPad Touch Panel Configuration (Optional)

- 1) Obtain the wireless network credentials from your IT Administrator.
- 2) Ensure the wireless network is configured for visibility to the Primary NetLinx master.
- 3) Connect your computer to the wireless network.
- 4) Connect your iPad to your computer using the supplied USB cable and follow the steps as prompted for registration and connection to iTunes
- 5) On your iPad, touch the Settings icon
- 6) Touch Wi-Fi
- 7) If Wi-Fi is OFF, touch the button to turn it ON
- 8) Under "Choose a Network..." you should see the SSID of your school's network.
- 9) Touch the network name. Enter the password and touch "Join".
- 10) You should now see a check mark next to the network name.
- 11) Click the button at the bottom of your iPad to return to the normal screen.
- 12) On your iPad, touch the App Store icon.
- 13) In the Search field, type TPControl. One word, no spaces.
- 14) Assuming steps 1-10 were successful, your iPad will find the TPControl app via the Internet.
- 15) Next to the TPControl App, touch FREE, then INSTALL
- 16) When download is complete, you'll have a DEMO version of TPControl. This is just the beginning and

SchoolView

prepares you to license your app and download the SchoolView file.

- 17) Click the button at the bottom of your iPad to return to the normal screen.
- 18) On your iPad, touch the Settings icon
- 19) Under the Apps section, touch TPControl
- 20) Touch Local Host and type the IP Address of your Primary NetLinx master (see the IP Map)
- 21) Touch Device ID and type 10002
- 22) Touch Button Hit and select OFF
- 23) Click the button at the bottom of your iPad to return to the normal screen.
- 24a) Launch TPControl App on iPad and touch screen once to pass startup screen
- 24) On your computer, browse to www.TPControl.com
- 25) Click Downloads at the top of the page (See Figure 1)
- 26) Scroll down to TPTransfer and click Download (See Figure 2)
- 27) When download is complete, locate and launch the file to install TPTransfer on your computer
- 28) In the new TPTransfer window on your computer, you should see your iPad listed. (See Figure 3).
- 29) In TPTransfer, in the line representing your iPad, click Get License.
- 30) On the next screen that appears, you should have option to Get Trial License (See Figure 4).
- 31) Follow the steps for the Trial License, including entry of your email address.
- 32) When your Trial License request is complete, you'll get a Token by email and should also be able to confirm that
on the www.TPControl.com page.
- 33) Enter that token on the TPTransfer window to activate a 21-day trial for your iPad. NOTE: You can purchase a license in similar fashion; just use a credit card then enter the new license key in TPTransfer.
- 34) Once your iPad is licensed (Trial or Permanent) for TPControl, we can upload the SchoolView Admin Panel file.
- 35) Save the attached TP4 file to your computer, in a location you will remember.
- 36) On the TPTransfer application, click Upload New
- 37) Browse to the TP4 file you just saved, click to select, and click Open (See Figure 5).
- 38) The file transfer (upload) should begin (See Figure 6).

NOTE: Figures 1-6 begin on next page.

SchoolView

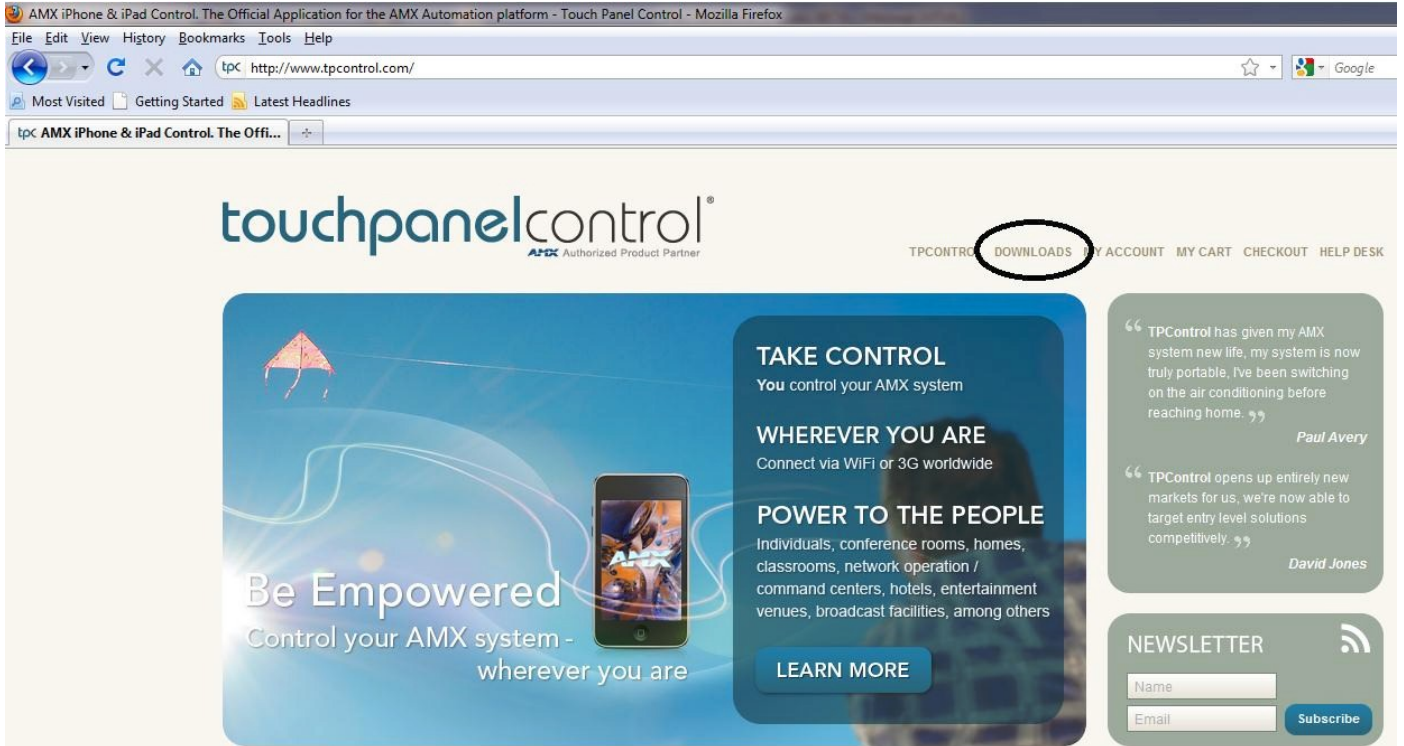
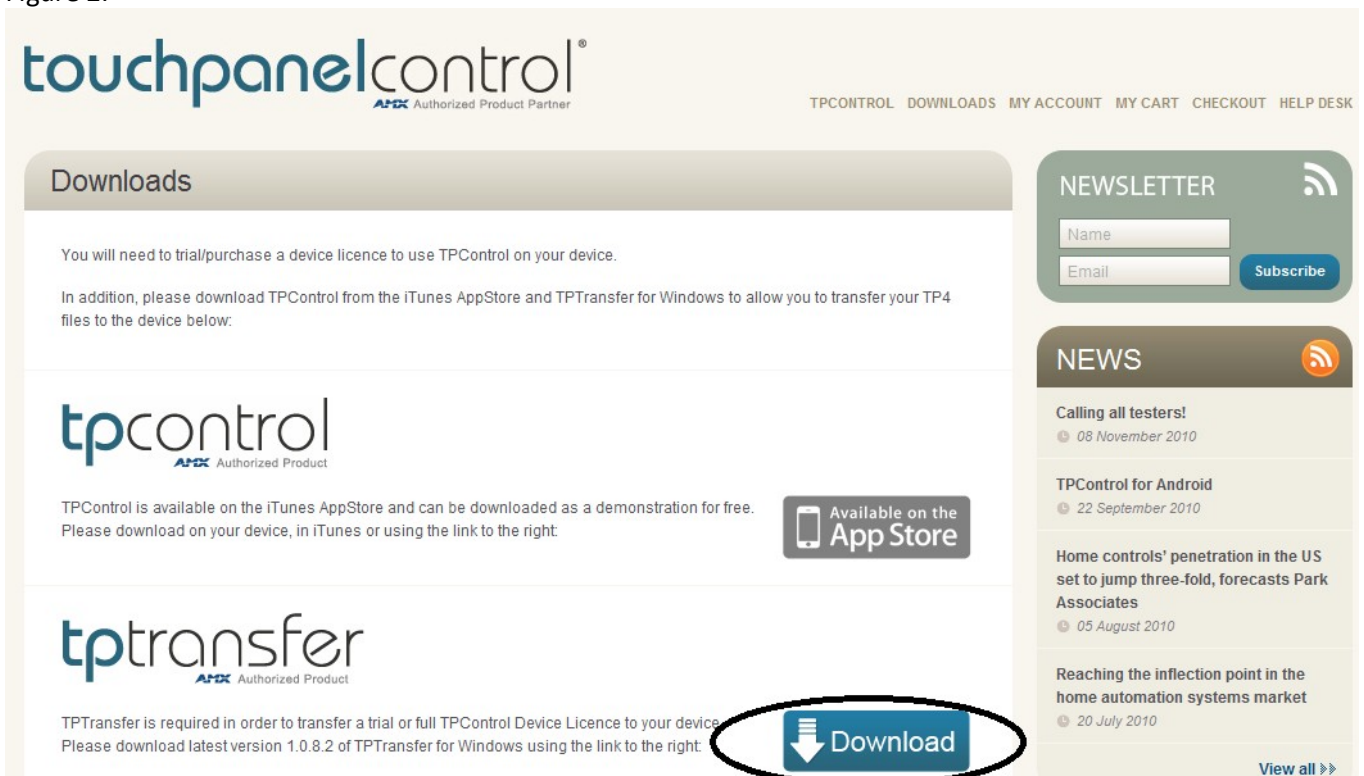


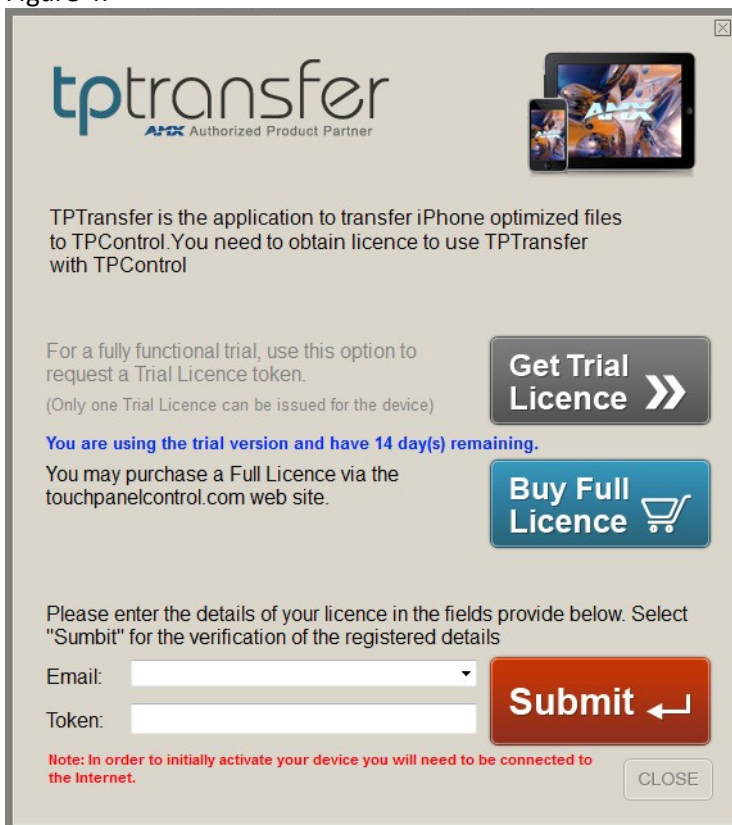
Figure 2:



SchoolView



Figure 4:



SchoolView

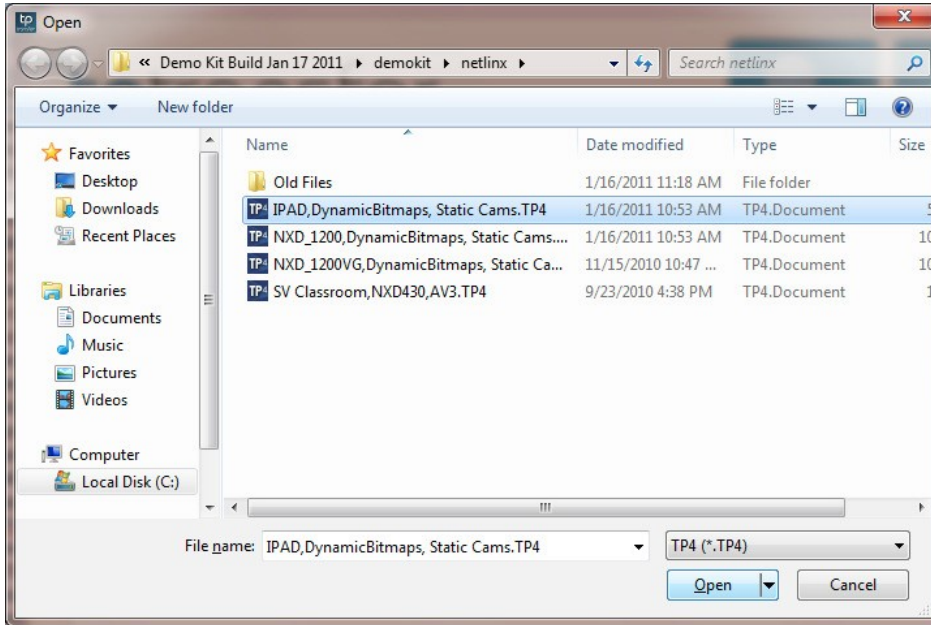


Figure 6:



SchoolView

Site Readiness Checklist

The checklist below was used when the Schoolview team loaded code onsite to insure the readiness of the location before traveling. Modern Schoolview systems are configured and setup by the integrators. This section is provided as a reference to assist the integrator with insuring all devices are online and ready. There is no need to send this form to the Schoolview team.

Site Name: _____

Date: _____

Dealer/Integrator: _____

The SchoolView software installation and/or training activities cannot occur until the site is "ready". Please confirm the following information pertaining to the readiness of the system for SchoolView software installation and training:

1. Data network is completely operational.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

2. All SchoolView assigned network ports, VLANs, subnets and IP addresses have been configured, and IGMP snooping/PIM routing has been configured correctly for multicast audio and video streams.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

3. All SchoolView assigned IP addresses and multicast video streams are accessible from common network ports, including those that will be utilized by teacher PCs.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

4. Audio rack is wired and tested, and all hardware is installed.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

5. Video rack is wired and tested, and all hardware is installed.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

6. SchoolView classroom systems are configured and installed, along with displays (if applicable) in all classrooms.

SchoolView

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

7. All speakers (classrooms, hallways, administration, outside, etc.) are installed and tested.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

8. All microphones (e.g. PA & Push to Talk) and monitor speaker in administration area are installed and tested.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

9. Video broadcast cart (if applicable) is complete and tested.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

10. Local sound systems, e.g., Gym, Cafeteria, Auditorium, etc. (if applicable) are complete and tested.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

11. All miscellaneous elements, such as doorbells, power relays, digital clocks, etc. are installed and tested.

Completed: _____ (Y/N) If not, anticipated date: _____ (mm/dd)

Comments: _____

BY SIGNING BELOW YOU CERTIFY THAT THE ABOVE INFORMATION IS CORRECT. IT IS FURTHER ACKNOWLEDGED THAT YOU WILL BE RESPONSIBLE FOR CHARGES FOR UNSCHEDULED ON SITE TIME INCURRED BY SCHOOLVIEW DUE TO AN INACCURATE OR INCOMPLETE RESPONSE TO THIS SITE READINESS CHECKLIST.

By: _____

Title: _____

Firm: _____

PLEASE EMAIL THIS FORM TO

SUPPORT@SCHOOLVIEWSOLUTIONS.COM

SchoolView

Commissioning Task List

The following tasks can be completed in conjunction with the Site Readiness Checklist. Positive results from these tasks will provide confidence to everyone that the system is truly ready for SchoolView software deployment.

1. Ping all devices to confirm the IP addresses are online. This can be accomplished easily in one step by utilizing any widely and freely available IP scanner tool, such as Angry IP Scanner.
2. Establish TELNET connections to NetLinx masters and confirm IP addresses and device type are correct.
3. Establish SSH connections to touch panels and video decoders (Enzo or SVSI) and confirm IP addresses and device type are correct.
4. Browse to all audio decoder/encoder IP addresses to confirm those are the expected type of device.
 - a. Another optional (and more definitive) test: While present in each classroom / zone, reboot the audio decoder and listen to make sure the assigned IP address is announced in that room.
 - b. The above test (a) is dependent on ALL of the following statements being TRUE:
 1. Sonic IP has not been disabled on the audio decoder (You may use headphones plugged directly into the audio decoder to verify).
 2. The line in and output levels of the GL-300 have not been reduced (default condition will allow audio to pass).
 - c. Once you have verified the above, if still no audio; check the wiring and connections.
5. Browse to all video encoders to confirm those are the expected type of device, and that they have the correct settings configured.
6. In the video rack, confirm all video sources appear on the preview monitor via the preview switcher.
7. Start the video encoder stream(s) and view in VLC player on your PC to ensure all streams are functional and the network is correctly configured.
8. With video streams present, confirm that the activity lights on the network switches are not rapidly and constantly flashing on ports that should not be receiving a stream (PCs, NetLinx, etc.).
 - a. If all port activity lights blink exactly the same, it may indicate that IGMP snooping is not correctly configured on the network switches.
 - b. If you can only view video streams when attached to the same switch as the encoders, but not in remote areas of the campus, it may indicate that PIM routing is not correctly configured.

SchoolView

SchoolView Software Deployment

The following sections will explain how to deploy SchoolView software to each device in the system. Network settings shown throughout are examples only, and should be replaced by the actual values assigned to be used on your particular project. There are many different software components in the SchoolView system, but if the following processes are followed exactly and in the order they are presented, software deployment can be very simple. Each individual software deployment process is also dependent on the affected hardware being online and properly configured, as described in the [SchoolView Hardware Configuration](#) section.

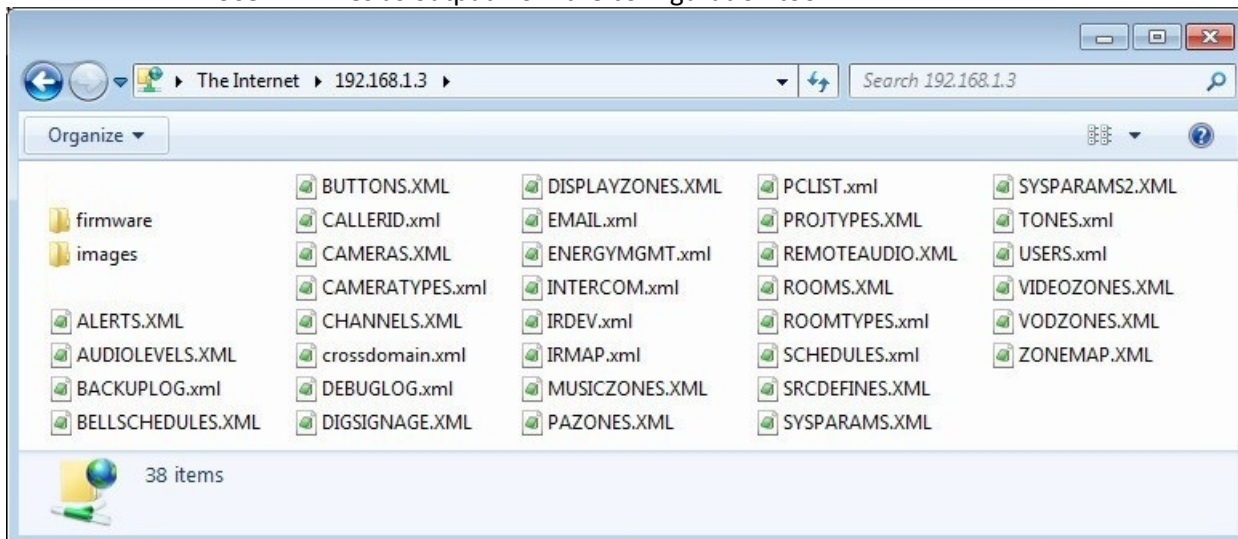
To deploy the SchoolView software to each device, follow these steps:

Loading Site Configuration Files

- 1) Obtain the site specific configuration files for your project from the output of the configuration tool.
 - a. The files referred to in the following sections are all part of this package.
 - b. The files listed below are the only ones you need to transfer to the primary master. It does not negatively affect the system to transfer XML files not in the following list that are created by the tool. If you make manual changes to the XML files only changes to the files in the following list will affect the system operation.
 - ALERTS.XML
 - AMXALERTS.XML
 - AUDIOLEVELS.XML
 - BELLSCHEDULES.XML
 - BUTTONS.XML
 - CAMERAS.XML
 - CAMERATYPES.XML
 - CHANNELS.XML
 - CUSTOM.XML
 - DIGSIGNAGE.XML
 - DISPLAYZONES.XML
 - EMAIL.XML
 - ENERGYMANAGEMENT.XML
 - GROUPZONES.XML
 - HVAC.XML
 - ICONS.XML
 - IRDEV.XML
 - IRMAP.XML
 - LIGHTING.XML
 - MUSICZONES.XML
 - PAZONES.XML
 - PCLIST.XML
 - PHONEEXTS.XML
 - PROJTYPES.XML
 - REMOTEAUDIO.XML
 - RESOURCES.XML
 - ROOMS.XML
 - ROOMTYPES.XML
 - SCHEDULES.XML
 - SRCDEFINES.XML
 - SYSPARAMS.XML

SchoolView

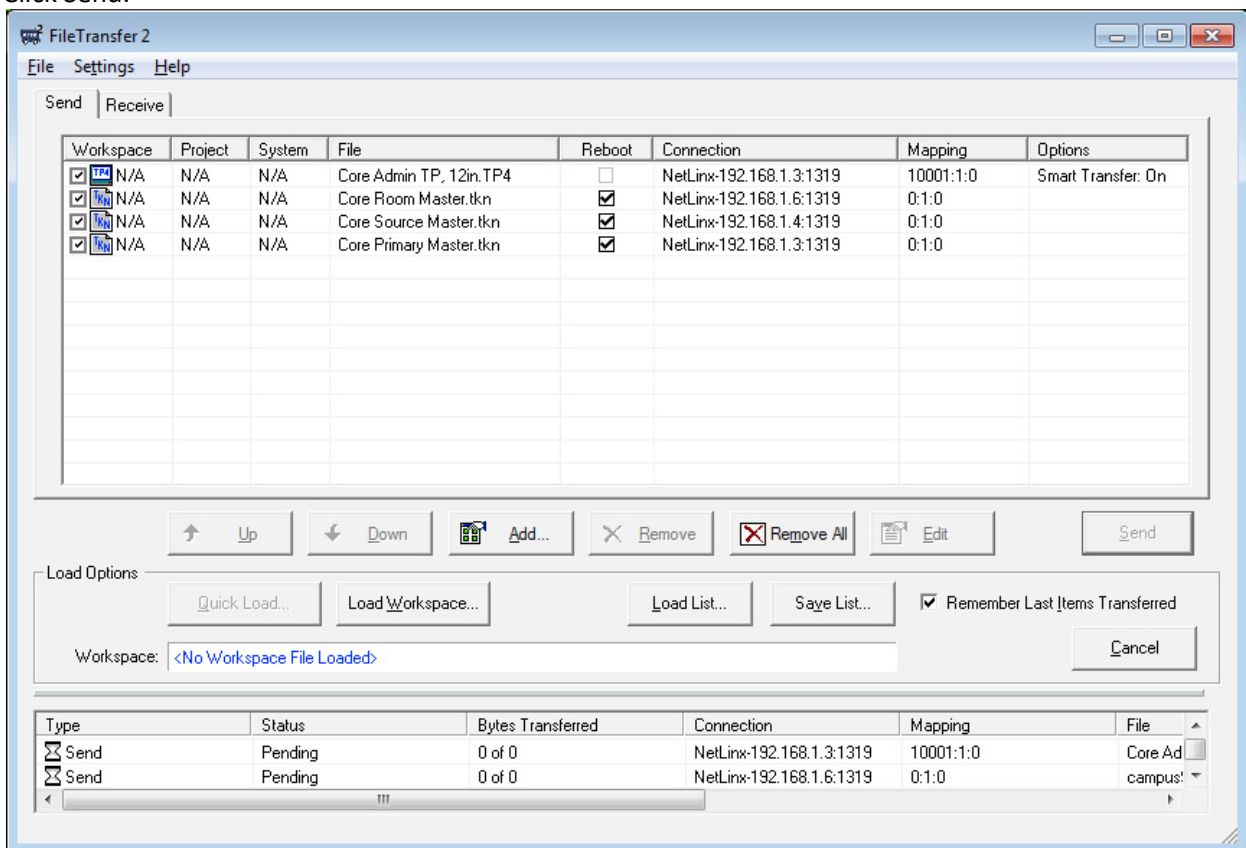
- SYSPARAMS2.XML
 - TONES.XML
 - USERS.XML
 - VIDEOZONES.XML
 - ZONEMAP.XML
- 2) Use an FTP client such as FileZilla (free, open source software available at <http://filezilla-project.org/>) or Windows Explorer to open an FTP connection to the primary NetLinx master (e.g., <ftp://192.168.1.3/>).
 - a. The credentials are: administrator/password.
 - b. If using a highly configurable client such as FileZilla, be sure to select BINARY transfer mode. Windows Explorer uses BINARY mode by default, while Windows' command line FTP uses ASCII mode by default.
 - 3) If there are any files on the primary master, delete them.
 - 4) Upload the necessary files provided by the configuration tool, Schoolview release, and driver design.
 - 5) The files should be organized on the primary master as shown below (and as delivered):
 - a. "firmware" folder.
 - i. Files used by the system to load the audio decoder/encoder firmware/software.
 - ii. Use firmware files found in the Schoolview release.
 - b. "images" folder.
 - i. PNG images used by the system to display the floor plan and logo.
 - ii. Use the images as output from the configuration tool.
 - c. All XML site configuration files.
 - i. Use XML files as output from the configuration tool.



SchoolView

Loading Admin Touch Panel File and NetLinx Software

- 1) Open AMX File Transfer tool inside NetLinx Studio.
- 2) Click Add.
- 3) On the Other tab, select the appropriate file type and click Add again.
- 4) Choose the correct file and click Open.
- 5) Define the appropriate Device, Port and System values for this file and click OK twice.
- 6) Choose the item you've just added, then click Edit -> Communication Settings.
- 7) Add or select the appropriate master communication settings and click OK.
- 8) Repeat steps 2) through 7) for each touch panel and NetLinx file.
- 9) Ensure all appropriate check-boxes on the left side of the window are selected.
- 10) If "Remember Last Items Transferred" is checked, you can still open this dialog later and re-send necessary files.
- 11) Alternatively (highly recommended), you can save out this list of files to re-load later.
- 12) Click Send.

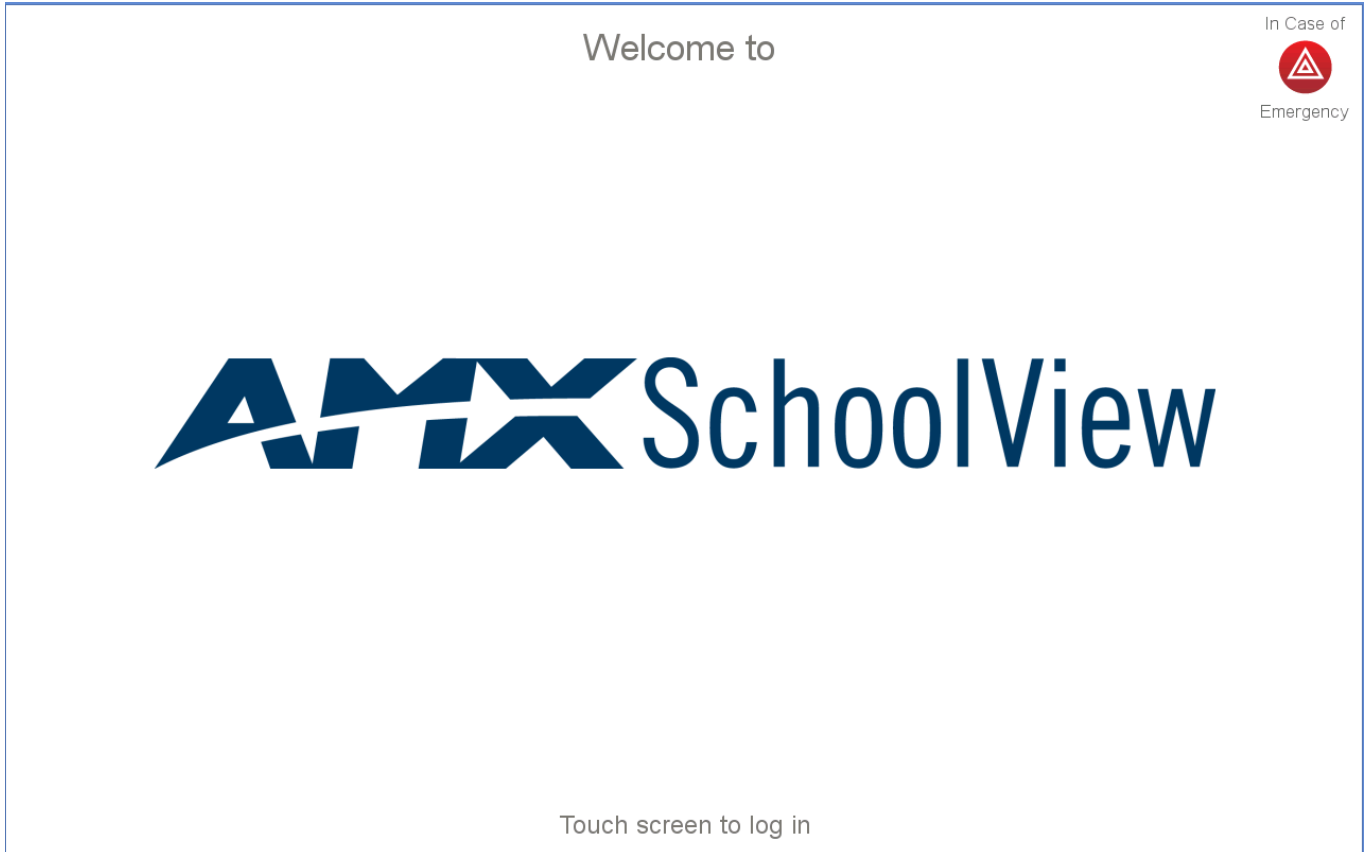


- 13) Examine the status window at the bottom to confirm all transfers completed.
- 14) If any of the transfers do fail, make note of them and retry as described above.

SchoolView

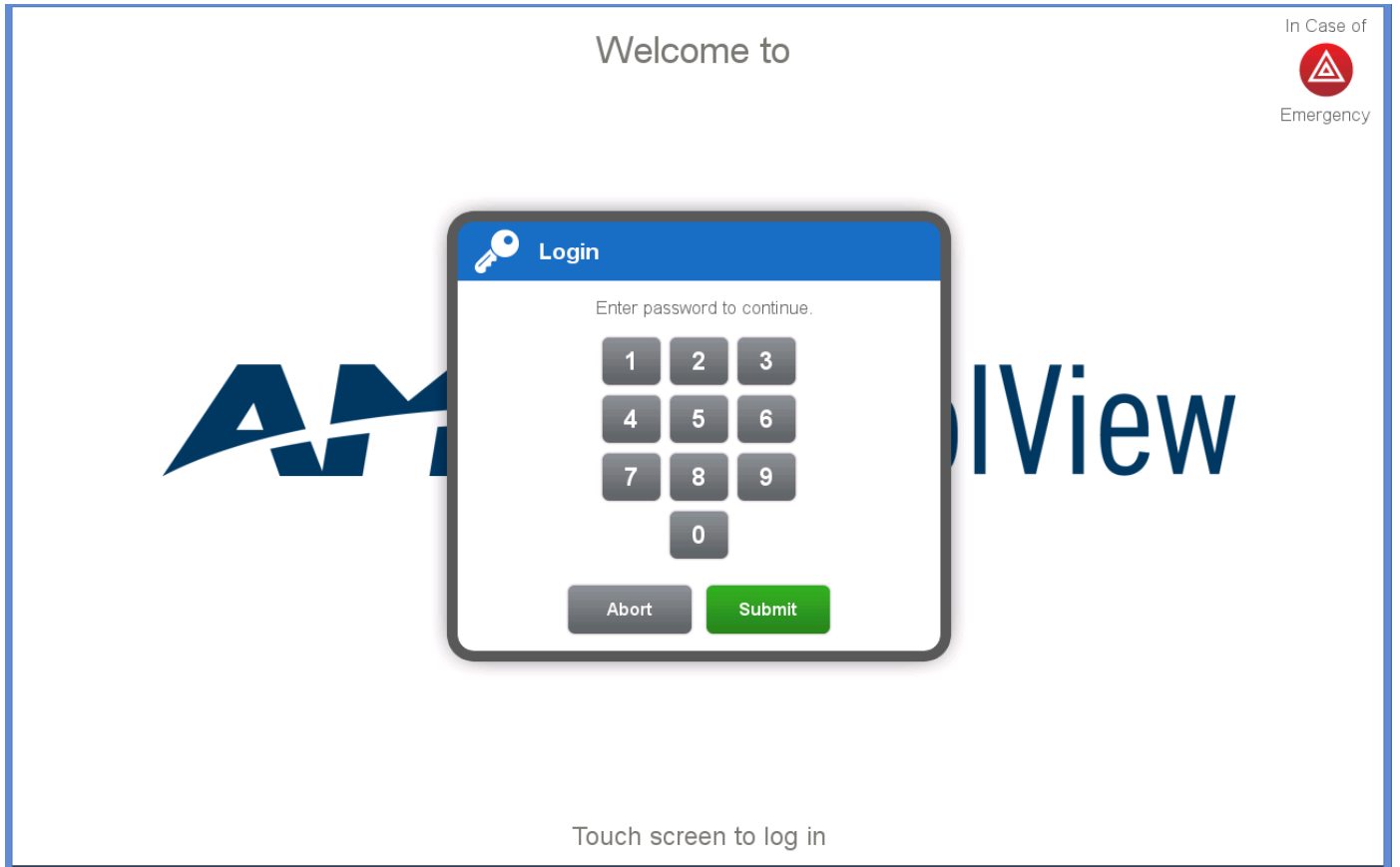
Loading and Configuring Other Software from the Admin TP

- 1) After completing the previous section, the system should boot up and configure the Admin touch panel.
- 2) If you uploaded a custom logo file to the /images/ folder you should see it on the admin touch panel.
- 3) Touch the screen to proceed.



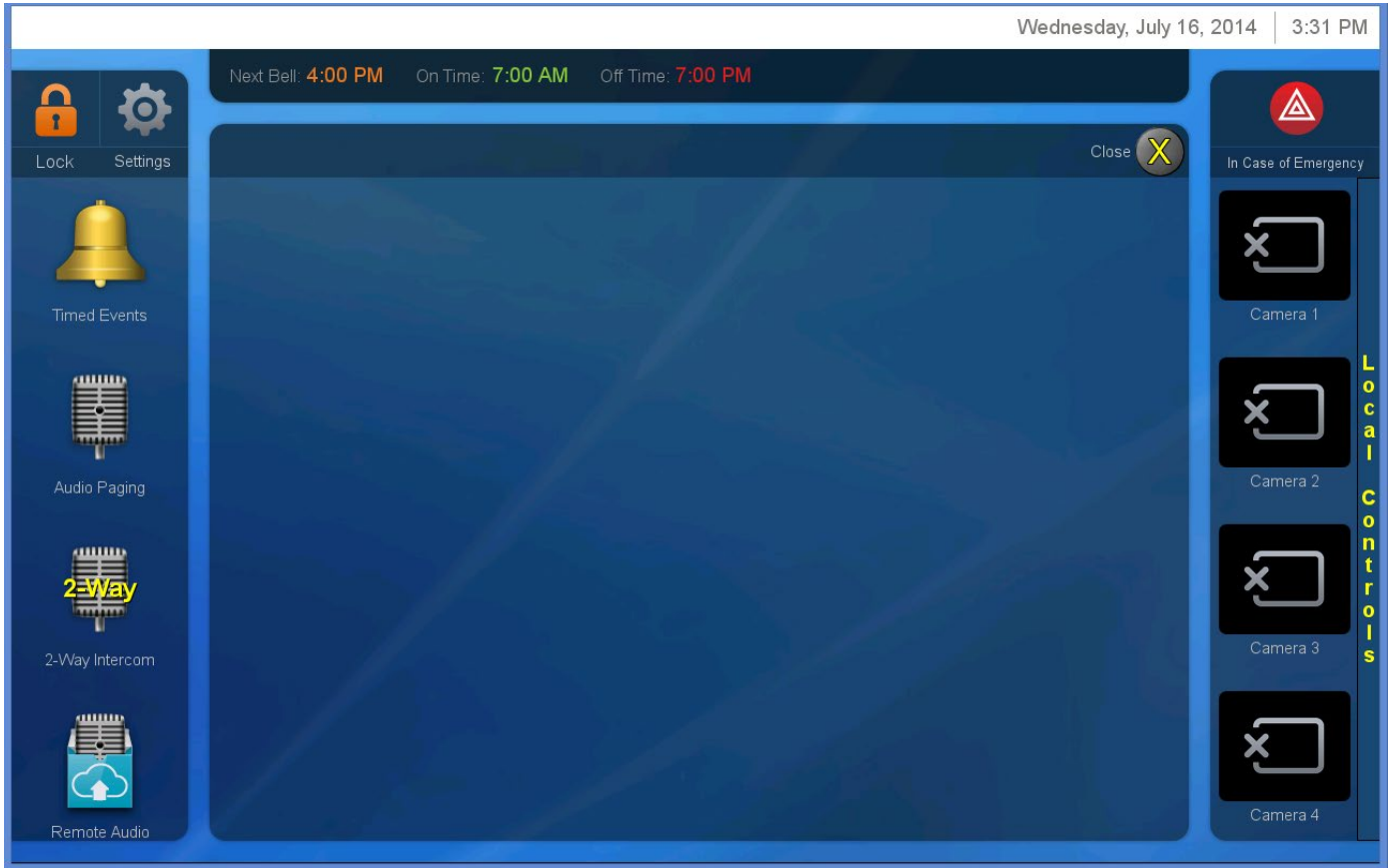
SchoolView

4) Enter the default Admin password “1379” to proceed to the touch panel main page.



SchoolView

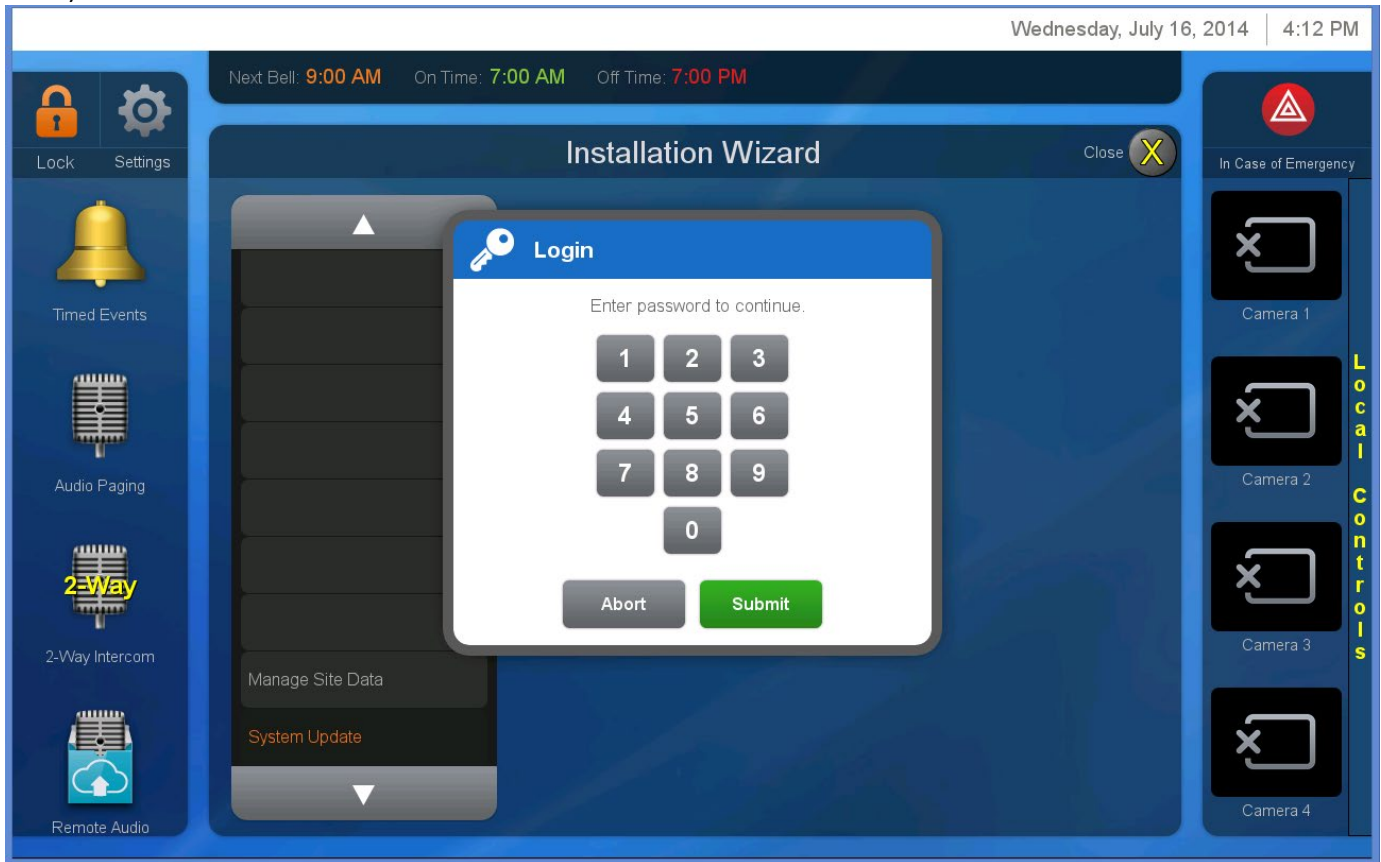
6) Select Settings to launch the System Management Page



SchoolView

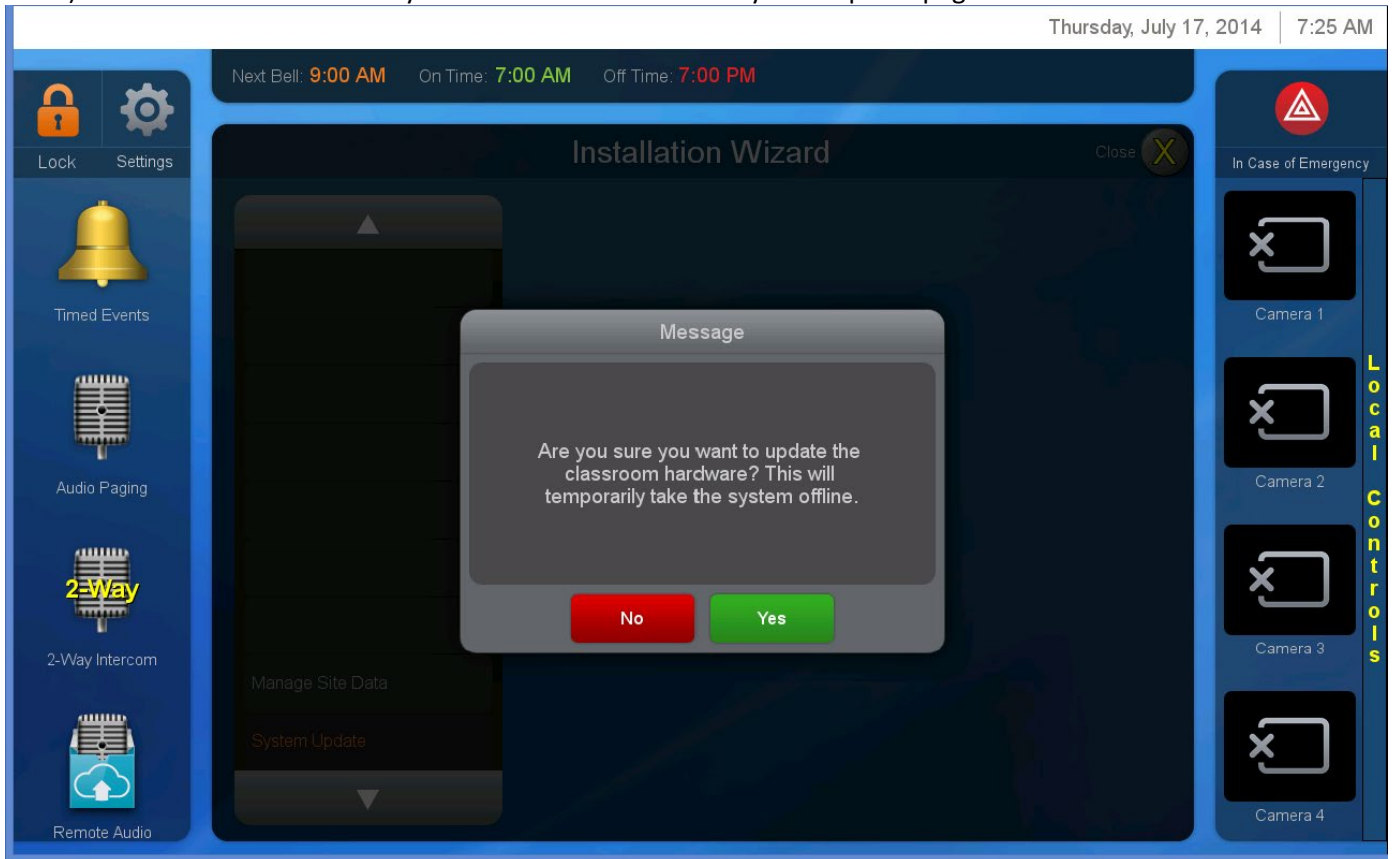
Press the down arrow twice at the bottom of the setting menu until you see System Update.

- 7) Enter the System Update password "973526".
- 8) Press Done.



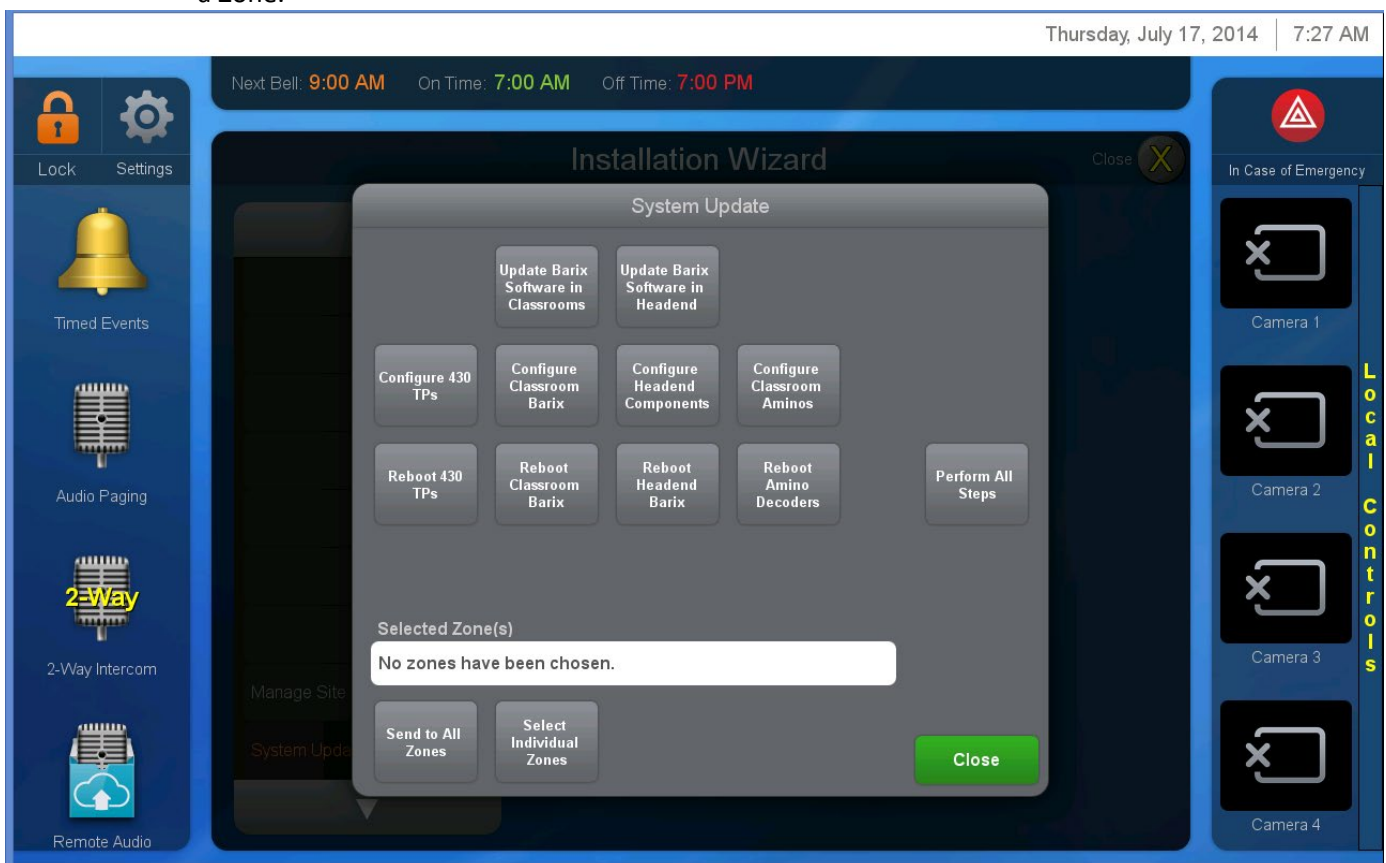
SchoolView

9) Press YES to confirm that you wish to continue to the System Update page.



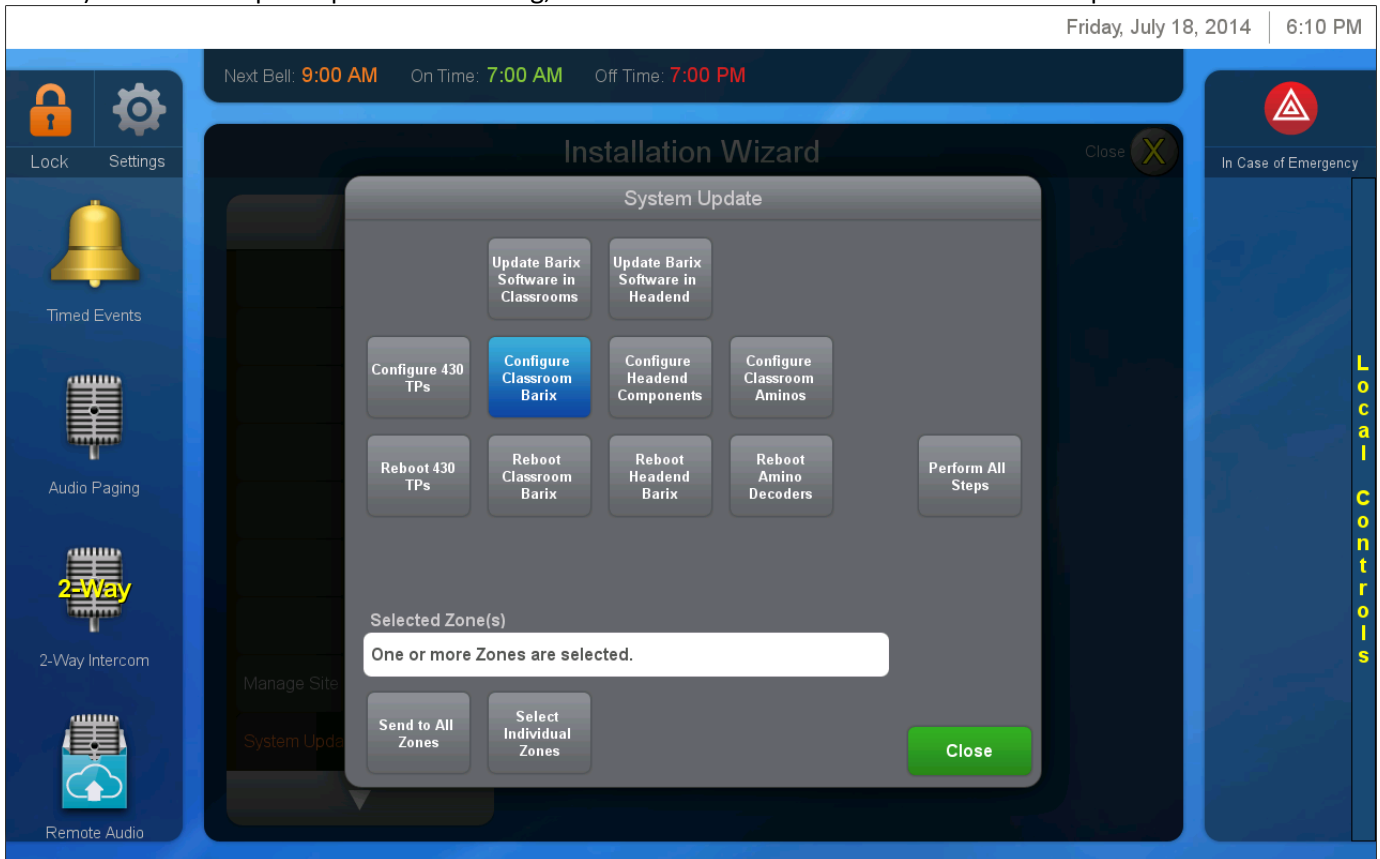
SchoolView

- 10) You will be presented with several options to update the system.
- Top row: Update Barix software (firmware load) to all audio decoder/encoders in the system. These processes can take several minutes to approximately an hour to complete depending on the size of the system.
 - Middle row: Send configuration commands to all system devices. These processes should only take a few minutes to complete.
 - Bottom row: Reboot devices by type. These are provided for your convenience. All of the other processes you can initiate from this page also result in reboots, so these are not strictly necessary.
 - Perform All Steps: This button runs all of the processes in turn.
 - Before selecting an Update, Configure or Reboot button you must select either the Send to All Zones button or the Select Individual Zones button. Note that common zone audio decoders will not be configured with the Headend buttons but can be configured with the Classroom buttons if selected as a Zone.



SchoolView

11) While each update process is running, the associated button will flash on the touch panel.



SchoolView

- 12) Upon completion of an update process, you should see a Trouble List pop-up as shown below.
a. If loading or configuration of any devices failed, they will be listed here.

Friday, July 18, 2014 | 6:16 PM

Next Bell: 9:00 AM On Time: 7:00 AM Off Time: 7:00 PM

Lock Settings

Timed Events

Audio Paging

2-Way Intercom

Remote Audio

In Case of Emergency

Local Controls

System Status

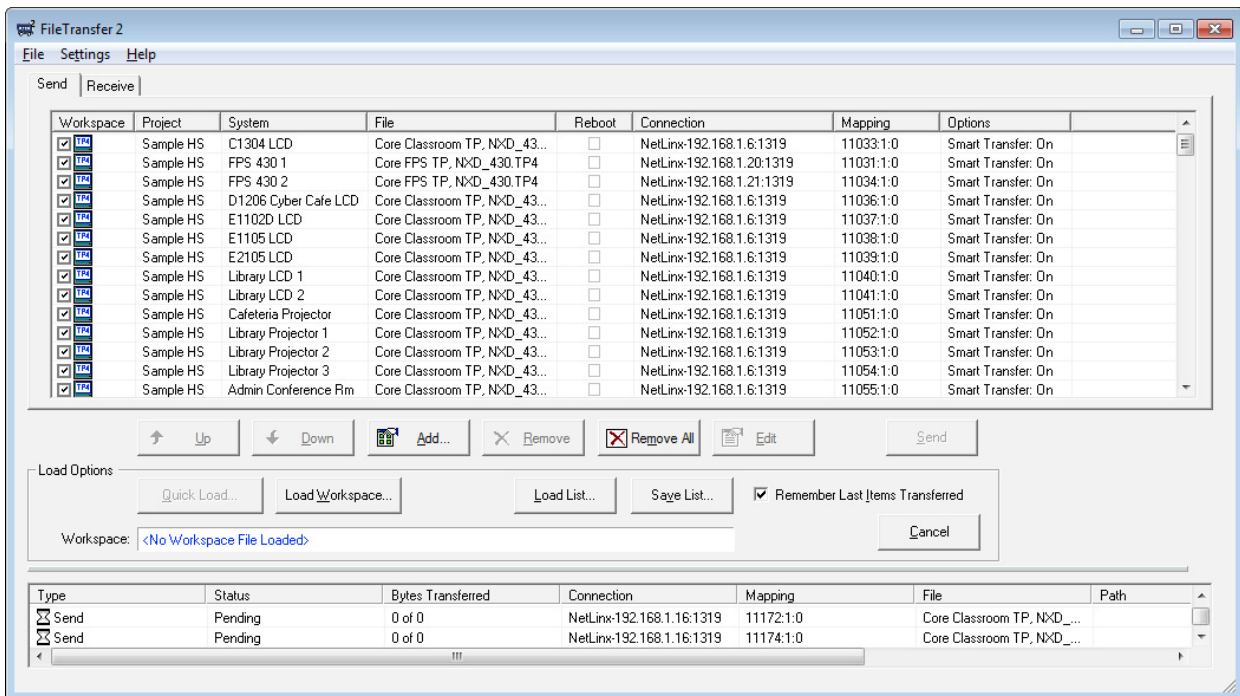
The following devices need attention.

OK

SchoolView

Loading Classroom Touch Panel Files

- 1) Open AMX File Transfer tool inside NetLinX Studio.
- 2) Click Add.
- 3) On the Other tab, select the appropriate file type and click Add again.
- 4) Choose the correct file and click Open.
- 5) Define the appropriate Device, Port and System values for this file and click OK twice.
- 6) Choose the item you've just added, then click Edit -> Communication Settings.
- 7) Add or select the appropriate master communication settings and click OK.
- 8) Repeat steps 2) through 7) for each touch panel and NetLinX file.
- 9) Ensure all appropriate check-boxes on the left side of the window are selected.
- 10) If "Remember Last Items Transferred" is checked, you can still open this dialog later and re-send necessary files.
- 11) Alternatively (highly recommended), you can save out this list of files to re-load later.
- 12) Click Send.



- 1) Examine the status window at the bottom to confirm all transfers completed.
- 2) If any of the transfers do fail, make note of them and retry as described above.

SchoolView

User Training Guidelines (Admin & Teacher)

We have found that the most efficient and effective training method is to divide the training into two general categories; several teacher training sessions and one larger administration training session. Our suggestion would be to start the teacher training portion as soon as possible in the morning and then conduct the administration training when school is out in the afternoon.

It is also very helpful if attendance is required.

Administration Training

- 1) Time: 3 hours.
- 2) Attendees should include the following:
 - a. Administrators
 - b. Front office personnel
 - c. Librarians
 - d. District or Campus Technology personnel

Teacher Training

- 1) Time: 1 hour for each session.
 - a. Generally it works well if we can work with a small group of teachers rotating through during their off hour or planning period.
- 2) Attendees should include the following:
 - a. Teachers
 - b. Librarians
 - c. District or Campus Technology personnel

Chapter Goals

- Explain IP multicast addressing.
- Learn the basics of Internet Group Management Protocol (IGMP).
- Explain how multicast in Layer 2 switching works.
- Define multicast distribution trees.
- Learn how multicast forwarding works.
- Explain the basics of protocol-independent multicast (PIM).
- Define multiprotocol BGP.
- Learn how Multicast Source Discovery Protocol (MSDP) works.
- Explain reliable multicast: PGM.

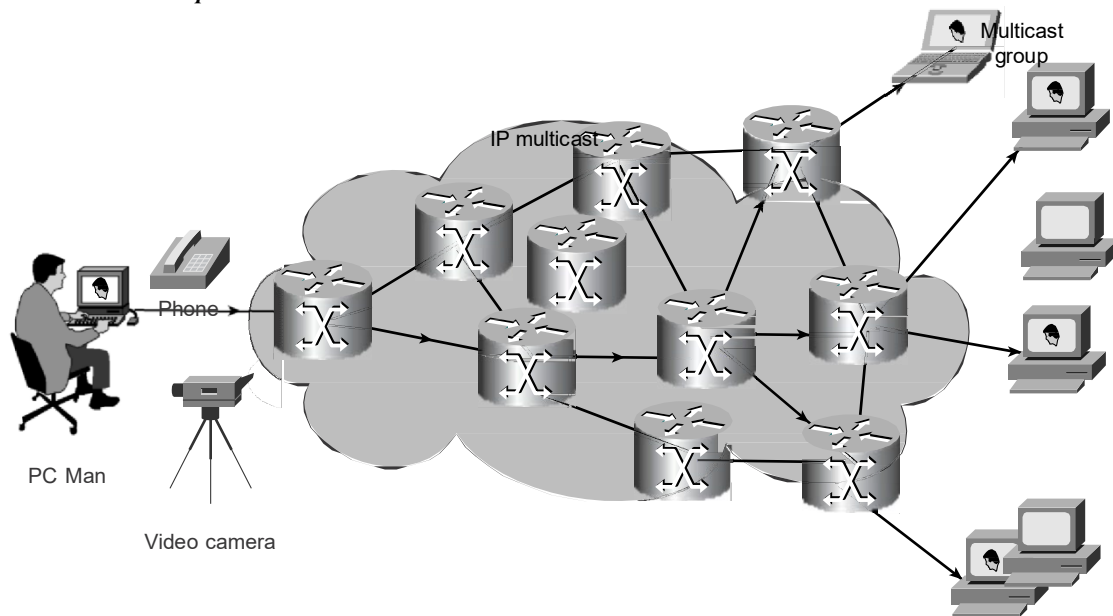
Internet Protocol Multicast

Background

Internet Protocol (IP) multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast include videoconferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

IP Multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers while using the least network bandwidth of any competing technology. Multicast packets are replicated in the network by Cisco routers enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols resulting in the most efficient delivery of data to multiple receivers possible. All alternatives require the source to send more than one copy of the data. Some even require the source to send an individual copy to each receiver. If there are thousands of receivers, even low-bandwidth applications benefit from using Cisco IP Multicast. High-bandwidth applications, such as MPEG video, may require a large portion of the available network bandwidth for a single stream. In these applications, the only way to send to more than one receiver simultaneously is by using IP Multicast. Figure 43-1 demonstrates how data from one source is delivered to several interested recipients using IP multicast.

Figure 43-1 Multicast Transmission Sends a Single Multicast Packet Addressed to All Intended Recipients



Multicast Group Concept

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flowing to a particular group must join the group using IGMP. Hosts must be a member of the group to receive the data stream.

IP Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

IP Class D Addresses

The *Internet Assigned Numbers Authority (IANA)* controls the assignment of IP multicast addresses. It has assigned the old Class D address space to be used for IP multicast. This means that all IP multicast group addresses will fall in the range of 224.0.0.0 to 239.255.255.255.



Note

This address range is only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.

Reserved Link Local Addresses

The IANA has reserved addresses in the 224.0.0.0 through 224.0.0.255 to be used by network protocols on a local network segment. Packets with these addresses should never be forwarded by a router; they remain local on a particular LAN segment. They are always transmitted with a time-to-live (TTL) of 1.

Network protocols use these addresses for automatic router discovery and to communicate important routing information. For example, OSPF uses 224.0.0.5 and 224.0.0.6 to exchange link state information. Table 43-1 lists some of the well-known addresses.

Table 43-1 Link Local Addresses

Address	Usage
224.1.1.1	All systems on this subnet
224.1.1.2	All routers on this subnet
224.1.1.5	OSPF routers
224.1.1.6	OSPF designated routers
224.0.0.12	DHCP server/relay agent

Globally Scoped Address

The range of addresses from 224.0.1.0 through 238.255.255.255 are called globally scoped addresses. They can be used to multicast data between organizations and across the Internet.

Some of these addresses have been reserved for use by multicast applications through IANA. For example, 224.0.1.1 has been reserved for Network Time Protocol (NTP).

More information about reserved multicast addresses can be found at <http://www.isi.edu/in-notes/iana/assignments/multicast-addresses>.

Limited Scope Addresses

The range of addresses from 239.0.0.0 through 239.255.255.255 contains limited scope addresses or administratively scoped addresses. These are defined by RFC 2365 to be constrained to a local group or organization. Routers are typically configured with filters to prevent multicast traffic in this address range from flowing outside an autonomous system (AS) or any user-defined domain. Within an autonomous system or domain, the limited scope address range can be further subdivided so those local multicast boundaries can be defined. This also allows for address reuse among these smaller domains.

Glop Addressing

RFC 2770 proposes that the 233.0.0.0/8 address range be reserved for statically defined addresses by organizations that already have an AS number reserved. The AS number of the domain is embedded into the second and third octets of the 233.0.0.0/8 range.

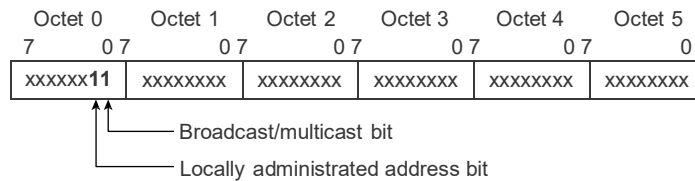
For example, the AS 62010 is written in hex as F23A. Separating out the two octets F2 and 3A, we get 242 and 58 in decimal. This would give us a subnet of 233.242.58.0 that would be globally reserved for AS 62010 to use.

Layer 2 Multicast Addresses

Normally, network interface cards (NICs) on a LAN segment will receive only packets destined for their burned-in MAC address or the broadcast MAC address. Some means had to be devised so that multiple hosts could receive the same packet and still be capable of differentiating among multicast groups.

Fortunately, the IEEE LAN specifications made provisions for the transmission of broadcast and/or multicast packets. In the 802.3 standard, bit 0 of the first octet is used to indicate a broadcast and/or multicast frame. Figure 43-2 shows the location of the broadcast/multicast bit in an Ethernet frame.

Figure 43-2 IEEE 802.3 MAC Address Format



This bit indicates that the frame is destined for an arbitrary group of hosts or all hosts on the network (in the case of the broadcast address, 0xFFFF.FFFF.FFFF).

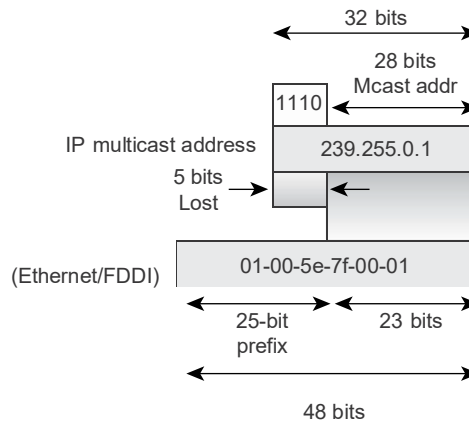
IP multicast makes use of this capability to transmit IP packets to a group of hosts on a LAN segment.

Ethernet MAC Address Mapping

The IANA owns a block of Ethernet MAC addresses that start with 01:00:5E in hexadecimal. Half of this block is allocated for multicast addresses. This creates the range of available Ethernet MAC addresses to be 0100.5e00.0000 through 0100.5e7f.ffff.

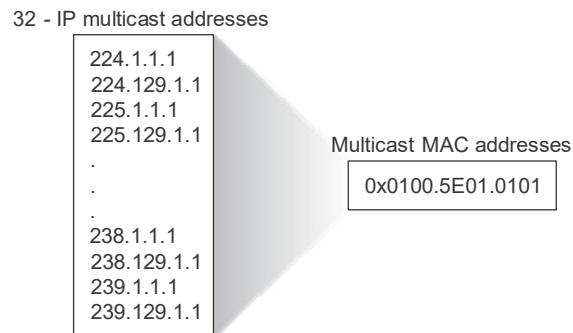
This allocation allows for 23 bits in the Ethernet address to correspond to the IP multicast group address. The mapping places the lower 23 bits of the IP multicast group address into these available 23 bits in the Ethernet address (shown in Figure 43-3).

Figure 43-3 Mapping of IP Multicast to Ethernet/FDDI MAC Address



Because the upper 5 bits of the IP multicast address are dropped in this mapping, the resulting address is not unique. In fact, 32 different multicast group IDs all map to the same Ethernet address (see Figure 43-4).

Figure 43-4 MAC Address Ambiguities

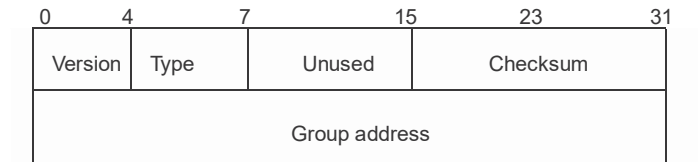


Internet Group Management Protocol

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IGMP Version 1

RFC 1112 defines the specification for IGMP Version 1. A diagram of the packet format is found in Figure 43-5.

Figure 43-5 IGMP Version 1 Packet Format

In Version 1, there are just two different types of IGMP messages:

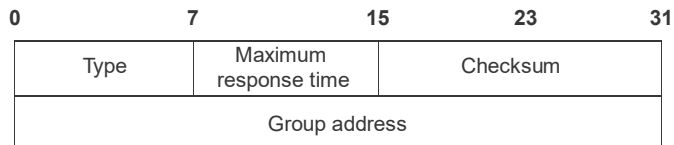
- Membership query
- Membership report

Hosts send out IGMP membership reports corresponding to a particular multicast group to indicate that they are interested in joining that group. The router periodically sends out an IGMP membership query to verify that at least one host on the subnet is still interested in receiving traffic directed to that group. When there is no reply to three consecutive IGMP membership queries, the router times out the group and stops forwarding traffic directed toward that group.

IGMP Version 2

RFC 2236 defines the specification for IGMP Version 2.

A diagram of the packet format follows in Figure 43-6.

Figure 43-6 IGMPv2 Message Format

In Version 2, there are four types of IGMP messages:

- Membership query
- Version 1 membership report
- Version 2 membership report
- Leave group

IGMP Version 2 works basically the same as Version 1. The main difference is that there is a leave group message. The hosts now can actively communicate to the local multicast router their intention to leave the group. The router then sends out a group-specific query and determines whether there are any remaining hosts interested in receiving the traffic. If there are no replies, the router times out the group and stops forwarding the traffic. This can greatly reduce the leave latency compared to IGMP Version 1. Unwanted and unnecessary traffic can be stopped much sooner.

Multicast in the Layer 2 Switching Environment

The default behavior for a Layer 2 switch is to forward all multicast traffic to every port that belongs to the destination LAN on the switch. This would defeat the purpose of the switch, which is to limit traffic to the ports that need to receive the data.

Two methods exist by which to deal with multicast in a Layer 2 switching environment efficiently—Cisco Group Management Protocol (CGMP) and IGMP snooping.

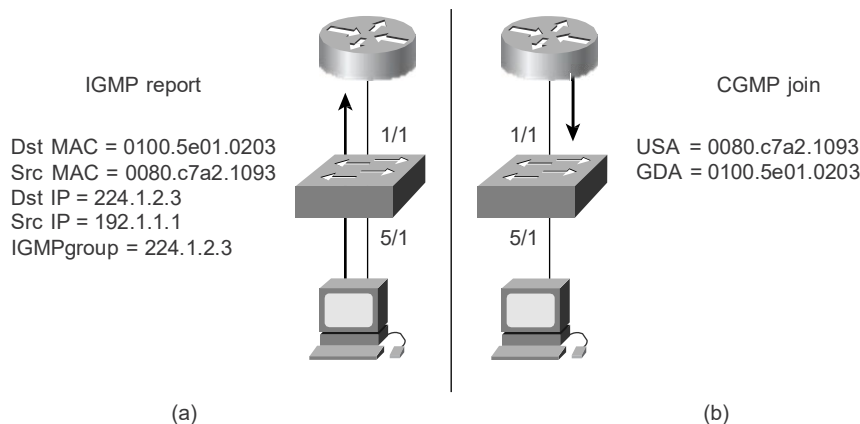
Cisco Group Management Protocol

CGMP is a Cisco-developed protocol that allows Catalyst switches to leverage IGMP information on Cisco routers to make Layer 2 forwarding decisions. CGMP must be configured both on the multicast routers and on the Layer 2 switches. The net result is that with CGMP, IP multicast traffic is delivered only to those Catalyst switch ports that are interested in the traffic. All other ports that have not explicitly requested the traffic will not receive it.

The basic concept of CGMP is shown in Figure 43-7. When a host joins a multicast group (part A), it multicasts an unsolicited IGMP membership report message to the target group (224.1.2.3, in this example). The IGMP report is passed through the switch to the router for the normal IGMP processing. The router (which must have CGMP enabled on this interface) receives this IGMP report and processes it as it normally would, but in addition it creates a CGMP join message and sends it to the switch.

The switch receives this CGMP join message and then adds the port to its content addressable memory (CAM) table for that multicast group. Subsequent traffic directed to this multicast group will be forwarded out the port for that host. The router port is also added to the entry for the multicast group. Multicast routers must listen to all multicast traffic for every group because the IGMP control messages are also sent as multicast traffic. With CGMP, the switch must listen only to CGMP join and CGMP leave messages from the router. The rest of the multicast traffic is forwarded using its CAM table exactly the way the switch was designed.

Figure 43-7 Basic CGMP Operation



IGMP Snooping

IGMP snooping requires the LAN switch to examine, or snoop, some Layer 3 information in the IGMP packets sent between the hosts and the router. When the switch hears the IGMP host report from a host for a particular multicast group, the switch adds the host's port number to the associated multicast table entry. When the switch hears the IGMP leave group message from a host, it removes the host's port from the table entry.

Because IGMP control messages are transmitted as multicast packets, they are indistinguishable from multicast data at Layer 2. A switch running IGMP snooping examines every multicast data packet to check whether it contains any pertinent IGMP control information. If IGMP snooping has been implemented on a low-end switch with a slow CPU, this could have a severe performance impact when

Multicast Distribution Trees

data is transmitted at high rates. The solution is to implement IGMP snooping on high-end switches with special ASICs that can perform the IGMP checks in hardware. CGMP is ideal for low-end switches without special hardware.

Multicast Distribution Trees

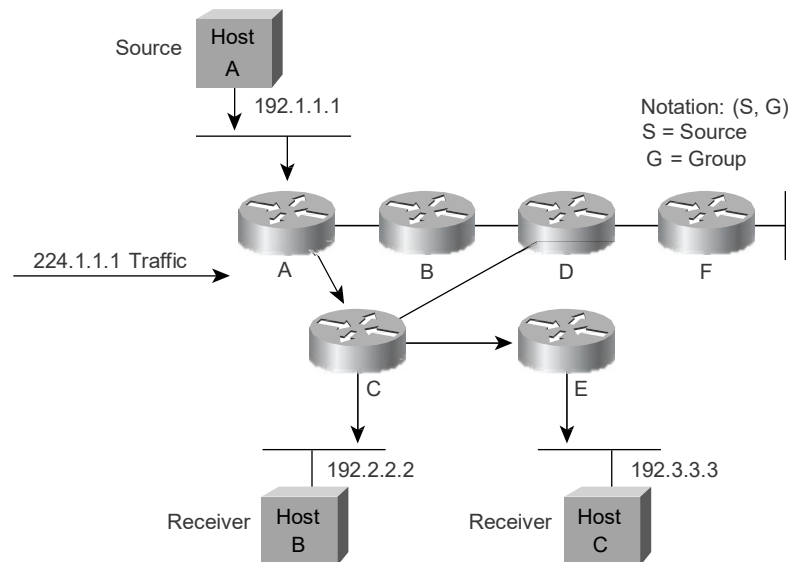
Multicast-capable routers create distribution trees that control the path that IP multicast traffic takes through the network to deliver traffic to all receivers. The two basic types of multicast distribution trees are source trees and shared trees.

Source Trees

The simplest form of a multicast distribution tree is a *source tree* whose root is the source of the multicast tree and whose branches form a spanning tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).

Figure 43-8 shows an example of an SPT for group 224.1.1.1 rooted at the source, Host A, and connecting two receivers, hosts B and C.

Figure 43-8 Host A Shortest Path Tree



The special notation of (S,G), pronounced “S comma G,” enumerates an SPT in which S is the IP address of the source and G is the multicast group address. Using this notation, the SPT for the example in Figure 43-7 would be (192.1.1.1, 224.1.1.1).

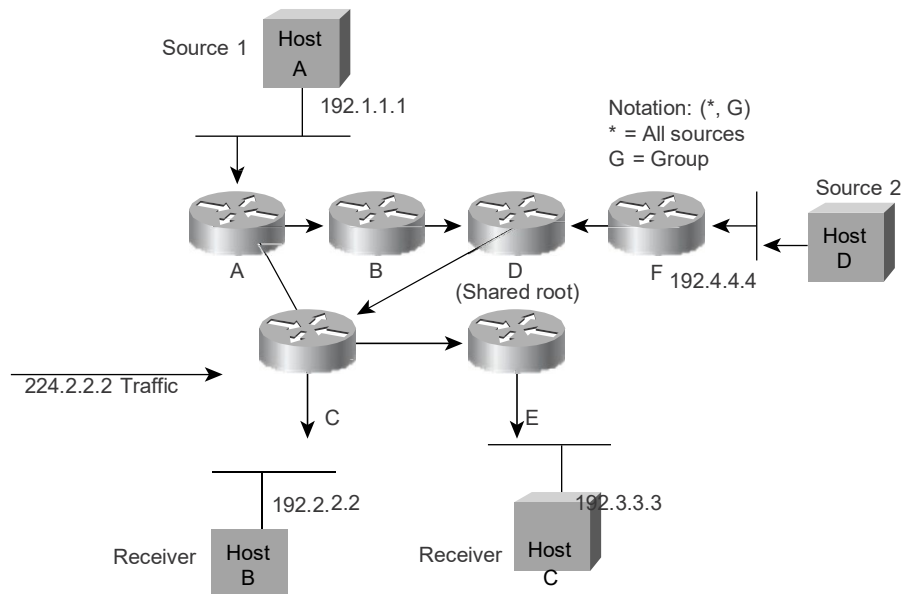
The (S,G) notation implies that a separate SPT exists for each individual source sending to each group, which is correct. For example, if Host B is also sending traffic to group 224.1.1.1 and hosts A and C are receivers, then a separate (S,G) SPT would exist with a notation of (192.2.2.2,224.1.1.1).

Shared Trees

Unlike source trees that have their root at the source, *shared trees* use a single common root placed at some chosen point in the network. This shared root is called the *rendezvous point (RP)*.

Figure 43-9 shows a shared tree for the group 224.2.2.2 with the root located at Router D. When using a shared tree, sources must send their traffic to the root, and then the traffic is forwarded down the shared tree to reach all receivers.

Figure 43-9 Shared Distribution Tree



In this example, multicast traffic from the source hosts A and D travels to the root (Router D) and then down the shared tree to the two receivers, hosts B and C. Because all sources in the multicast group use a common shared tree, a wildcard notation written as $(*, G)$, pronounced “star comma G,” represents the tree. In this case, $*$ means all sources, and the G represents the multicast group. Therefore, the shared tree shown in Figure 43-8 would be written as $(*, 224.2.2.2)$.

Both SPT and shared trees are loop-free. Messages are replicated only where the tree branches.

Members of multicast groups can join or leave at any time, so the distribution trees must be dynamically updated. When all the active receivers on a particular branch stop requesting the traffic for a particular multicast group, the routers prune that branch from the distribution tree and stop forwarding traffic down that branch. If one receiver on that branch becomes active and requests the multicast traffic, the router dynamically modifies the distribution tree and starts forwarding traffic again.

Shortest path trees have the advantage of creating the optimal path between the source and the receivers. This guarantees the minimum amount of network latency for forwarding multicast traffic. This optimization does come with a price, though: The routers must maintain path information for each source. In a network that has thousands of sources and thousands of groups, this can quickly become a resource issue on the routers. Memory consumption from the size of the multicast routing table is a factor that network designers must take into consideration.

Shared trees have the advantage of requiring the minimum amount of state in each router. This lowers the overall memory requirements for a network that allows only shared trees. The disadvantage of shared trees is that, under certain circumstances, the paths between the source and receivers might not be the optimal paths—which might introduce some latency in packet delivery. Network designers must carefully consider the placement of the RP when implementing an environment with only shared trees.

Multicast Forwarding

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not really care about the source address—it only cares about the destination address and how to forward the traffic towards that destination. The router scans through its routing table and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

In multicast routing, the source is sending traffic to an arbitrary group of hosts represented by a multicast group address. The multicast router must determine which direction is upstream (toward the source) and which direction (or directions) is downstream. If there are multiple downstream paths, the router replicates the packet and forwards the traffic down the appropriate downstream paths—which is not necessarily all paths. This concept of forwarding multicast traffic away from the source, rather than to the receiver, is called *reverse path forwarding*.

Reverse Path Forwarding

Reverse path forwarding (RPF) is a fundamental concept in multicast routing that enables routers to correctly forward multicast traffic down the distribution tree. RPF makes use of the existing unicast routing table to determine the upstream and downstream neighbors. A router forwards a multicast packet only if it is received on the upstream interface. This RPF check helps to guarantee that the distribution tree will be loop-free.

RPF Check

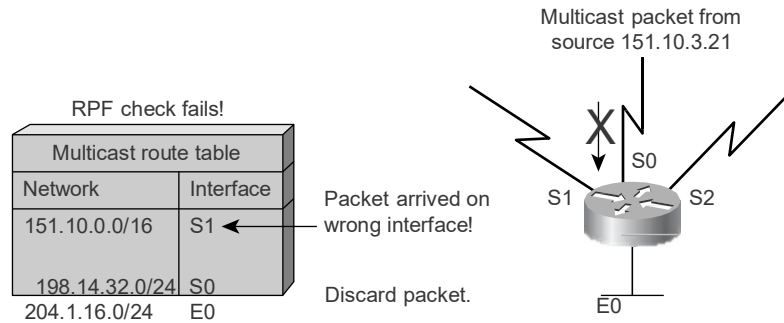
When a multicast packet arrives at a router, the router performs an RPF check on the packet. If the RPF check is successful, the packet is forwarded. Otherwise, it is dropped.

For traffic flowing down a source tree, the RPF check procedure works as follows:

-
- Step 1** Router looks up the source address in the unicast routing table to determine whether it has arrived on the interface that is on the reverse path back to the source.
 - Step 2** If packet has arrived on the interface leading back to the source, the RPF check is successful and the packet is forwarded.
 - Step 3** If the RPF check in Step 2 fails, the packet is dropped.

Figure 43-10 shows an example of an unsuccessful RPF check.

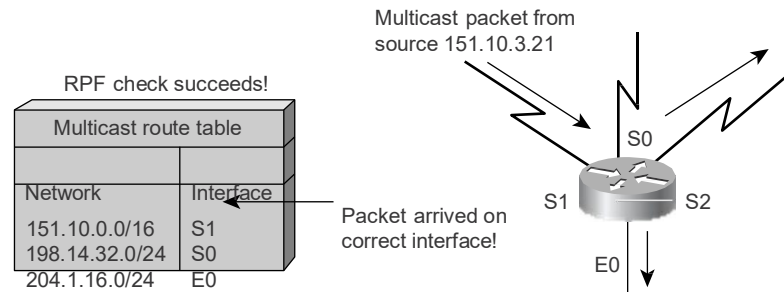
Figure 43-10 RPF Check Fails



A multicast packet from source 151.10.3.21 is received on interface S0. A check of the unicast routing table shows that the interface that this router would use to forward unicast data to 151.10.3.21 is S1. Because the packet has arrived on S0, the packet will be discarded.

Figure 43-11 shows an example of a successful RPF check.

Figure 43-11 RPF Check Succeeds



This time the multicast packet has arrived on S1. The router checks the unicast routing table and finds that S1 is the correct interface. The RPF check passes and the packet is forwarded.

Protocol-Independent Multicast

Protocol-independent multicast (PIM) gets its name from the fact that it is IP routing protocol-independent. PIM can leverage whichever unicast routing protocols are used to populate the unicast routing table, including EIGRP, OSPF, BGP, or static routes. PIM uses this unicast routing information to perform the multicast forwarding function, so it is IP protocol-independent. Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. PIM does not send and receive multicast routing updates between routers like other routing protocols do.

PIM Dense Mode

PIM Dense Mode (PIM-DM) uses a push model to flood multicast traffic to every corner of the network. This is a brute-force method for delivering data to the receivers, but in certain applications, this might be an efficient mechanism if there are active receivers on every subnet in the network.

PIM-DM initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbors prune back the unwanted traffic. This process repeats every 3 minutes.

The flood and prune mechanism is how the routers accumulate their state information—by receiving the data stream. These data streams contain the source and group information so that downstream routers can build up their multicast forwarding tables. PIM-DM can support only source trees—(S,G) entries. It cannot be used to build a shared distribution tree.

PIM Sparse Mode

PIM Sparse Mode (PIM-SM) uses a pull model to deliver multicast traffic. Only networks that have active receivers that have explicitly requested the data will be forwarded the traffic. PIM-SM is defined in RFC 2362.

PIM-SM uses a shared tree to distribute the information about active sources. Depending on the configuration options, the traffic can remain on the shared tree or switch over to an optimized source distribution tree. The latter is the default behavior for PIM-SM on Cisco routers. The traffic starts to flow down the shared tree, and then routers along the path determine whether there is a better path to the source. If a better, more direct path exists, the designated router (the router closest to the receiver) will send a join message toward the source and then reroute the traffic along this path.

PIM-SM has the concept of an RP, since it uses shared trees—at least initially. The RP must be administratively configured in the network. Sources register with the RP, and then data is forwarded down the shared tree to the receivers. If the shared tree is not an optimal path between the source and the receiver, the routers dynamically create a source tree and stop traffic from flowing down the shared tree. This is the default behavior in IOS. Network administrators can force traffic to stay on the shared tree by using a configuration option (`ip pim spt-threshold infinity`).

PIM-SM scales well to a network of any size, including those with WAN links. The explicit join mechanism prevents unwanted traffic from flooding the WAN links.

Sparse-Dense Mode

Cisco has implemented an alternative to choosing just dense mode or just sparse mode on a router interface new IP. This was necessitated by a change in the paradigm for forwarding multicast traffic via PIM that became apparent during its development. It turned out that it was more efficient to choose sparse or dense on a per group basis rather than a per router interface basis. Sparse-dense mode facilitates this ability.

Network administrators can also configure sparse-dense mode. This configuration option allows individual groups to be run in either sparse or dense mode, depending on whether RP information is available for that group. If the router learns RP information for a particular group, it will be treated as sparse mode; otherwise, that group will be treated as dense mode.

Multiprotocol Border Gateway Protocol

Multiprotocol Border Gateway Protocol (MBGP) gives a method for providers to distinguish which route prefixes they will use for performing multicast RPF checks. The RPF check is the fundamental mechanism that routers use to determine the paths that multicast forwarding trees will follow and successfully deliver multicast content from sources to receivers.

MBGP is described in RFC 2283, Multiprotocol Extensions for BGP-4. Since MBGP is an extension of BGP, it brings along all the administrative machinery that providers and customers like in their interdomain routing environment. Including all the inter-AS tools to filter and control routing (e.g., route maps). Therefore, by using MBGP, any network utilizing internal or external BGP can apply the multiple policy control knobs familiar in BGP to specify routing (and thereby forwarding) policy for multicast.

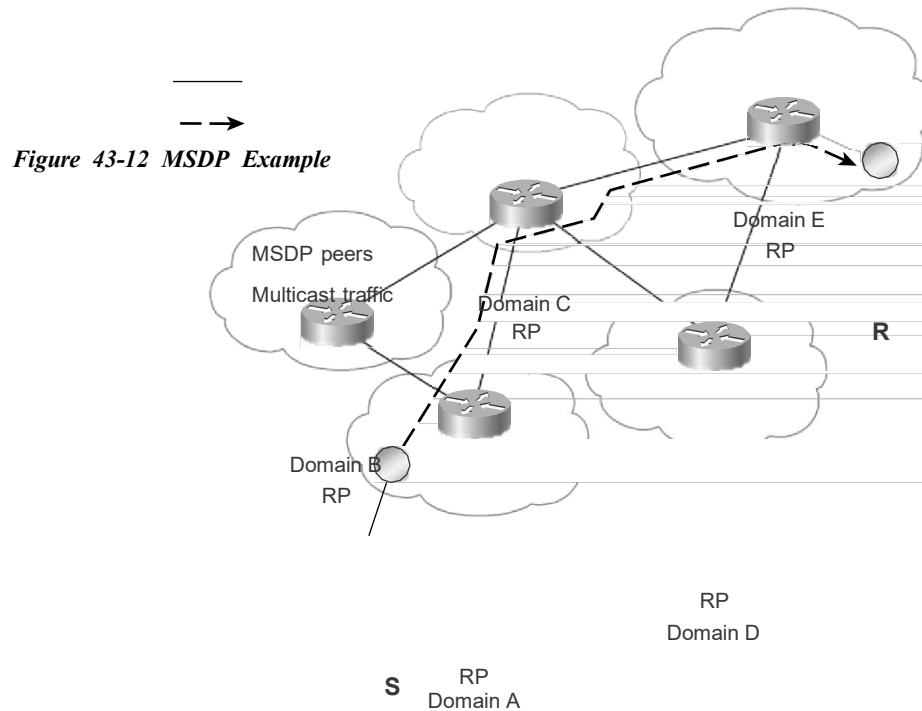
Two path attributes, `MP_REACH_NLRI` and `MP_UNREACH_NLRI` have been introduced in BGP4+. These new attributes create a simple way to carry two sets of routing information—one for unicast routing and one for multicast routing. The routes associated with multicast routing are used to build the multicast distribution trees.

The main advantage of MBGP is that an internet can support noncongruent unicast and multicast topologies. When the unicast and multicast topologies are congruent, MBGP can support different policies for each. MBGP provides a scalable policy based interdomain routing protocol.

Multicast Source Discovery Protocol

In the PIM Sparse mode model, multicast sources and receivers must register with their local Rendezvous Point (RP). Actually, the closest router to the sources or receivers registers with the RP but the point is that the RP knows about all the sources and receivers for any particular group. RPs in other domains have no way of knowing about sources located in other domains. MSDP is an elegant way to solve this problem. MSDP is a mechanism that connects PIM-SM domains and allows RPs to share information about active sources. When RPs in remote domains know about active sources they can pass on that information to their local receivers and multicast data can be forwarded between the domains. A nice feature of MSDP is that it allows each domain to maintain an independent RP which does not rely on other domains, but it does enable RPs to forward traffic between domains.

The RP in each domain establishes an MSDP peering session using a TCP connection with the RPs in other domains or with border routers leading to the other domains. When the RP learns about a new multicast source within its own domain (through the normal PIM register mechanism), the RP encapsulates the first data packet in a Source Active (SA) message and sends the SA to all MSDP peers. The SA is forwarded by each receiving peer using a modified RPF check, until it reaches every MSDP router in the interconnected networks—theoretically the entire multicast internet. If the receiving MSDP peer is an RP, and the RP has a (*,G) entry for the group in the SA (there is an interested receiver), the RP will create (S,G) state for the source and join to the shortest path tree for the state of the source. The encapsulated data is decapsulated and forwarded down that RP's shared tree. When the packet is received by a receiver's last hop router, the last-hop may also join the shortest path tree to the source. The source's RP periodically sends SAs, which include all sources within that RP's own domain. Figure 43-12 shows how data would flow between a source in domain A to a receiver in domain E.



192.1.1.1, 224.2.2.2

MSDP was developed for peering between Internet Service Providers (ISPs). ISPs did not want to rely on an RP maintained by a competing ISP to service their customers. MSDP allows each ISP to have their own local RP and still forward and receive multicast traffic to the Internet.

Anycast RP-Logical RP

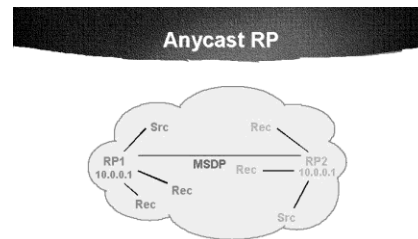
A very useful application of MSDP is called anycast RP. This is a technique for configuring a multicast sparse-mode network to provide for fault tolerance and load sharing within a single multicast domain.

Two or more RPs are configured with the same IP address on loopback interfaces—say, 10.0.0.1, for example (refer to Figure 43-13). The loopback address should be configured as a 32 bit address. All the downstream routers are configured so that they know that their local RP's address is 10.0.0.1. IP routing automatically selects the topologically closest RP for each source and receiver. Because some sources might end up using one RP and some receivers a different RP, there needs to be some way for the RPs to exchange information about active sources. This is done with MSDP. All the RPs are configured to be MSDP peers of each other. Each RP will know about the active sources in the other RP's area. If any of the RPs fail, IP routing will converge and one of the RPs will become the active RP in both areas.



Note The Anycast RP example above uses IP addresses from RFC 1918. These IP addresses are normally blocked at interdomain borders and therefore are not accessible to other ISPs. You must use valid IP addresses if you want the RPs to be reachable from other domains.

Figure 43-13 Anycast RP



Note The RPs are used only to set up the initial connection between sources and receivers. After the last-hop routers join the shortest path tree, the RP is no longer necessary.

Multicast Address Dynamic Client Allocation Protocol

The *Multicast Address Dynamic Client Allocation Protocol (MADCAP)* is defined in RFC 2730 as a protocol that allows hosts to request a multicast address allocation dynamically from a MADCAP server. The concept is very similar to the way DHCP works today and is built on a client/server model.

Multicast-Scope Zone Announcement Protocol

Multicast-Scope Zone Announcement Protocol (MZAP) is defined in RFC 2776 as a protocol that allows networks to automatically discover administratively scoped zones relative to a particular location.

Reliable Multicast-Pragmatic General Multicast

Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for applications that require ordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss.

The PGM Reliable Transport Protocol itself is implemented on the sources and the receivers. The source maintains a transmit window of outgoing data packets and retransmits individual packets when it receives a negative acknowledgment (NAK). The network elements (routers) assist in suppressing an implosion of NAKs (when a failure does occur) and aids in efficient forwarding of the retransmitted data just to the networks that need it.

PGM is intended as a solution for multicast applications with basic reliability requirements. The specification for PGM is network layer-independent. The Cisco implementation of PGM Router Assist supports PGM over IP.

Today, the specification for PGM is an Internet draft that can be found on the IETF web site (<http://www.ietf.org>) under the name “PGM Reliable Transport Protocol.”

Review Questions

Q—*What is the range of available IP multicast addresses?*

A—224.0.0.0 to 239.255.255.255.

Q—*What is the purpose of IGMP?*

A—IGMP is used between the hosts and their local multicast router to join and leave multicast groups.

Q—*What is an advantage of IGMPv2 over IGMPv1?*

A—IGMPv2 has a leave group message that can greatly reduce the latency of unwanted traffic on a LAN.

Q—*What is a potential disadvantage of IGMP snooping over CGMP on a low-end Layer 2 switch?*

A—IGMP snooping requires the switch to examine every multicast packet for an IGMP control message. On a low-end switch, this might have a severe performance impact.

Q—*What is an advantage of shortest path (or source) trees compared to shared trees?*

A—Source trees guarantee an optimal path between each source and each receiver, which will minimize network latency.

Q—*What is an advantage of using shared trees?*

A—Shared trees require very little state to be kept in the routers, which requires less memory.

Q—*What information does the router use to do an RPF check?*

A—The unicast routing table.

Q—*Why is protocol-independent multicast called “independent”?*

A—PIM works with any underlying IP unicast routing protocol—RIP, EIGRP, OSPF, BGP or static routes.

Q—*What is the main advantage of MBGP?*

A—Providers can have noncongruent unicast and multicast routing topologies.

Q—*How do RPs learn about sources from other RPs with MSDP?*

A—RPs are configured to be MSDP peers with other RPs. Each RP forwards source active (SA) messages to each other.

Q—*What is the purpose of the anycast RP?*

A—Load balancing and fault tolerance.

For More Information

Williamson, Beau. *Developing IP Multicast Networks*. Indianapolis: Cisco Press, 2000. Multicast Quick Start Configuration Guide (<http://www.cisco.com/warp/customer/105/48.html>)

Appendix B: RFC 4541-Considerations for IGMP

Also found online at <http://tools.ietf.org/html/rfc4541>

Network Working Group M. Christensen
Request for Comments: 4541 Thrane & Thrane
Category: Informational K. Kimball
 Hewlett-Packard
 F. Solensky
 Calix
 May 2006

Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This memo describes the recommendations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping switches. These are based on best current practices for IGMPv2, with further considerations for IGMPv3- and MLDv2-snooping. Additional areas of relevance, such as link layer topology changes and Ethernet-specific encapsulation issues, are also considered.

1. Introduction

The IEEE bridge standard [[BRIDGE](#)] specifies how LAN packets are 'bridged', or as is more commonly used today, switched between LAN segments. The operation of a switch with respect to multicast packets can be summarized as follows. When processing a packet whose destination MAC address is a multicast address, the switch will forward a copy of the packet into each of the remaining network interfaces that are in the forwarding state in accordance with [[BRIDGE](#)]. The spanning tree algorithm ensures that the application of this rule at every switch in the network will make the packet accessible to all nodes connected to the network.

This behaviour works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is

intended for only a small number of nodes. Packets will be flooded into network segments where no node has any interest in receiving the packet. While nodes will rarely incur any processing overhead to filter packets addressed to unrequested group addresses, they are unable to transmit new packets onto the shared media for the period of time that the multicast packet is flooded. In general, significant bandwidth can be wasted by flooding.

In recent years, a number of commercial vendors have introduced products described as "IGMP snooping switches" to the market. These devices do not adhere to the conceptual model that provides the strict separation of functionality between different communications layers in the ISO model, and instead utilize information in the upper level protocol headers as factors to be considered in processing at the lower levels. This is analogous to the manner in which a router can act as a firewall by looking into the transport protocol's header before allowing a packet to be forwarded to its destination address.

In the case of IP multicast traffic, an IGMP snooping switch provides the benefit of conserving bandwidth on those segments of the network where no node has expressed interest in receiving packets addressed to the group address. This is in contrast to normal switch behavior where multicast traffic is typically forwarded on all interfaces.

Many switch datasheets state support for IGMP snooping, but no recommendations for this exist today. It is the authors' hope that the information presented in this document will supply this foundation.

The recommendations presented here are based on the following information sources: The IGMP specifications [[RFC1112](#)], [[RFC2236](#)] and [[IGMPv3](#)], vendor-supplied technical documents [[CISCO](#)], bug reports [[MSOFT](#)], discussions with people involved in the design of IGMP snooping switches, MAGMA mailing list discussions, and on replies by switch vendors to an implementation questionnaire.

Interoperability issues that arise between different versions of IGMP are not the focus of this document. Interested readers are directed to [[IGMPv3](#)] for a thorough description of problem areas.

The suggestions in this document are based on IGMP, which applies only to IPv4. For IPv6, Multicast Listener Discovery [[MLD](#)] must be used instead. Because MLD is based on IGMP, we do not repeat the entire description and recommendations for MLD snooping switches. Instead, we point out the few cases where there are differences from IGMP.

Note that the IGMP snooping function should apply only to IPv4 multicasts. Other multicast packets, such as IPv6, might be suppressed by IGMP snooping if additional care is not taken in the implementation as mentioned in the recommendations section. It is desired not to restrict the flow of non-IPv4 multicasts other than to the degree which would happen as a result of regular bridging functions. Likewise, MLD snooping switches are discouraged from using topological information learned from IPv6 traffic to alter the forwarding of IPv4 multicast packets.

2. IGMP Snooping Recommendations

The following sections list the recommendations for an IGMP snooping switch. The recommendation is stated and is supplemented by a description of a possible implementation approach. All implementation discussions are examples only and there may well be other ways to achieve the same functionality.

2.1. Forwarding rules

The IGMP snooping functionality is separated into a control section (IGMP forwarding) and a data section (Data forwarding).

2.1.1. IGMP Forwarding Rules

1) A snooping switch should forward IGMP Membership Reports only to those ports where multicast routers are attached.

Alternatively stated: a snooping switch should not forward IGMP Membership Reports to ports on which only hosts are attached. An administrative control may be provided to override this restriction, allowing the report messages to be flooded to other ports.

This is the main IGMP snooping functionality for the control path.

Sending membership reports to other hosts can result, for IGMPv1 and IGMPv2, in unintentionally preventing a host from joining a specific multicast group.

When an IGMPv1 or IGMPv2 host receives a membership report for a group address that it intends to join, the host will suppress its own membership report for the same group. This join or message suppression is a requirement for IGMPv1 and IGMPv2 hosts. However, if a switch does not receive a membership report from the host it will not forward multicast data to it.

This is not a problem in an IGMPv3-only network because there is no suppression of IGMP Membership reports.

The administrative control allows IGMP Membership Report messages to be processed by network monitoring equipment such as packet analyzers or port replicators.

The switch supporting IGMP snooping must maintain a list of multicast routers and the ports on which they are attached. This list can be constructed in any combination of the following ways:

- a) This list should be built by the snooping switch sending Multicast Router Solicitation messages as described in IGMP Multicast Router Discovery [[MRDISC](#)]. It may also snoop Multicast Router Advertisement messages sent by and to other nodes.
- b) The arrival port for IGMP Queries (sent by multicast routers) where the source address is not 0.0.0.0.

The 0.0.0.0 address represents a special case where the switch is proxying IGMP Queries for faster network convergence, but is not itself the Querier. The switch does not use its own IP address (even if it has one), because this would cause the Queries to be seen as coming from a newly elected Querier. The 0.0.0.0 address is used to indicate that the Query packets are NOT from a multicast router.

- c) Ports explicitly configured by management to be IGMP-forwarding ports, in addition to or instead of any of the above methods to detect router ports.
- 2) IGMP networks may also include devices that implement "proxy-reporting", in which reports received from downstream hosts are summarized and used to build internal membership states. Such proxy-reporting devices may use the all-zeros IP Source-Address when forwarding any summarized reports upstream. For this reason, IGMP membership reports received by the snooping switch must not be rejected because the source IP address is set to 0.0.0.0.
 - 3) The switch that supports IGMP snooping must flood all unrecognized IGMP messages to all other ports and must not attempt to make use of any information beyond the end of the network layer header.

In addition, earlier versions of IGMP should interpret IGMP fields as defined for their versions and must not alter these fields when forwarding the message. When generating new messages, a given

IGMP version should set fields to the appropriate values for its

own version. If any fields are reserved or otherwise undefined for a given IGMP version, the fields should be ignored when parsing the message and must be set to zeroes when new messages are generated by implementations of that IGMP version. An exception may occur if the switch is performing a spoofing function, and is aware of the settings for new or reserved fields that would be required to correctly spoof for a different IGMP version.

The reason to worry about these trivialities is that IGMPv3 overloads the old IGMP query message using the same type number (0x11) but with an extended header. Therefore there is a risk that IGMPv3 queries may be interpreted as older version queries by, for example, IGMPv2 snooping switches. This has already been reported [[IETF56](#)] and is discussed in [section 2.2](#).

- 4) An IGMP snooping switch should be aware of link layer topology changes caused by Spanning Tree operation. When a port is enabled or disabled by Spanning Tree, a General Query may be sent on all active non-router ports in order to reduce network convergence time. Non-Querier switches should be aware of whether the Querier is in IGMPv3 mode. If so, the switch should not spoof any General Queries unless it is able to send an IGMPv3 Query that adheres to the most recent information sent by the true Querier. In no case should a switch introduce a spoofed IGMPv2 Query into an IGMPv3 network, as this may create excessive network disruption.

If the switch is not the Querier, it should use the 'all-zeros' IP Source Address in these proxy queries (even though some hosts may elect to not process queries with a 0.0.0.0 IP Source Address). When such proxy queries are received, they must not be included in the Querier election process.

- 5) An IGMP snooping switch must not make use of information in IGMP packets where the IP or IGMP headers have checksum or integrity errors. The switch should not flood such packets but if it does, it should also take some note of the event (i.e., increment a counter). These errors and their processing are further discussed in [[IGMPv3](#)], [[MLD](#)] and [[MLDv2](#)].
- 6) The snooping switch must not rely exclusively on the appearance of IGMP Group Leave announcements to determine when entries should be removed from the forwarding table. It should implement a membership timeout mechanism such as the router-side functionality of the IGMP protocol as described in the IGMP and MLD specifications (See Normative Reference section for IGMPv1-3 and MLDv1-2) on all its non-router ports. This timeout value should be configurable.

2.1.2. Data Forwarding Rules

- 1) Packets with a destination IP address outside 224.0.0.X which are not IGMP should be forwarded according to group-based port membership tables and must also be forwarded on router ports.

This is the main IGMP snooping functionality for the data path. One approach that an implementation could take would be to maintain separate membership and multicast router tables in software and then "merge" these tables into a forwarding cache.

- 2) Packets with a destination IP (DIP) address in the 224.0.0.X range which are not IGMP must be forwarded on all ports.

This recommendation is based on the fact that many host systems do not send Join IP multicast addresses in this range before sending or listening to IP multicast packets. Furthermore, since the 224.0.0.X address range is defined as link-local (not to be routed), it seems unnecessary to keep the state for each address in this range. Additionally, some routers operate in the 224.0.0.X address range without issuing IGMP Joins, and these applications would break if the switch were to prune them due to not having seen a Join Group message from the router.

- 3) An unregistered packet is defined as an IPv4 multicast packet with a destination address which does not match any of the groups announced in earlier IGMP Membership Reports.

If a switch receives an unregistered packet, it must forward that packet on all ports to which an IGMP router is attached. A switch may default to forwarding unregistered packets on all ports. Switches that do not forward unregistered packets to all ports must include a configuration option to force the flooding of unregistered packets on specified ports.

In an environment where IGMPv3 hosts are mixed with snooping switches that do not yet support IGMPv3, the switch's failure to flood unregistered streams could prevent v3 hosts from receiving their traffic. Alternatively, in environments where the snooping switch supports all of the IGMP versions that are present, flooding unregistered streams may cause IGMP hosts to be overwhelmed by multicast traffic, even to the point of not receiving Queries and failing to issue new membership reports for their own groups.

It is encouraged that snooping switches at least recognize and process IGMPv3 Join Reports, even if this processing is limited to the behavior for IGMPv2 Joins, i.e., is done without considering

any additional "include source" or "exclude source" filtering. When IGMPv3 Joins are not recognized, a snooping switch may incorrectly prune off the unregistered data streams for the groups (as noted above); alternatively, it may fail to add in forwarding to any new IGMPv3 hosts if the group has previously been joined as IGMPv2 (because the data stream is seen as already having been registered).

- 4) All non-IPv4 multicast packets should continue to be flooded out to all remaining ports in the forwarding state as per normal IEEE bridging operations.

This recommendation is a result of the fact that groups made up of IPv4 hosts and IPv6 hosts are completely separate and distinct groups. As a result, information gleaned from the topology between members of an IPv4 group would not be applicable when forming the topology between members of an IPv6 group.

- 5) IGMP snooping switches may maintain forwarding tables based on either MAC addresses or IP addresses. If a switch supports both types of forwarding tables then the default behavior should be to use IP addresses. IP address based forwarding is preferred because the mapping between IP multicast addresses and link-layer multicast addresses is ambiguous. In the case of Ethernet, there is a multiplicity of 1 Ethernet address to 32 IP addresses [[RFC1112](#)].
- 6) Switches which rely on information in the IP header should verify that the IP header checksum is correct. If the checksum fails, the information in the packet must not be incorporated into the forwarding table. Further, the packet should be discarded.
- 7) When IGMPv3 "include source" and "exclude source" membership reports are received on shared segments, the switch needs to forward the superset of all received membership reports on to the shared segment. Forwarding of traffic from a particular source S to a group G must happen if at least one host on the shared segment reports an IGMPv3 membership of the type INCLUDE(G, Slist1) or EXCLUDE(G, Slist2), where S is an element of Slist1 and not an element of Slist2.

The practical implementation of the (G,S1,S2,...) based data forwarding tables are not within the scope of this document. However, one possibility is to maintain two (G,S) forwarding lists: one for the INCLUDE filter where a match of a specific (G,S) is required before forwarding will happen, and one for the EXCLUDE filter where a match of a specific (G,S) will result in no forwarding.

2.2. GMP Snooping-Related Problems

A special problem arises in networks consisting of IGMPv3 routers as well as IGMPv2 and IGMPv3 hosts interconnected by an IGMPv2 snooping switch as recently reported [[IETF56](#)]. The router will continue to maintain IGMPv3 even in the presence of IGMPv2 hosts, and thus the network will not converge on IGMPv2. But it is likely that the IGMPv2 snooping switch will not recognize or process the IGMPv3 membership reports. Groups for these unrecognized reports will then either be flooded (with all of the problems that may create for hosts in a network with a heavy multicast load) or pruned by the snooping switch.

Therefore, it is recommended that in such a network, the multicast router be configured to use IGMPv2. If this is not possible, and if the snooping switch cannot recognize and process the IGMPv3 membership reports, it is instead recommended that the switch's IGMP snooping functionality be disabled, as there is no clear solution to this problem.

3. IPv6 Considerations

In order to avoid confusion, the previous discussions have been based on the IGMP protocol which only applies to IPv4 multicast. In the case of IPv6, most of the above discussions are still valid with a few exceptions that we will describe here.

The control and data forwarding rules in the IGMP section can, with a few considerations, also be applied to MLD. This means that the basic functionality of intercepting MLD packets, and building membership lists and multicast router lists, is the same as for IGMP.

In IPv6, the data forwarding rules are more straight forward because MLD is mandated for addresses with scope 2 (link-scope) or greater. The only exception is the address FF02::1 which is the all hosts link-scope address for which MLD messages are never sent. Packets with the all hosts link-scope address should be forwarded on all ports.

MLD messages are also not sent regarding groups with addresses in the range FF00::/15 (which encompasses both the reserved FF00::/16 and node-local FF01::/16 IPv6 address spaces). These addresses should never appear in packets on the link.

Equivalent to the IPv4 behaviors regarding the null IP Source address, MLD membership reports must not be rejected by an MLD snooping switch because of an unspecified IP source address (::).

Additionally, if a non-Querier switch spoofs any General Queries (as

addressed in [Section 2.1](#) above, for Spanning Tree topology changes), the switch should use the null IP source address (::) when sending said queries. When such proxy queries are received, they must not be included in the Querier election process.

The three major differences between IPv4 and IPv6 in relation to multicast are:

- The IPv6 protocol for multicast group maintenance is called Multicast Listener Discovery [[MLDv2](#)]. MLDv2 uses ICMPv6 message types instead of IGMP message types.
- The RFCs [[IPV6-ETHER](#)] and [[IPV6-FDDI](#)] describe how 32 of the 128 bit DIP addresses are used to form the 48 bit DMAC addresses for multicast groups, while [[IPV6-TOKEN](#)] describes the mapping for token ring DMAC addresses by using three low-order bits. The specification [[IPV6-1394](#)] makes use of a 6 bit channel number.
- Multicast router discovery is accomplished using the Multicast Router Discovery Protocol (MRDISC) defined in [[MRDISC](#)].

The IPv6 packet header does not include a checksum field. Nevertheless, the switch should detect other packet integrity issues such as address version and payload length consistencies if possible. When the snooping switch detects such an error, it must not include information from the corresponding packet in the MLD forwarding table. The forwarding code should instead drop the packet and take further reasonable actions as advocated above.

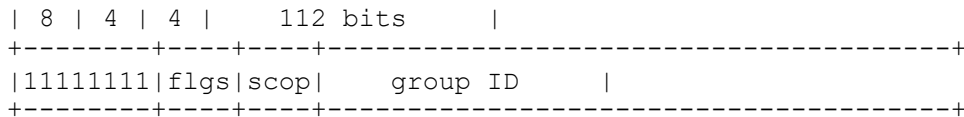
The fact that MLDv2 is using ICMPv6 adds new requirements to a snooping switch because ICMPv6 has multiple uses aside from MLD. This means that it is no longer sufficient to detect that the next-header field of the IP header is ICMPv6 in order to identify packets relevant for MLD snooping. A software-based implementation which treats all ICMPv6 packets as candidates for MLD snooping could easily fill its receive queue and bog down the CPU with irrelevant packets. This would prevent the snooping functionality from performing its intended purpose and the non-MLD packets destined for other hosts could be lost.

A solution is either to require that the snooping switch looks further into the packets, or to be able to detect a multicast DMAC address in conjunction with ICMPv6. The first solution is desirable when a configuration option allows the administrator to specify which ICMPv6 message types should trigger a CPU redirect and which should not. The reason is that a hardcoding of message types is inflexible for the introduction of new message types. The second solution introduces the risk that new protocols that use ICMPv6 and multicast

DMAC addresses could be incorrectly identified as MLD. It is suggested that solution one is preferred when the configuration option is provided. If this is not the case, then the implementor should seriously consider making it available since Neighbor Discovery messages would be among those that fall into this false positive case and are vital for the operational integrity of IPv6 networks.

The mapping from IP multicast addresses to multicast DMAC addresses introduces a potentially enormous overlap. The structure of an IPv6 multicast address is shown in the figure below. As a result, there are 2^{112-32} , or more than $1.2e24$ unique DIP addresses which map into a single DMAC address in Ethernet and FDDI. This should be compared to 2^5 in the case of IPv4.

Initial allocation of IPv6 multicast addresses, as described in [\[RFC3307\]](#), however, cover only the lower 32 bits of group ID. While this reduces the problem of address ambiguity to group IDs with different flag and scope values for now, it should be noted that the allocation policy may change in the future. Because of the potential overlap it is recommended that IPv6 address based forwarding is preferred to MAC address based forwarding.



4. IGMP Questionnaire

As part of this work, the following questions were asked on the MAGMA discussion list and were sent to known switch vendors implementing IGMP snooping. The individual contributions have been anonymized upon request and do not necessarily apply to all of the vendors' products.

The questions were:

Q1 Do your switches perform IGMP Join aggregation? In other words, are IGMP joins intercepted, absorbed by the hardware/software so that only one Join is forwarded to the querier?

Q2 Is multicast forwarding based on MAC addresses? Would datagrams addressed to multicast IP addresses 224.1.2.3 and 239.129.2.3 be forwarded on the same ports-groups?

[RFC 4541](#) IGMP and MLD Snooping Switches Considerations May 2006

Q3 Is it possible to forward multicast datagrams based on IP addresses (not routed)? In other words, could 224.1.2.3 and 239.129.2.3 be forwarded on different port-groups with unaltered TTL?

Q4 Are multicast datagrams within the range 224.0.0.1 to 224.0.0.255 forwarded on all ports whether or not IGMP Joins have been sent?

Q5 Are multicast frames within the MAC address range 01:00:5E:00:00:01 to 01:00:5E:00:00:FF forwarded on all ports whether or not IGMP joins have been sent?

Q6 Does your switch support forwarding to ports on which IP multicast routers are attached in addition to the ports where IGMP Joins have been received?

Q7 Is your IGMP snooping functionality fully implemented in hardware?

Q8 Is your IGMP snooping functionality partly software implemented?

Q9 Can topology changes (for example spanning tree configuration changes) be detected by the IGMP snooping functionality so that for example new queries can be sent or tables can be updated to ensure robustness?

The answers were:

```

-----+-----+-----+-----+-----+-----+
| Switch Vendor |
-----+-----+-----+-----+-----+
| 1 | 2 | 3 | 4 | 5 | 6 |
-----+-----+-----+-----+-----+
Q1 Join aggregation | x | x | x | | x | x |
Q2 Layer-2 forwarding | x | x | x | x | (1) | |
Q3 Layer-3 forwarding | (1) | | (1) | | (1) | x |
Q4 224.0.0.X aware | (1) | x | (1) | (2) | x | x |
Q5 01:00:5e:00:00:XX aware | x | x | x | (2) | x | x |
Q6 Mcast router list | x | x | x | x | x | x |
Q7 Hardware implemented | | | | | |
Q8 Software assisted | x | x | x | x | x | x |
Q9 Topology change aware | x | x | x | x | | (2) |
-----+-----+-----+-----+-----+

```

x Means that the answer was Yes.

(1) In some products (typically high-end) Yes; in others No.

(2) Not at the time that the questionnaire was received but expected in the near future.

5. References

5.1. Normative References

- [BRIDGE] IEEE Std. 802.1D-2004 IEEE Standard for Local and metropolitan area networks, Media Access Control (MAC) Bridges
- [IGMPv3] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", [RFC 3376](#), October 2002.
- [IPV6-1394] Fujisawa, K. and A. Onoe, "Transmission of IPv6 Packets over IEEE 1394 Networks", [RFC 3146](#), October 2001.
- [IPV6-ETHER] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", [RFC 2464](#), December 1998.
- [IPV6-FDDI] Crawford, M., "Transmission of IPv6 Packets over FDDI Networks", [RFC 2467](#), December 1998.
- [IPV6-TOKEN] Crawford, M., Narten, T., and S. Thomas, "Transmission of IPv6 Packets over Token Ring Networks", [RFC 2470](#), December 1998.
- [MLD] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", [RFC 2710](#), October 1999.
- [MLDv2] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", [RFC 3810](#), June 2004.
- [MRDISC] Haberman, B. and J. Martin, "Multicast Router Discovery", [RFC 4286](#), December 2005.
- [RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, [RFC 1112](#), August 1989.
- [RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", [RFC 2236](#), November 1997.
- [RFC3307] Haberman, B., "Allocation Guidelines for IPv6 Multicast Addresses", [RFC 3307](#), August 2002.

5.2. Informative References

- [CISCO] Cisco Tech Notes, "Multicast In a Campus Network: CGMP and IGMP snooping",
<http://www.cisco.com/warp/public/473/22.html>
- [IETF56] Briefing by Dave Thaler, Microsoft, presented to the MAGMA WG at the 56'th IETF meeting in San Francisco,
<http://www.ietf.org/proceedings/03mar/index.html>
- [MSOFT] Microsoft support article Q223136, "Some LAN Switches with IGMP Snooping Stop Forwarding Multicast Packets on RRAS Startup", <http://support.microsoft.com/support/articles/Q223/1/36.ASP>

6. Security Considerations

Under normal network operation, the snooping switch is expected to improve overall network performance by limiting the scope of multicast flooding to a smaller portion of the local network. In the event of forged IGMP messages, the benefits of using a snooping switch might be reduced or eliminated.

Security considerations for IGMPv3 at the network layer of the protocol stack are described in [[IGMPv3](#)]. The introduction of IGMP snooping functionality does not alter the handling of multicast packets by the router as it does not make use of link layer information.

There are, however, changes in the way that the IGMP snooping switch handles multicast packets within the local network. In particular:

- A Query message with a forged source address which is less than that of the current Querier could cause snooping switches to forward subsequent Membership reports to the wrong network interface. It is for this reason that IGMP Membership Reports should be sent to all multicast routers as well as the current Querier.
- It is possible for a host on the local network to generate Current-State Report Messages that would cause the switch to incorrectly believe that there is a multicast listener on the same network segment as the originator of the forged message. This will cause unrequested multicast packets to be forwarded into the network segments between the source and the router. If the router

requires that all Multicast Report messages be authenticated as described in [section 9.4](#) of [[IGMPv3](#)], it will discard the forged Report message from the host inside the network in the same way

Christensen, et al. Informational [Page 13]

[RFC 4541](#) IGMP and MLD Snooping Switches Considerations May 2006

that it would discard one which originates from a remote location. It is worth noting that if the router accepts unauthenticated Report messages by virtue of them having arrived over a network interface associated with the internal network, investigating the affected network segments will quickly narrow the search for the source of the forged messages.

-As noted in [[IGMPv3](#)], there is little motivation for an attacker to forge a Membership report message since joining a group is generally an unprivileged operation. The sender of the forged Membership report will be the only recipient of the multicast traffic to that group. This is in contrast to a shared LAN segment (HUB) or network without snooping switches, where all other hosts on the same segment would be unable to transmit when the network segment is flooding the unwanted traffic.

The worst case result for each attack would remove the performance improvements that the snooping functionality would otherwise provide. It would, however, be no worse than that experienced on a network with switches that do not perform multicast snooping.

7. Acknowledgements

We would like to thank Martin Bak, Les Bell, Yiqun Cai, Ben Carter, Paul Congdon, Toerless Eckert, Bill Fenner, Brian Haberman, Edward Hilquist, Hugh Holbrook, Kevin Humphries, Isidor Kouvelas, Pekka Savola, Suzuki Shinsuke, Jaff Thomas, Rolland Vida, and Margaret Wasserman for comments and suggestions on this document.

Furthermore, the following companies are acknowledged for their contributions: 3Com, Alcatel, Cisco Systems, Enterasys Networks, Hewlett-Packard, Vitesse Semiconductor Corporation, Thrane & Thrane. The ordering of these names do not necessarily correspond to the column numbers in the response table.

Christensen, et al. Informational [Page 14]

[RFC 4541](#) IGMP and MLD Snooping Switches Considerations May 2006

Authors' Addresses

Morten Jagd Christensen
Thrane & Thrane
Lundtoftegaardsvej 93 D
2800 Lyngby
DENMARK

E-Mail: mjc@tt.dk

Karen Kimball
Hewlett-
Packard
8000 Foothills Blvd.
Roseville, CA 95747
USA

E-Mail: karen.kimball@hp.com

Frank Solensky
Calix
43 Nanog Park
Acton, MA 01720
USA

E-Mail: frank.solensky@calix.com