

AMX AV/IT Administrators Guide

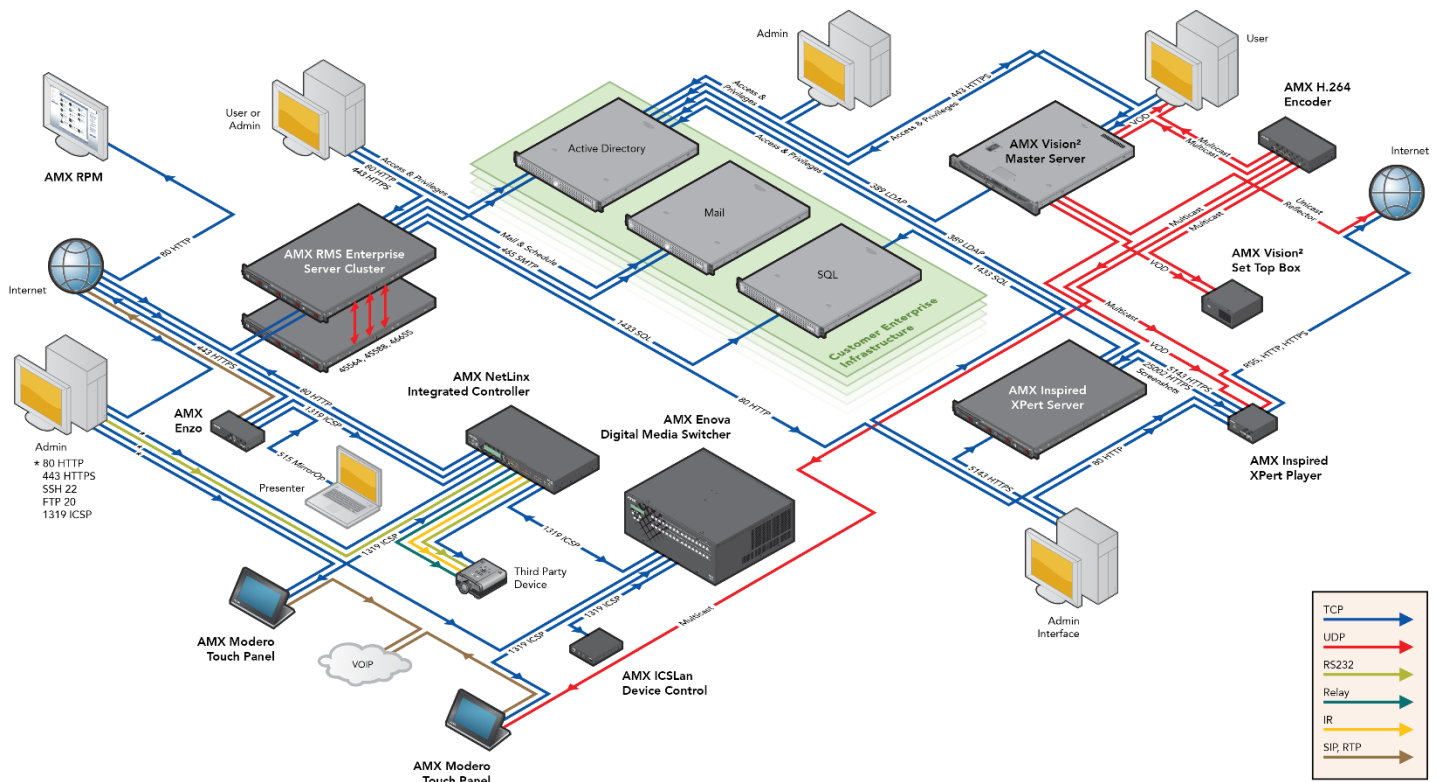


This document provides a technical overview of equipment and protocols encountered when implementing AMX products on the Enterprise Network. The goal of this document is to help AV/IT administrators during the buying process as they assess the network impact of integrating AMX equipment.

Contents

AMX Network Products	1
Central Controllers	1
Touch Panels	2
Media	2
Management.....	2
Network Environment.....	3
Physical Network requirements.....	3
DXLink vs. Ethernet	3
Wireless.....	3
Logical Network Topology.....	3
VLAN.....	3
Addressing requirements.....	4
Security	5
Ports and Services	5
Firewalls	5
Access Control.....	5
Passwords	7
Security Modes	8
Central Controller	8
Touch Panel.....	9
Control over IP	10
Internet Control System Protocol (ICSP).....	11
Device Addressing.....	11
Ethernet Transport of ICSP	12
Central Controller to Device connections.....	13
Communication Protocols and Network Impact	14
Central Controller to Central Controller connections.....	15
Central Controller to Central Controller Topology	16
Dual Network Interfaces (NICs)	17
Media	18
Digital Signage.....	18

Network Impact	18
Video Management and Distribution	19
Vision2.....	19
Video Streaming on IP Networks	20
Multicast on enterprise networks.....	21
Multicast Example.....	21
IGMP	22
IGMP Snooping	23
PIM.....	23
PIM Sparse Mode (PIM-SM).....	24
Storm Control.....	25
Management.....	25
RMS Enterprise	25
Scheduler	26
Network Impacts.....	26
Appendix A Ports and Protocols	27
Appendix B Default Values for AMX Products	32
Appendix C Operating systems	36



AMX Network Products

AMX hardware and software solutions simplify the way people interact with technology. With the increasing number of technologies and operating platforms at work and home, AMX solves the complexity of managing this technology with reliable, consistent and scalable systems. Our award-winning products span control and automation, system-wide switching and audio/video signal distribution, as well as digital signage and technology management. They are implemented worldwide in conference rooms, homes, classrooms, network operation and command centers, hotels, entertainment venues and broadcast facilities, among others

AMX manufactures a wide variety of devices designed to be implemented on IP networks including control systems, management systems, video transport devices and presentation systems.

Central Controllers

AMX Central Controllers are the brain of an integrated AV system. They contain the central programming required to control a variety of devices through any control interface including IP, RS-232, RS-422, RS-485, IR, Relay, Digital I/O, and Analog control as well control of almost any interface through adapters.

Central Controllers are available with a variety of control interfaces built into the controller or interfaces may be connected through ICSLan devices over IP. The Enova DVX and Enova DGX series switchers include a built in Central Controller within the chassis. In all cases the Central controller is a separate logical device from the interfaces or switches.

Touch Panels

AMX Touch Panels are multifunction devices on the network. In addition to the primary function as a control surface for the AV control system they have multiple other functions such as a video streaming display, status monitor, scheduling interface, SIP telephony endpoint, VNC host/client, and Audio/Video Intercom. The new G5 series of touch panels have the ability to run web apps including browsing and videoconferencing.

Media

Vision2 is a sophisticated, fully-integrated video capture, management, and broadcast system for organizations and homeowners wanting a comprehensive, yet simple-to-use, IP video delivery solution. Vision2 offers live, scheduled, or on-demand video, all managed from a convenient web interface. Through the web interface, you can perform the following:

- Capture and encode content
- Upload, archive, manage, and publish content
- Schedule programming
- Broadcast at selectable bitrate to any platform
- Provide live TV and video on-demand over Intranet to PCs and Set-top boxes attached to displays
- Provide video on-demand to supported tablets

Management

AMX's Resource Management Suite (RMS) is designed for any integrated spaces where IT, AV and facilities managers can benefit from a centralized remote management tool. By bringing together what have traditionally been discreet systems into a single management environment it provides real-time monitoring, device management, user behavior and energy utilization analytics. Utilizing this same communication infrastructure it also provides a central integration point for communication with external services such as scheduling systems and SNMP monitoring.

Rapid Project Maker (RPM) is a free cloud-based application which allows for semi-custom integration of AMX control systems without the expense of custom programming. From a web interface, RPM steps you through the process of configuring the control system to your specific equipment and application. RPM then generates the program files for the controller and user interfaces as well installation documentation including all cabling connections. Once you are happy with the design everything can be downloaded for transfer to the AMX AV system. No internet connectivity to the AV system is ever required. Configurations are stored on the cloud for easy configuration management which allows for moves, additions, and changes to be quickly implemented, just by modifying the existing project to the new feature. When new rooms are implemented in RPM, RMS code is automatically implemented to

bring the room into management. More information and account signup is available at <http://www.amxrpm.com>.

Network Environment

Physical Network requirements

AMX AV and control equipment is designed to use the same switched Ethernet infrastructure as other IT equipment. Considerations for bandwidth, VLANs, IP addressing scheme and PoE will be based on the actual equipment and scope of the project as in any other IT installation. Most AMX devices have 10/100BaseT ports and are compliant with the IEEE 802.3 100BASE-T specification. The units, by default, enters auto-negotiate mode, which automatically detects and configures itself for operation on the network to which it's connected. It is possible to force the mode of operation (10Mbps half, 10Mbps full, 100Mbps half, or 100Mbps full) via software configuration. **Some AMX devices have DXLink connections which are not directly connectable to an Ethernet switch.**

DXLink vs. Ethernet

In some cases audio, video, network and control may be transported over DXLink. Although this is using the same Cat6 cable as Ethernet and 100Mbps Ethernet can be tunneled through the cable along with the other signals it is not Ethernet and never attaches directly to a switch or router. Equipment that is connected over DXLink may also have an Ethernet jack for convenience in extending the control network. DXLink products do not support Spanning Tree so only one connection to a LAN is permitted within a switching system with DXLink support.

Wireless

AMX wireless touch panel are mobile devices that communicate with a NetLinx Central Controller via a standard 802.11a/b/g Wireless Access Point. They support both simple and enterprise security modes including password or certificate based authentication.

In a small system the control system can connect to a standalone access point, but in an enterprise with managed wireless the best practice would be to assign a separate AV SSID routed to the AV subnet. Using the existing engineered wireless plan and infrastructure will ensure that there is no RF interference that could be caused by a separate Wireless Access Point.

Logical Network Topology

VLAN

Best practices dictate that AV equipment be separated from other network traffic. There are several key strategies in segmenting traffic which drives this separation. The strategies and justification for separating AV into a separate VLAN(s) follow.

- Group devices by traffic patterns
 - AMX equipment communicates primarily among the AV devices with limited connectivity to the data network.

- Group devices for security and safety
 - There are limited valid reasons for remote access to the AMX equipment and the equipment controls potentially sensitive meetings.
 - AMX systems may control physical environments like projector lifts and lighting. Improper remote access could be a safety issue.
- Group devices by traffic types
 - AMX devices primarily communicate between each other using ICSP over IP.
 - There is significant broadcast traffic between AMX devices
- Group devices geographically
 - In a campus setting, which may have multiple VLANs due to LAN topology requirements, routing should be enabled between the control VLANs

AV Devices not on the control VLAN

- In the case of devices with network connections that utilize the Ethernet connection for both control and media, such as a VTC Codec or streaming encoder/decoder, the device should reside on the VLAN that makes the most sense for the media, but a static route should be set to the control network with an ACL to allow for traffic.
- In the case of a management system such as RMS, the best practice would be to have the RMS Server reside on the data network with a static route set to the control network with an access control list (ACL) to allow for traffic to and from RMS.

Addressing requirements

AMX equipment supports DHCP and Static addressing with one IP address per device. AMX Central Controllers do not act as a DHCP server.

Touch Panels and other peripheral devices register (bind) to the Central Controller so they need a constant unique reference to the Central Controller.

- This can be an IP address, either static or issued from a DHCP reservation. If DHCP without a reservation is used then an alternative ID is used, DNS name, MAC address, or system number.
- If MAC address or System Number is used then the Central Controller is required to send out a Netlinx Discovery Protocol (NDP) Broadcast to let the peripherals know the IP address of the Central Controller.
 - MAC address and system number binding require the peripherals to be on the same subnet as the Central Controller.
- If DNS Binding is used then the DHCP server must support Option 81 DHCP host name update, or static address assignments must be configured.

Touch Panels and other peripheral do not require a static IP address and can be configured with DHCP.

- If advanced features of the touch panel are used such as VNC for virtual Touch Panel interfaces then there may be an advantage to using a Static IP address or DNS records.

More information on binding requirements and impact is available in the Central Controller to Device connections section of this document.

Security

Ports and Services

The AMX Central Controller features a number of standard services which are on by default. These services can be individually disabled. The port assignments can be changed for all these services except FTP. Assigning security profiles will disable some services. A complete list of Ports and Protocols used across AMX Ethernet enabled products is in Appendix A.

Common Ports and Protocols Used (See Appendix A):	
Telnet	Port 23
ICSP	Port 1319
HTTP	Port 80
HTTPS	Port 443
SSH	Port 22
FTP	Port 21

Firewalls

AMX control systems are not required to have internet access to function. There are advanced applications which may require internet access. For example;

- RMS Enterprise Hosted Cloud Service which will require a HTTP access to the hosted service
- Individual applications on products such as digital signage which require access to external content sources such as XML or RSS feeds.
- TPControl app for mobile devices

RMS Enterprise Hosted Cloud Service and applications which require external content will always initiate a data exchange from inside the firewall. External control such as the TPControl app requires an externally routable IP address on the Central Controller on port 1319. Ports and protocols for all standard data communications on AMX products are found in Appendix A.

Access Control

AMX Central Controllers allow for multiple user accounts. These accounts should be set up using the least privilege strategy. This means that privileges are not granted unless necessary and not used unless intended. The requirement to use role based access control helps to reduce the complexity and potential errors associated with privileged account maintenance. Accounts may be created individually on each Central Controller or centrally in an LDAP Server. For more information on access control see <http://www.amx.com/assets/manuals/NetLinxControllers.WebConsole-ProgrammingGuide.FMv4.pdf>.

AMX Central Controller security allows the Administrator to define access rights for users or groups. A user represents a single potential client of the system while a group represents a logical collection of

users. Any properties possessed by groups (i.e., access rights, directory associations, etc.) are inherited by all the members of the group.

The following table lists the features the Administrator may grant or deny access to:

System Security Features:	
Central Controller Security Configuration	Access to the security configuration command of the Enova DVX central controller (Central Controller). Only those users with security configuration access rights granted will have access to the security configuration commands.
Telnet Security	Access to the device's Telnet interface. All basic commands are available to the user.
Terminal (RS-232) Security	Access to the Terminal Interface (Program Port) functionality through the RS-232 connector. All basic commands are available to the Site Administrator.
HTTP (Web Server) Security	Access to the HTTP server functionality. Directory associations assign specific directories/files to a particular user.
FTP Security	Access to the FTP server functionality. Only the Administrator account has access to the root directory; all other 'qualified' clients are restricted to the /user/ directory and its 'tree.'
ICSP	Access to the ICSP communication functionality. Communication and encryption rights are available to an authorized user.
ICSP Encryption	The access to the ICSP data encryption functionality. Enabling encryption of ICSP data requires that both: <ul style="list-style-type: none"> • AMX hardware or software communicating with the target Enova DVX central controller (Central Controller) provide a valid username and password. • All communication is encrypted.

In a typical secure setup there will be 3 User Groups

1. Super Admin
 - a. All Admin rights including password and configuration changes
 - 1) Terminal <RS232> Access Enabled
 - 2) Admin Change Password Access..... Enabled
 - 3) FTP Access Optional
 - 4) HTTP Access Optional
 - 5) Telnet/SSH/SFTP Access Optional
 - 6) Configuration Access Enabled
 - 7) ICSP Access..... Enabled
 - 8) ICSP Encryption Required Optional
2. Log Admin
 - a. Able to view system settings and access logs
 - 1) Terminal <RS232> Access Enabled
 - 2) Admin Change Password Access..... Disabled
 - 3) FTP Access..... Disabled
 - 4) HTTP Access Disabled
 - 5) Telnet/SSH/SFTP Access Disabled
 - 6) Configuration Access Disabled
 - 7) ICSP Access..... Disabled
 - 8) ICSP Encryption Required Optional
3. Touch Panel / ICSLan device
 - a. Each Touch Panel or ICSLan device should have a separate user account
 - b. User setup for touch panel control
 - 1) Terminal <RS232> Access Disabled
 - 2) Admin Change Password Access..... Disabled
 - 3) FTP Access..... Disabled
 - 4) HTTP Access Disabled
 - 5) Telnet/SSH/SFTP Access Disabled
 - 6) Configuration Access Disabled
 - 7) ICSP Access..... Enabled
 - 8) ICSP Encryption Required Enabled

Passwords

AMX components ship with well-known default passwords. Passwords should be changed from the default.

Default Passwords and settings are listed in Appendix B

Security Modes

Central Controller

By default the AMX controller and Touch Panels are in an unsecured mode allowing Telnet and http access.

There are three levels of security for the Enova DVX; Low, Medium, and High. The features for each mode are described as follows:

- Low Security Mode:
 - Factory default, shipped in this configuration.
 - Administrator and User accounts have a default password of “password.”
 - Telnet, HTTP, HTTPS, SSH are all enabled and require no authentication.
 - ‘Program Ports’ terminal configuration access requires no authentication.
 - ICSP communication protocol between devices: encryption and authentication are disabled.
 - FTP is enabled.
 - Minimum password requirements are 8 characters.
- Medium Security Mode:
 - Provisioning is done through a terminal session from an on-site workstation that is connected with an RS-232 cable to the ‘Program Port’ on the Enova DVX.
 - Site Administrator password is default to “Amx1234!”
 - HTTP, Telnet, and FTP are disabled.
 - SSH, HTTPS, and accessing the ‘Program Port’ for a terminal session requires authentication by the Site Administrator.
 - SSH, HTTPS, and terminal session timeouts are enabled.
 - ICSP communication protocol between devices has encryption and authentication enabled.
 - Minimum password requirement is 15 characters such that:
 - The password contains at least one uppercase alphabetic character.
 - The password contains at least one lowercase alphabetic character.
 - The password contains at least one numeric character.
 - The password contains at least one special character.
 - The password does not contain more than three consecutive repeating characters.
 - Login failure attempt pauses 4 seconds before another login attempt is allowed.

- After three consecutive unsuccessful login attempts, login lockout is enabled for 10 minutes.
- Login and logout audit logging is enabled.
- All existing user accounts are deleted to ensure password conformity.
- High Security Mode:
 - Provisioning is done through a terminal session from an on-site workstation that is connected with an RS-232 cable to the 'Program Port' on the Enova DVX.
 - Site Administrator password is default to "Amx1234!"
 - HTTP, Telnet, SSH, HTTPS, and FTP are disabled.
 - ICSP communication protocol between devices has encryption and authentication enabled.

The AMX Central Controller security allows the Site Administrator to define access rights for users or groups. A user represents a single potential client of the system while a group represents a logical collection of users. Any properties possessed by groups (i.e., access rights, directory associations, etc.) are inherited by all the members of the group.

Touch Panel

There are three levels of security for the Modero X Touch Panel; Low, Medium, and High. The feature set for each mode is described as follows:

- Low Security Mode:
 - Factory default, shipped in this configuration.
 - Administrator and User accounts have a default password of "1988."
 - Telnet and G4 web control are all enabled and require no authentication.
 - Telnet session timeouts are enabled.
 - Minimum password requirements are 8 characters.
- Medium Security Mode:
 - Provisioning is done through a protected setup page on the Modero X touch panel.
 - Site Administrator password is default to "Amx1234!"
 - Telnet is disabled.
 - Remote access via SSH requires authentication by the Site Administrator (SSH username is 'amx.')
 - SSH session timeouts are enabled.
 - G4 Web Control is disabled.
 - Minimum password requirement is 15 characters such that:
 - The password contains at least one uppercase alphabetic character.

- The password contains at least one lowercase alphabetic character.
- The password contains at least one numeric character.
- The password contains at least one special character.
- The password does not contain more than three consecutive repeating characters.
- Login failure attempt pauses 4 seconds before another login attempt is allowed.
- After three consecutive unsuccessful login attempts, login lockout is enabled for 10 minutes.
- Login and logout audit logging is enabled.
- High Security Mode:
 - Provisioning is done through a protected setup page on the Modero X touch panel.
 - Site Administrator password is default to “Amx1234!”
 - Telnet and SSH are disabled.
 - SSH is disabled through a manual process.
 - G4 Web Control is disabled
 - Minimum password requirement is 15 characters such that:
 - The password contains at least on uppercase alphabetic character.
 - The password contains at least one lowercase alphabetic character.
 - The password contains at least one numeric character.
 - The password contains at least one special character.
 - The password does not contain more than three consecutive repeating characters.
 - Login failure attempt pauses 4 seconds before another login attempt is allowed.
 - After three consecutive unsuccessful login attempts, login lockout is enabled for 10 minutes.
 - Login and logout audit logging is enabled.

Control over IP

From a control perspective there are two classes of logical AMX devices, Central Controllers and devices. Central Controllers run the software and control communications. Devices are the interfaces to the equipment being controlled. A Central Controller will generally have devices within the same chassis, but they are logically treated separately from the Central Controller.

AMX uses several standard protocols which are well documented elsewhere. AMX’s proprietary Internet Control System Protocol (ICSP) and its methodologies will be discussed here.

Internet Control System Protocol (ICSP)

AMX devices communicate with each other using a proprietary low level protocol called Internet Control System Protocol (ICSP). This protocol can be carried over the Ethernet TCP/IP connection, RS232 PPP connection, and ICSNet connection to devices. ICSP is routable within AMX devices independent of transport medium. Each ICSP client device is logically bound to a single Central Controller. If a second Central Controller need to communicate with a client device the ICSP communication is sent to the Central Controller the device is bound to and it is relayed to the client device through a Central Controller to Central Controller (M2M) connection.

ICSP may also be encrypted where required by the environment. Encrypted ICSP uses a Challenge-Handshake Authentication Protocol (CHAP) with a three way handshake using the MD5 hash algorithm. The encryption is ARC4 with a commonly derived key, with no key information is passed between the hosts. The entire ICSP packet, including headers, is encrypted and the resulting data encapsulated in a new eICSP packet.

Device Addressing

Each ICSP Device, regardless of transport type is addressed with a unique combination of System and Device with sub-addresses within Devices termed Ports. Addressing is specified as Device:Port:System (D:P:S)

System ID is associated with a logical Central Controller (1 Central Controller per System ID). Valid System numbers are 1 to 65535 and are unique within the network. System 0 is a wildcard referring to the local system

Device Number is bound to a single Central Controller (multiple Devices per Central Controller). Device numbers are unique within the System they are bound to. There is a limit of 200 devices bound to a single controller. Many devices have range limitations on the device number that may be used. If an incorrect device number outside of that range is assigned to a particular device, the module may not function properly.

Physical Device Numbers	
1-32000	Physical Devices
1-255	Access or AxLink devices
5001	Traditional device number for the NetLinx Integrated Device
5002	Traditional device number for the NetLinx Integrated Switcher
6001-6999	Traditional device numbers for ICSNet and ICSLan devices, including DXLink TX and RXs
10001-32000	Touch panels

Dynamically Assigned Device Numbers	
32001-32767	Dynamically assigned device numbers

Virtual Device Numbers	
32768-42000	Virtual Devices
32768-36964	User defined virtual devices
36865-37864	Dynamic Virtual Devices
37865-40999	NetLinx Module Virtual Devices
41000-42000	Duet Module Virtual Devices

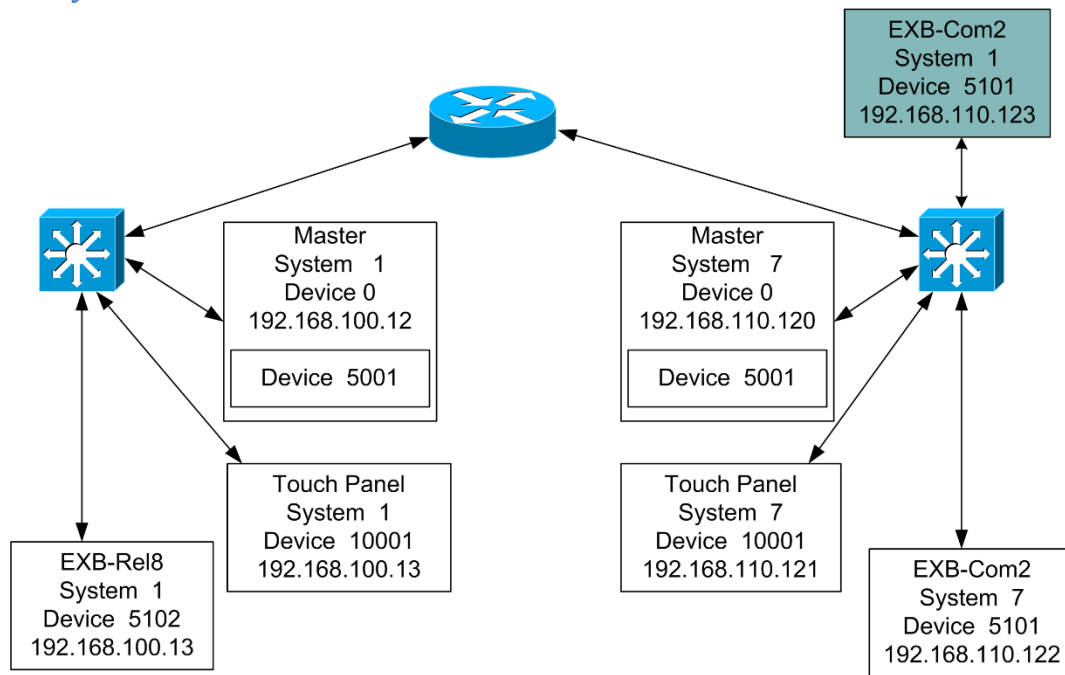
Ports are interfaces within a device (multiple ports per device) The number of ports depends on the device.

Ethernet Transport of ICSP

In Ethernet transport ICSP packets are encapsulated in the data payload and forwarded from and to port 1319. All ICSP packets are forwarded over IP based on the ICSP Routing table. At each ICSP hop point the ICSP packet is completely de-encapsulated and forwarded. No previous IP information (header, source, etc.) is forwarded with the ICSP packet.

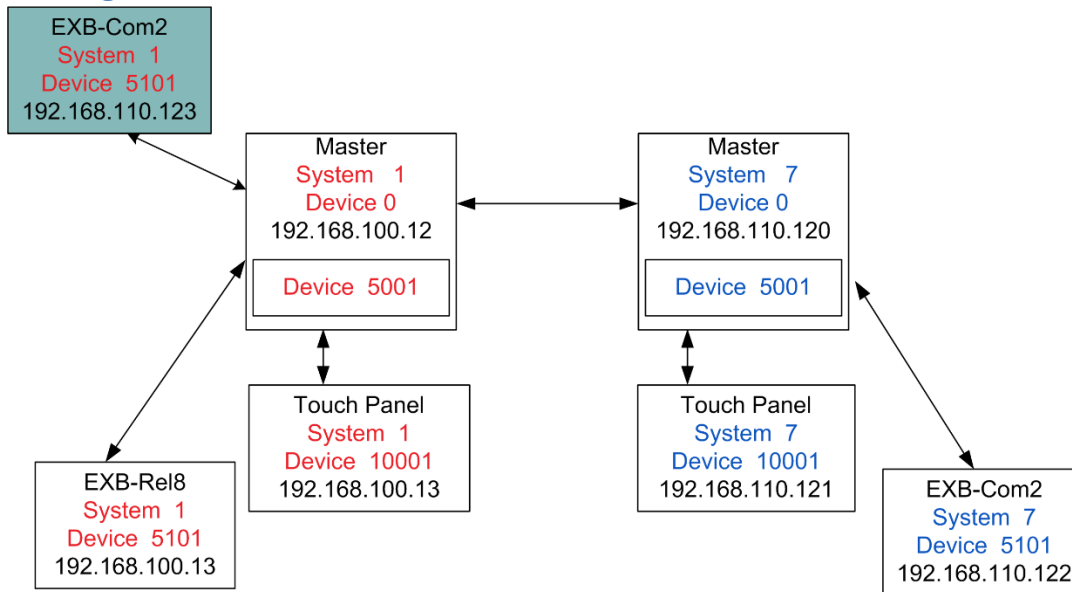
ICSP packets tunneled over Ethernet may follow a logical topology different from the physical topology. In the diagrams below the highlighted EXB-Com2 is on the same subnet as the System #7 Central Controller, but is logically bound to the System #1 Central Controller. Communication from the System #7 Central Controller to the EXB-Com2 D:P:S (5101:1:1) will travel from the System #7 Central Controller to the System #1 Central Controller and then will be forwarded to the EXB-Com2

Ethernet Physical Connection



Ethernet Physical Connection

ICSP Logical Connection



ICSP Logical Connection

Central Controller to Device connections

AMX Devices other than Touch Panels are logically bound to an individual Central Controller in one of four modes. The type of binding used will depend on network topology, IP address distribution strategy, and DNS local host resolution

Binding Type	Central Controller Unique Identification	Central Controller Address distribution	Notes
NDP	MAC Address	DHCP or Static	Must be on same Subnet NDP Broadcast must be enabled on Central Controller
UDP/URL	IP Address	Static or DHCP/DNS	For use on AMX only Networks DHCP must use DNS
TCP/URL	IP Address	Static or DHCP/DNS	For use on Mixed AMX and Data Networks DHCP must use DNS
Auto	System Number	DHCP or Static	Must be on same Subnet System Numbers must be unique to Central Controller NDP Broadcast must be enabled on Central Controller

Touch Panels have the following binding options:

Binding Type	Unique Identification	Central Controller Address distribution	Notes
URL	Central Controller IP Address	Static or DHCP/DNS	For use on Mixed AMX and Data Networks DHCP must use DNS
Listen	Touch Panel IP Address (entered in Central Controller URL List)	Static or DHCP/DNS	For use on Mixed AMX and Data Networks DHCP must use DNS
Auto	System Number	DHCP or Static	Must be on same Subnet System Numbers must be unique to Central Controller NDP Broadcast must be enabled on Central Controller

Discovery of devices by the Central Controller is the responsibility of the device itself—it must report itself to the Central Controller. The Central Controller does not “poll” for new devices. The process of “reporting” simply involves sending a Device Info message to the Central Controller. Once the Device Info message is received by the Central Controller an ACK message is generated back to the sending device for confirmation.

If the “reporting” device does not receive an ACK from the Central Controller, it will continue to send Device Info messages to the Central Controller periodically in an attempt to establish a connection. The periodic rate at which Device Info messages are sent is somewhat medium dependent, however, ICSNet devices generate Device Info messages at random intervals between one and three seconds.

Communication Protocols and Network Impact

AMX AV control systems generate a variety of messages. Typically the packets are small

NDP Broadcast: If NDP Broadcast is enabled, the Central Controller periodically transmits a multicast on 239.255.250.251 with source and destination port 1319. This is required for NDP binding.

ICSP Blink: The NetLinx Central Controller generates a UDP broadcast message, with source and destination port 1319, every five seconds. The ICSP Blink is used as a Central Controller beacon in auto device binding. It cannot be disabled. The large quantity of broadcast traffic incurred with multiple devices is a prime justification for a separate AV VLAN.

ICSP Keep alive: The Central Controller ensures that devices are still on-line by communicating with them periodically. The periodic rate is five seconds. This communication can take the form

of any ICSP message that is specifically directed to/from that device (i.e. this does not include broadcast messages).

For most devices the amount of ICSP communication is minimal and only occurs in response to user input-which is, relatively speaking, very infrequent. During these quiescent times, the Central Controller will generate a keepalive Request every five seconds to determine if the device is still on-line. The device must respond to keepalive requests with a keepalive response messages. The Central Controller sends a 29 byte TCP or UDP unicast message, depending on binding, with source and destination port 1319, to each bound device every 5 seconds. Devices respond with a 40 byte message.

Zero Config: If the Central Controller does not have an IP address that is assigned to it, then zero configuration networking uses link-local addressing to create an IP address in a range from 169.254.1.0 to 169.254.254.25. When an IP address is chosen, the link-local process sends out a query with that IP address onto the network to check whether the IP address is already in use. If there is no response, the IP address is then assigned to the Central Controller. This can be disabled

NetLinx Events: An "event" in NetLinx is defined as a button press on a user interface, a level value change, or other control message. By their nature, control messages are relatively short and infrequent. For example, a button press message is 33 bytes long...for each button press event there is a corresponding button release event that occurs (also 33 bytes long). An event is a unicast message in either direction between a device and the Central Controller with source and destination port 1319.

Other Protocol Messages: Network packets may come from other application protocols. HTTP, FTP, and Telnet protocols are well understood and the full implications, with respect to network utilization, of their usage are not covered by this document. However, they require interaction with a user and, therefore, their network utilization is very sporadic.

Central Controller to Central Controller connections

In an enterprise system it is often desirable to have control of remote devices bound to other Central Controllers. AMX facilitates this through Central Controller to Central Controller (CC2CC) communications. This is sometimes called "Master to Master (M2M)" communications referring to legacy devices.

By design, all NetLinx Central Controllers do not automatically make a CC2CC connection with other NetLinx Central Controllers by virtue of being on the same network. The connection between them must be made intentionally by adding them to a list. This connection list is called the "URL List". The URL List can have a maximum of 250 connections. The URL List on the NetLinx Central Controller is used to force the Central Controller to initiate a TCP connection to the specified URL/IP address. Therefore, the first step in assembling a CC2CC system is to set unique system numbers on each Central Controller. Valid system numbers are 1 to 65535, system 0 is a wildcard referring to the local system. The next step is to configure the URL List in either of the Central Controllers, but not both, to point to the other Central Controller. For example, in Illustration 1 NetLinx Central Controller system #1 could have its URL List configured with a single entry that contains the IP address of the NetLinx Central Controller system #7; this will establish a two-way connection. The system #7 Central Controller does not need to have a URL

entry to communicate with system #1. If the system #7 Central Controller's URL List does contain the IP address for system #1 a relay loop will be created which will lead to problems.

OK		
URL Entry	Master 1	Master 7
1	7	

OK		
URL Entry	Master 1	Master 7
1		1

WRONG		
URL Entry	Master 1	Master 7
1	7	1

Once the systems are connected to each other they exchange ICSP routing information such that each Central Controller will learn about all the Central Controllers connected to each other. The implementation of Central Controller ICSP routing primarily involves the communication of ICSP routing tables between Central Controllers. The ICSP routing table is built using the entries within the local URL List, the DPS entries in the DEFINE_DEVICE section of the code, and from the ICSP routing tables exchanged between connected Central Controllers. ICSP Routing tables are exchanged between Central Controllers upon their initial connection and updates to the ICSP routing tables are exchanged periodically. ICSP route table transmission has a certain amount of randomization built in to prevent flooding the network with ICSP routing table transmissions when a Central Controller reports online/offline. Each Central Controller in a network will add a minor random delay (1-5 seconds) so that they don't all transmit at the same time.

*Note: Any TCP/IP devices, including NetLinX Central Controllers, which utilize DHCP to obtain its TCP/IP configuration, are subject to having their IP address change at any time. Therefore, NetLinX Central Controller's IP address must be static unless the network supports Dynamic DNS AND a DHCP server capable of updating the DNS tables on behalf of the DHCP client. If a Dynamic DNS/DHCP server is available then the NetLinX Central Controller's host name may be used in the URL List.

Central Controller to Central Controller Topology

In a system with more than two Central Controllers who need to communicate, the topology of the logical routes may be a concern. In the Star Topology below if Central Controller #2 needs to communicate with a device bound to Central Controller #3, then a ICSP packet is sent over IP to Central Controller #1, the packet is de-encapsulated, read, re-encapsulated in an IP Packet and then sent to Central Controller #3, where it is de-encapsulated, read and forwarded to the device.

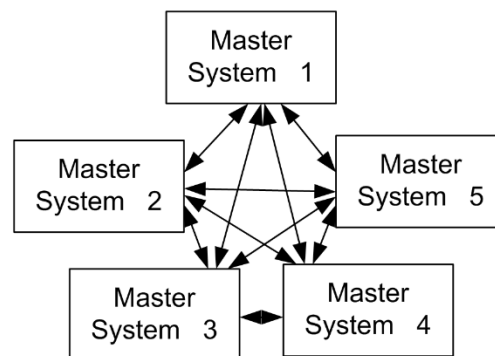
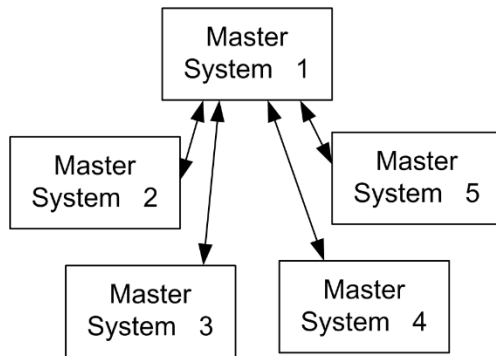
In systems with a large amount of control between systems a fully meshed topology may be more appropriate. In the fully meshed topology each Central Controller is aware of all other Central Controllers. Routing loops are avoided by the use of a "ROUTE MODE DIRECT" command in each Central Controller which allows communication only between Central Controllers who are logically connected using the URL List.

Star Topology

URL Entry	Master 1	Master 2	Master 3	Master 4	Master 5
1	2				
2	3				
3	4				
4	5				

Fully Meshed Topology

URL Entry	Master 1	Master 2	Master 3	Master 4	Master 5
1	2	3	4	5	
2	3	4	5		
3	4	5			
4	5				



For more information on M2M connectivity, architecture and scalability see AMX Tech note 919 “Central Controller-to-Central Controller Unveiled” <http://www.amx.com/techsupport/PDFs/919.pdf>

Dual Network Interfaces (NICs)

Some AMX NX-Series controllers have two 10/100BaseT Ethernet connections. The first is intended for interconnection to the Data Network for external network communications such as database access or scheduling. The second, the ICS LAN is intended for communication with AV devices.

These two Ethernet interfaces occupy separate logical address space and act as a specifically programmable Application Layer Relay. Any data that needs to be passed between the Data Network and the ICS LAN is fully de-encapsulated, validated as required and re-sent based on the application requirements to the other network. This minimizes the possibility that any vulnerabilities on the ICS LAN can create a path to the data network.

The application layer of the central controller proxies all control and configuration of ISCP clients.

Media

Digital Signage

The Inspired Signage software suite is made up of a set of collaborating applications:

Player: The Player renders and displays animated content on screen. The Player does not require user interaction and can be configured over the web using the Player Web Configuration Tool.

Composer: Composer is a content management application, used to customize, manage, and publish content to the Post Office for distribution to one or more Players. Composer is a web application installed on a server accessible by supported browsers over the intranet. Composer can be used by many users with different rights over the content and content management process.

Post Office: Post Office manages and optimizes the transfer and distribution of media files, Templates, and Playlists to the Players in an Inspired Signage Solution. The Post Office is usually installed on the same machine as Composer, however in very large systems it can be placed on a separate machine for maximum performance.

XPORT: XPORT is the application in charge of automatically fetching data from databases, files, and other structured data (for example XML feeds and files, or database queries for status displays) and generating content from it. The content generated by XPORT is passed to Composer for publishing via the Post Office.

Previewer: The Previewer application generates a frame by frame preview of selected signage content to enable users to see how this content will look on screen.

Network Impact

In Digital Signage the content is uploaded to the players as bulk unicast uploads. These uploads can be large if there is video content. In systems with a large number of players it may be best to schedule content updates in off hours. If content is uploaded during business hours, it may be best to put uploads into a low QOS Que.

Additional network and security information is available in the “Network and Security Guide - Inspired XPert” available on amx.com at

<http://www.amx.com//assets/manuals/InspiredXPert.NetworkandSecurityGuide.pdf>

Video Management and Distribution

Vision2

Vision2 consists of number services which correspond to the main video functions:

Archive: The Vision2 Archive service provides a multi-format, multi-bitrate storage system for video or audio files. Video in the archive can be accessed on demand by PC users, from tablets, or set-top boxes. Users can attach metadata to each video containing information about the video contents; this metadata can be customized by the system administrator. The Vision2 search feature can then be used to search videos by the contents of the metadata.

DVB: The Vision2 DVB Service provides and manages a single Digital Video Broadcast (DVB) multiplex of live TV channels to the system. Terrestrial, satellite, and cable TV providers now use digital rather than analog transmission systems to deliver their content.

Record: The Vision2 Record Service provides the ability to record a Transport Streamed MPEG Live Channel into an Archive. You can either record continuously creating files of a fixed duration, or you can manually record a specific event. Alternatively you can schedule recordings to happen at particular times and dates.

Producer: The Vision2 Producer Services allows you to create a scheduled TV channel. You can schedule the Producer to display either MPEG 2/ MPEG 2 - h264 Live Channels or MPEG-2 or MP4 H.264 files from a Vision2 archive.

Reflector: The Vision2 Reflector Service is used for the following tasks:

- To unicast a local MPEG 2/ MPEG 2 h264 vision2 channel over the internet (multicast streams cannot travel over the internet) so that remote users can view this channel, this could be to a remote vision2 installation.
- To receive a unicast MPEG 2/ MPEG 2 h264 vision2 stream from a remote Vision2 installation and broadcast this as a local live channel.
- To add an external source e.g. unicast MPEG 2/ MPEG 2 h264 stream from the internet/local network as a local live channel. Like unmanaged channel but for unicast rather than multicast
- To make a copy of a local MPEG 2/ MPEG 2 h264 vision2 channel and broadcast it from a second network interface card. This is less common

Encoder: NMX-ENC H.264 Encoders connect directly to sources including PCs, cameras and set top boxes and provide the on-ramp to stream the video on a network using a network media solution like Vision2. These robust encoders offer standardized, bandwidth-efficient encoding for SD and HD sources.

Decoder: The STB-04 is an Amino H140 Set Top Box (STB) that ships with a firmware version tested for compatibility with the Vision² system. The STB-04 will decode MPEG-2 and H.264 streams up to 720p. The STB-04 is capable of displaying live MPEG multicast streams as well as playing Video on Demand of MPEG-2 and H.264 content when carried in a MPEG2-TS.

Vision2 streams can also be decoded on PCs and Tablets.

Video Streaming on IP Networks

Network Requirements	
Physical Interfaces:	RJ-45 connectors, 10Base-T, 100Base-TX, 1000Base-T
Layer 2 Services:	<ul style="list-style-type: none"> • Managed Switch • IGMP Snooping V1 or V2 (Not router dependent for operation) • IGMP Querier (One per Subnet) • Spanning Tree Protocol (STP)
Layer 3 Services (if required)	<ul style="list-style-type: none"> • Multicast Routing • PIM Rendezvous point • QoS
Optional:	<ul style="list-style-type: none"> • Storm Control Broadcast and Multicast

There are two main ways that Vision2 servers and NMX encoders send data to decoders: multicast and unicast.

Unicast: Unicast is a one-to-one connection between the decoder and the source. Unicast uses IP delivery methods such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), which are session-based protocols. When a decoder connects using unicast to a Vision2 server, that client has a direct relationship to the server. Each unicast client that connects to the server takes up additional bandwidth. For example, if you have 10 clients all playing 1 Mbps streams, those clients as a group are taking up 10 Mbps. If you have only one client playing the 1 Mbps stream, only 1 Mbps is being used.

Unicast is used in applications like video on demand from the Archive, or as reflected to an external location over non-multicast networks. Due to the increased network consumption, it is not suitable for applications where multiple viewers are receiving the same content simultaneously.

Since Unicast is widely understood it will not be discussed in depth in this document.

Multicast: Multicast is a one-to-one or more connection between multiple decoders and the source. The multicast source relies on multicast-enabled routers to forward the packets to all client subnets that have clients listening. There is no direct relationship between the decoders and the source, the decoders subscribe to a multicast group and the network ensures delivery of the stream. Each client that listens to the multicast adds no additional overhead on the server. The server sends out only one stream per source. The same load is experienced on the source whether only one client or 1,000 clients are listening.

Multicast on the Internet is not practical because the Internet is generally not multicast-enabled. To extend Multicast streams over the Internet a Reflector is used to convert them to Unicast.

Multicast on enterprise networks

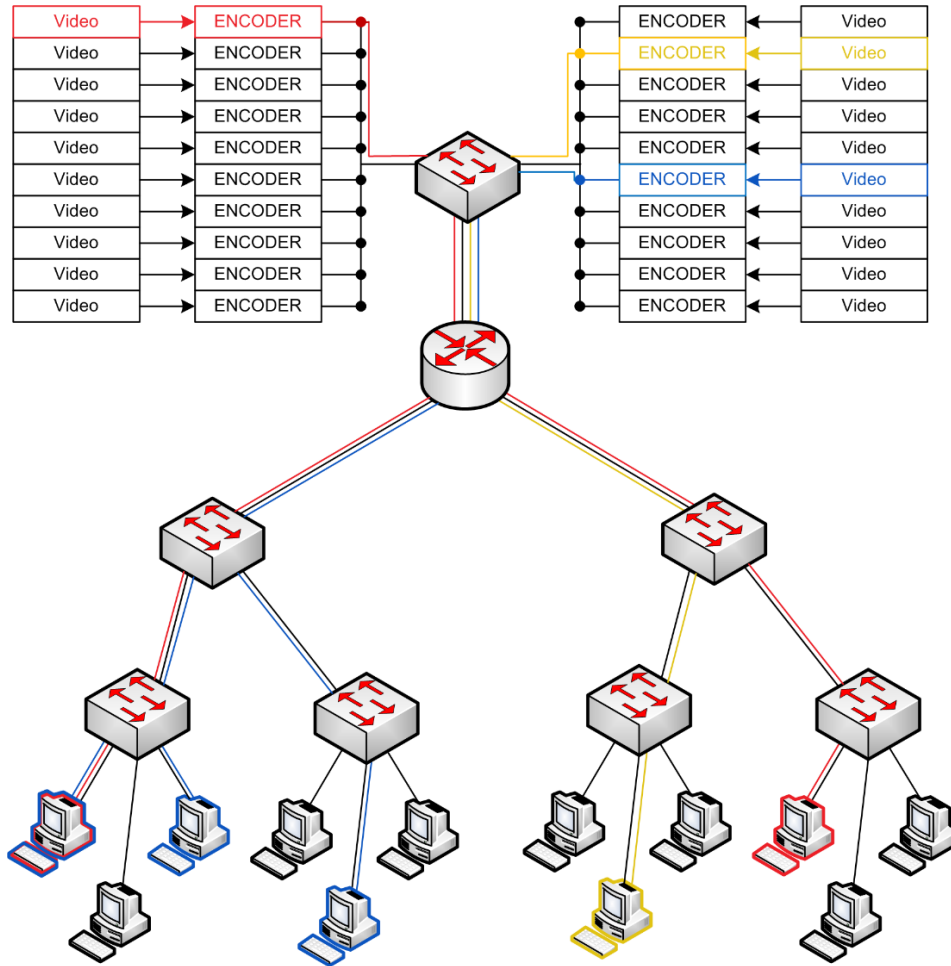
IP multicast is a mechanism for one sender sending data to multiple recipients, but only sending a single copy. It is accomplished by the sender forwarding UDP packets to a multicast IP address and port. The range of IP addresses reserved for multicast is 224.0.0.0 - 239.255.255.255. Without additional controls, such as IGMP and PIM (discussed below), multicasts are forwarded (flooded) to all ports like broadcasts. Unlike broadcasts, multicasts can be routed. Additionally while all broadcasts are processed by the network interface and passed up the stack to the host, multicasts are filtered by the NIC and only multicasts the host is subscribed to are processed.

Multicast addressing: The range of IP addresses reserved for multicast is 224.0.0.0 - 239.255.255.255, however many address ranges are reserved for special purposes. Best practice for streaming is to use the range from 234.0.0.0 to 238.255.255.255, unless there is a specific reason to use other addressing.

Multicast devices do not detect address conflict; many devices could transmit on the same multicast address without a failure. For example all Members of a group send IGMP Membership reports to the same multicast address. Conceivably all the streaming devices could be transmitting to the same multicast address on different ports. This is not the best practice in the case of streaming sources. If that is done all members of the group would receive all streams even if they were only viewing one.

Multicast Example

The illustration below depicts a multicast traffic across a properly configured layer 2 network. Although all the encoders are transmitting a multicast stream, only the streams with a host in the (color coded) multicast group are forwarded to the distribution switch. From the distribution switch on, each multicast stream is only forwarded on any given segment if there is a downstream host joined to the multicast group.



IGMP

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP exists in three backwards compatible versions with IGMPv2 being the most common.

The IGMP message is very simple. It consists of only four things, version, message type, checksum, and the group, i.e. multicast address, to be joined. There are only three message types: Membership Report, which doubles as a join message and is sent to the multicast group address; Queries, asking group members to report if they are still listening which are either sent to the multicast group address or All Hosts (224.0.0.1); and Leave Group, which is sent when a member wants to stop receiving the multicast and is sent to All Routers (224.0.0.2)

IGMP has two types of systems sending messages:

Querier: The IGMP Querier is a process that runs on a switch or router. Its responsibility is to send out IGMP group membership queries on a timed interval, to retrieve IGMP membership reports from active members, and to allow updating of the group membership tables. There is

one active Querier per subnet. In IGMPv2 and v3 if there is more than one Querier then the Queriers hold an election and the one with the lowest IP address is chosen to be active.

The Querier sends periodic Membership Queries to the All Hosts (224.0.0.1) address. It also sends out queries to a specific multicast address when it sees an IGMP leave message to check and see if there is still a listener on the network segment.

The Querier listens for Membership Reports and updates group membership tables used by the adjacent router to determine if the subnet should have a given multicast forwarded to it. The Querier removes group from the table after a timeout period if it has not seen a Membership Report during the period.

IGMP Packets are sent with a TTL of 1 so they are not forwarded through a router.

Group Member: A Group Member is any client that has joined a multicast group. A Group Member joins the group by sending a membership report to the group multicast address. The network logs the Membership report in the group membership table (for the router) and the Switch IGMP cache (for IGMP Snooping) and the Member starts receiving the multicast.

A Group Member responds to IGMP Queries by sending a membership report to the group multicast address of all groups it is a member of for a general query and a membership report to the group multicast address for a group query, to keep the tables updated.

In IGMPV2 a Member sends an IGMP Leave to the to the group multicast address when it no longer wants to receive the multicast.

IGMP Snooping

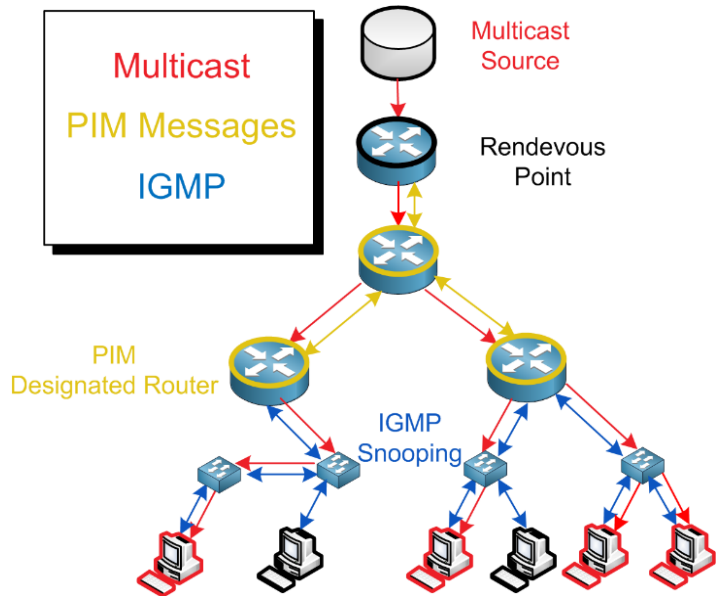
The purpose of IGMP was originally to prune multicast forwarding at a router level. With the advent switching instead of hubs the need to prune multicast at a port level was desired. IGMP snooping was developed for this. In IGMP snooping the network switch listens for the IGMP messages and forwards the multicast packets from the VLAN only to the Ethernet ports that are sources of IGMP membership reports and keeps a cache, very much like the IGMP routing table to keep track of the members. Entries in the cache have a timeout function so if no Membership Reports are received the entry is removed from the cache.

This also works in switch to switch connections. The switch that supports IGMP snooping must flood all unrecognized IGMP messages to all other ports, therefore upstream switches receive new Membership reports to snoop and update their caches.

In the base IGMP protocol a Member responds to a Query after a random amount of time. If a member hears a response before the timer runs out, they do not respond. In IGMP snooping Membership Reports are suppressed to Members so all Members respond to all Queries.

PIM

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for IP networks that provide for distribution of multicast data between routers and across networks. PIM builds *trees* (multicast routes) which ensure shortest path and loop suppression. There are four varieties of PIM:



PIM Sparse Mode (PIM-SM): Build trees rooted at a *Rendezvous point*. Trees are built before any multicast packets are sent. PIM-SM can create shortest path trees for each source. PIM-SM scales well and is the most commonly used PIM mode for video in enterprises.

PIM Dense Mode (PIM-DM): uses dense multicast routing. It creates trees by flooding the network with all the multicast traffic and pruning back routes that are not subscribed to the Multicast Group. This is used in applications that almost all hosts are subscribed to a Multicast, but the flooding can create issues in bandwidth heavy applications like streaming.

Bidirectional PIM: explicitly builds shared bi-directional trees and scales well for applications that communicate between device pools on multicast. Rarely used for streaming unless implemented for another application.

PIM Source-Specific Multicast (PIM-SSM): builds trees that are rooted in just one source. It can be more secure than other implementations because clients subscribe to specific sources. PIM-SSM requires IGMPV3 to be implemented.

PIM Sparse Mode (PIM-SM)

In PIM-SM Routers can take one of two roles:

Rendezvous Point (RP): The Rendezvous Point is a function on a router which is responsible for keeping track of multicast sources and building trees to distribute multicast to other routers. With a Rendezvous Point other routers do not need to know the addresses of the sources for every multicast group. All they need to know is the IP address of the RP router. The RP router discovers the sources for all multicast groups and forwards multicast packets to designated routers requesting them.

The Rendezvous Point function can be manually assigned to routers or can be automatically assigned. Depending on the streaming application it is typically best to manually assign the RP designation to the router immediately adjacent to the encoder VLAN. This minimizes encapsulated data and uses the least router processing power.

Designated Router (DR): The Designated Router is any multicast router in a network that is not the Rendezvous Point. The function of a DR is to send and forward PIM Join messages to the Rendezvous Point to initiate a multicast to its networks and if attached to a multicast source, forward encapsulated multicast packets to the RP for distribution.

Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Storm control uses thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the threshold is reached.

Storm control only works on inbound packets to a switch port so a careful application where there is a possibility of a multicast storm.

Because on layer 2, broadcasts are seen as a subset of multicast, when configuring storm control in a switch port, if you're setting limits to both multicast and broadcast, you should set multicast limit higher than the broadcast limit, otherwise both broadcasts and multicasts will be limited by the multicast level. This is especially important in a spanning tree configuration to not block spanning tree BPDUs.

In AMX's implementation, multicast clients do not request retransmission of multicast data and are therefore not likely to cause multicast storms. However, all multicast traffic is suppressed by multicast storm control, so if video is mission critical then consideration must be made.

Management

RMS Enterprise is scalable client/server based software for IT and AV managers that provides remote management capabilities for AV assets and building systems. The software features a user-friendly dashboard making it easy to centralize the management and monitoring of AV equipment, lights, HVAC and other building functions. It contains an integrated Apache Tomcat web server to provide an intuitive user interface without requiring local access.

RMS Enterprise supports globally deployed systems by adding support for WAN and Internet based connections. A client-server communication strategy utilizing a service-oriented architecture (SOA), supports globally distributed client/endpoint communication.

RMS Enterprise

RMS Enterprise provides large scale management for user and roles, as well for tracking user activities including an audit trail of who performed each activity and when it was completed. The server software supports authentication, encryption and protection from cross-site scripting to prevent security threats. The use of Hibernate and its parameterized queries protects RMS server against SQL injection attacks.

RMS Enterprise may be deployed in a number of configurations to satisfy the needs of the customer. These deployment options include a single server stand-alone solution in a local network up to a multi-server deployment in a web farm for scalability, redundancy, and load balancing.

Data collected by the application is stored in an SQL database. For small deployments (<50 systems) this may operate from an SQL Express instance however it is recommended, and in larger deployments, required, that a separate SQL database be utilized.

Scheduler

RMS Enterprise Scheduler provides ad-hoc bookings and assists attendees in locating meeting rooms by displaying the scheduled appointments on a touch screen in the meeting room and adjacent to room entrances. It also provides automation capabilities for event start and end times.

The RMS Interface for Exchange (RMS-SCH-EWS) utilizes the Microsoft® Exchange Web Services API to communicate with Exchange 2010 servers. This scheduling Plug-In updates scheduling information in Exchange Server and that information also synchronizes with AMX Touch Panels via the RMS Exchange Plug-In - making the scheduling information seamless between Outlook and AMX Touch Panels.

The RMS Enterprise Interface for Lotus Notes Domino (RMS-SCH-LN) provides access to multiple Notes resources. This variety of connection options provides a robust and flexible solution for attaching RMS application rooms to Notes calendars.

Network Impacts

AMX controllers, signage players and Enzo communicate with RMS Enterprise 4.X communicates with the AMX central controller through a HTTP web services API. All communication is initiated from the client device to allow for easy firewall transversal. All communication with the RMS server is performed by these devices, however, as part of the control system infrastructure these may in turn connect to third party devices and expose them to RMS.

Ports and protocols are listed in Appendix A. Due to the highly scalable nature of RMS a separate document “RMS Enterprise Network & Scalability White Paper” is available on amx.com

Appendix A Ports and Protocols

Control:

Product	IN/OUT	Port	Protocol	Service	Description	Disable?	Configurable Port #	Comments
NI-700/ 900/ 2100/ 3100/ 4100 NX-1200/ 2200/ 3200/ 4200 DVX Series DGX Series		20/21	TCP	FTP	Central Controller has a built-in FTP server	Yes	no	
	IN	22	TCP	SSH	SSH Server side SSH V2	Yes	Yes	
	IN/OUT	23	TCP	Telnet	Telnet	Yes	Yes	Can be configured with passwords
	IN/OUT	80	TCP	HTTP	The Central Controller has a built-in web server that complies with the HTTP 1.0 specification and supports all of the required features of HTTP v1.1 Netlinx Central Controller must use HTTP outbound for RMS	Yes	Yes	http must be used for communications to RMS 4.X, non-standard http ports may be assigned
	IN	443	TCP	HTTPS	Secure HTML	Yes	No	https server for system support
	Out	161	TCP	SNMP	Device reporting	Yes	No	support for RFC1213 Ethernet
	IN/OUT	1319	TCP	ICSP	Communication between the Central Controller and AMX devices. Including Software upgrades.	Yes	Yes	
	IN/OUT	1319	UDP	ICSP	Communication between the Central Controller and AMX devices. Including Software upgrades. Device Discovery Broadcasts	No	Yes	
	IN/OUT		ICMP	ICMP	Ping	No	No	AMX equipment will respond to ICMP ping requests
	IN	500	UDP	IKE	Internet Key Exchange (IKE) Embedded	No	No	
	IN	10500	TCP	XML/Java	Server side Java	Yes	no	This port is connected to by the client web browser's JVM when Internet Inside control pages are retrieved from the NetLinx Central Controller's web server
	IN	5900	TCP	VNC	Virtual Panel Control	Yes	Yes	
	OUT	53	TCP	DNS	DNS queries	Yes	No	
	OUT	53	UDP	DNS	DNS queries	Yes	No	
	OUT	67	UDP	DHCP	IP address discovery	Yes	No	
	IN	68	UDP	DHCP	IP address discovery	Yes	No	
	OUT	9131	UDP	DDP	Device Discovery Protocol	Yes	No	Discovery of third party devices using multi-cast beaconing on 239.255.250.250
IN/OUT	3839	TCP	RMS	Central Controller communication to RMS. Only required if the legacy option is enabled to support prior generation RMS 3.x client endpoints.	Yes	Yes	Required for RMS integration ACL for this port on AV network to/from RMS required	

Product	IN/OUT	Port	Protocol	Service	Description	Disable?	Configurable Port #	Comments
ICSLan Device Control Boxes	IN/OUT	1319	TCP	ICSP	Communication between the Central Controller and AMX devices. Including Software upgrades.	Yes	Yes	
	IN/OUT	1319	UDP	ICSP	Communication between the Central Controller and AMX devices. Including Software upgrades. Device Discovery Broadcasts	Yes	Yes	
	IN/OUT	23	TCP	Telnet		Yes	Yes	
	OUT	53	TCP	DNS	DNS queries	Yes	No	
	OUT	67	UDP	DHCP	IP address discovery	Yes	No	
	IN	68	UDP	DHCP	IP address discovery	Yes	No	

Touch Panels

Product	IN/OUT	Port	Protocol	Service	Description	Disable ?	Configurable Port #	Comments	
Moderio X® Series Touch Panels	IN/OUT	23	TCP	Telnet		Yes	No		
	IN/OUT	80	TCP	HTTP		Yes	Yes		
	IN	5900	TCP	VNC	Virtual Panel Control	Yes	Yes		
	IN/OUT	1319	TCP	ICSP	Communication between the Central Controller and AMX devices. Including Software upgrades.	Yes	Yes		
	IN/OUT	1319	UDP	ICSP	Communication between the Central Controller and AMX devices. Including Software upgrades. Device Discovery Broadcasts	Yes	Yes		
	OUT	53	TCP	DNS	DNS queries	Yes	No		
	OUT	67	UDP	DHCP	IP address discovery	Yes	No		
	IN	68	UDP	DHCP	IP address discovery	Yes	No		
	IN/OUT			ICMP	ICMP	Ping	No	No	AMX equipment will respond to ICMP ping requests
	IN/OUT	5060	TCP	SIP	VoIP	Yes	Yes		
	IN/OUT	5060	UDP	SIP	VoIP	Yes	Yes		
	IN/OUT	16348 - 32768	UDP	VOIP RTP	VoIP	Yes	No		
	IN/OUT	3478		STUN	VoIP	Yes	Yes		

Product	IN/OUT	Port	Protocol	Service	Description	Disable?	Configurable Port #	Comments
NXV-300	IN/OUT	23	TCP	Telnet		Yes	No	
	IN/OUT	80	TCP	HTTP		Yes	Yes	
	IN	5900	TCP	VNC	Virtual Panel Control	Yes	Yes	
	IN/OUT	1319	TCP	ICSP	Communication between the Central Controller and AMX devices. Including Software upgrades.	Yes	Yes	
	IN/OUT	1319	UDP	ICSP	Communication between the Central Controller and AMX devices. Including Software upgrades. Device Discovery Broadcasts	Yes	Yes	
	OUT	53	TCP	DNS	DNS queries	Yes	No	
	OUT	67	UDP	DHCP	IP address discovery	Yes	No	
	IN	68	UDP	DHCP	IP address discovery			
	OUT		IGMP		IGMP	Yes	Yes	
	IN/OUT	5060	TCP	SIP	VoIP	Yes	Yes	
	IN/OUT	5060	UDP	SIP	VoIP	Yes	Yes	
	IN/OUT	16348-32768	UDP	VOIP RTP	VoIP	Yes	No	
IN/OUT	3478		STUN	VoIP	Yes	Yes		

Management

Product	IN/OUT	Port	Protocol	Service	Description	Disable?	Configurable Port #	Comments
RMS	IN/Out	3839	TCP	RMS		No	Yes	Required for RMS integration ACL for this port on AV network to/from RMS required
	IN	80	TCP	HTTP	Endpoint device communication and web user interface.	No	Yes	
	IN	443	TCP	HTTPS	Web user interface	No	No	User access can be restricted to 443 This communication is Data network facing
	OUT	443	TCP	HTTPS	Web user interface	No	No	Network communication from the RMS scheduling service to the Microsoft Exchange web services
	IN	8009	TCP	Proxy AJP		Yes	No	If an AJP proxy is used ports 80/443 can be disabled or firewalled on the local RMS server machine; however they will need to be exposed on the proxy server.
	IN	161	UDP	SNMP	Option for integration with othe infrastructure	Yes	Yes	
	IN/OUT	45564	UDP	TRIBES	Server cluster/failover configuration		Yes	
	IN/OUT	45588	UDP	Hibernate Search + Jgroups	Server cluster/failover configuration	Yes	No	
	IN/OUT	46655	UDP	Infinispan + Jgroups	Server cluster/failover configuration	Yes	No	
	Out	25	TCP	SMTP	Mail	Yes	Yes	
	Out	587	TCP	SMTP w/ TLS	Mail	Yes	Yes	
	Out	465	TCP	SMTP w/ SSL	Mail	Yes	Yes	
	Out	162	UDP	SNMP traps		Yes	No	
	Out	389	TCP	LDAP	If Integrating with LDAP	Yes	No	
	Out	5093	TCP	RMS Licensing Server	Server cluster/failover configuration	Yes	No	
Out	1433	TCP	Microsoft SQL Server	Remote MS SQL server/cluster over the network.	Yes	No	Connection to SQL Server	

Digital Signage

Product	IN/OUT	Port	Protocol	Service	Description	Disable?	Configurable Port #	Comments
Inspired XPert Server	IN	16754	TCP		Composer uses this port to connect to Preview (note Preview component can be on a remote machine)	No	Yes	Used if host machine does not support graphics or if only used as server.
	Out	1433	TCP	Microsoft SQL Server	Composer uses this port to connect to SQL Server (note SQL can be installed on a remote Server machine)	No	Yes	
	IN	5143	TCP	HTTPS	Composer web application port	No	Yes	
	Out	21	TCP	FTP	FTP port, used for outgoing publish operations to Players	No	No	
	IN	21	TCP	FTP	Ftp used for Publishing If Post Office is installed on separate Server	No	No	

Product	IN/OUT	Port	Protocol	Service	Description	Disable?	Configurable Port #	Comments
Inspired XPert Player	IN	25002	TCP		Control devices attached to Player serial port	No	No	
	IN	80	TCP	HTTP	Used for Player web configuration tool	No	No	
	IN	25050	TCP	HTTPS	Player port used for remote screenshot, getting/setting public variables for control over displayed content, Player status monitor service	No	No	
	IN	21	TCP	FTP	Ftp used for Publishing	No	No	
	IN/OUT	5900	TCP	VNC	Player administration	No	No	
	Out	Various	TCP/UDP	HTTP/S RSS etc	Network Content	N/A	N/A	Dependent on application

Appendix B Default Values for AMX Products

Central Controllers		
NI-700/ 900/ 2100/ 3100/ 4100 DVX Series DGX Series	Default Administrator User Name	administrator
	Default Administrator Password	password
	Default User Name	NetLinx
	Default Password	password
	Default Administrator User Name (High Security Mode)	administrator
	Default Administrator Password (High Security Mode)	Amx1234!
	Default IP Address:	DHCP (zero-config)
	Default Console Port Settings:	38400, N, 8, 1
	Reset to Factory Defaults:	NetLinx Studio: Diagnostics>Device Addressing Reset To Factory Defaults Central Controller Configuration Manager webpages: Device Pulldown "System Number N" System Button Manage System Tab Reset To Factory Defaults
NX-1200/ 2200/ 3200/ 4200 DVX Series DGX Series	Default Administrator User Name	administrator
	Default Administrator Password	password
	Default User Name	NetLinx
	Default Password	password
	Default Administrator User Name (High Security Mode)	administrator
	Default Administrator Password (High Security Mode)	Amx1234!
	Default IP Address:	DHCP (zero-config)
	Default Static IP Address (LAN Port):	192.168.1.3
	Default IP Address (ICSLAN Port):	198.18.0.1 / 255.255.0.0 (DHCP Server)

Modero X® Series G4 Touch Panels		
	Default IP Address:	DHCP (zero-config)
	Default Settings Password	1988
	Default Administrator User Name (High Security Mode)	administrator
	Default Administrator Password (High Security Mode)	Amx1234!
	SSH User Name	amx
Modero X® Series G5 Touch Panels		
	Default IP Address:	DHCP (zero-config)
	Default Settings Password	1988
	Default Administrator User Name (High Security Mode)	administrator
	Default Administrator Password (High Security Mode)	Amx1234!
	SSH User Name	amx

Digital Signage		
IS-PLAYER-200	Default IP Address:	DHCP (zero-config)
IS-SPX-1000	Default IP Address:	DHCP (zero-config)
	Default User Name	<none>
	Default Password	<none>
	Reset to Factory Defaults:	<ol style="list-style-type: none"> 1. Unplug the unit from the power. 2. Push the reset button and keep it pressed. 3. Power up the IS-SPX-1000 unit. 4. Wait with the reset button pressed for at least 8 seconds. 5. Release the reset button.
IS-XPT-2000	Default IP Address:	DHCP (zero-config)

Wireless		
NXA-WAP1000	Default IP Address	192.168.0.1
	Default User Name	admin
	Default Password	1988
	Reset to Factory Defaults:	Pressing and holding the Hard Reset button on the rear panel for six seconds resets the unit to

		factory default settings.
NXA-WAPZD1000 (Zone Director)	Default IP Address	DHCP/ 192.168.0.2 Note: The NXA-WAPZD1000 is shipped with its default IP address settings as "DHCP", but if it is installed outside of a DHCP network, the device will revert to the default IP address (192.168.0.2).
	Default Console Port Settings:	115200, N, 8, 1
	Default User Name: admin	admin
	Default Password: admin	admin
	Reset to Factory Defaults:	Press and hold the Reset button for 8 seconds. The Status LED will now start flashing green to denote its default status.

Video Management/ Distribution		
V2 Server	Default IP Address	DHCP Note: (use 'ping V2AMX-<SVCTAG>' to find IP address. <SVCTAG> is the service name, which you can find on the front of your server.
	Default User Name	Administrator
	Default Password	Vision2
NMX-ENC	Default IP Address	DHCP
	Default Administrator Name	admin
	Default Administrator Password	1988
STB-04	Default IP Address	DHCP
STB-04 MAX-CSE	Default Administrator account Name	N/A
	Default Administrator account Password	leaves
	Default IP Address	DHCP
MAX-CSE MAX-CSD10	Default Administrator account Name	admin
	Default Administrator account Password	1988
	Default Browser Name	administrator
	Default Browser Password	password
	Default IP Address	DHCP
MAX-CSD10	Default Administrator account Name	admin
	Default Administrator account Password	1988
	Default Browser Name	administrator
	Default Browser Password	password

Appendix C Operating systems

AMX equipment runs on a variety of embedded operating system. Check the actual installed equipment for version information.

Operating System Description:

Product	Operating System	Comments
NI-700/ 900/ 2100/ 3100/ 4100/ DVX Series DGX 8/ 16/ 32	VxWorks	The DVX, DGX and NI series Central Controllers use the VxWorks Real Time Operating System (RTOS) kernel developed by WindRiver. The RTOS is embedded and is inaccessible to users or administrators. The VxWorks RTOS includes task management, encryption management, and the IP stack. All of the firmware runs within this RTOS.
NX-1200/ 2200/ 3200/ 4200 DGX64	Linux	The NX series of Central Controllers uses an embedded version of the Linux Operating System (OS) kernel. All of the EXB firmware runs within this embedded OS.
ISCLan Device Control Boxes	QNX Neutrino:	The EXB-Series of ISCLan devices touch panel uses an embedded version of QNX micro-kernel. All of the EXB firmware runs within this embedded OS.
Modero X® Series Touch Panels	Linux	The Modero X series touch panels use an embedded version of the Linux Operating System (OS) kernel. All of the Modero X main processor firmware runs within this embedded OS.
Modero X® Series G5 Touch Panels	Linux	The Modero X series G5 touch panels use a custom build of Linux. All of the Modero X G5 main processor firmware runs within this OS.
Inspired XPert Server	Installed on local Windows server	
Inspired XPert Player	Embedded Windows 7	
Vision 2 Central Controller	Windows 2008 R2	
NMX-ENC	Linux	
MAX-CSE	Linux	
Enzo	Linux	Enzo uses an embedded version of the Linux Operating System (OS) kernel. All of the Enzo main processor firmware runs within this embedded OS.
RMS	Installed on local Windows server	

