Overview

Document Revision v1.0

The following reference guide provides details surrounding operation of NetworkHD endpoints with consideration to secure communications and best practices on a network.

Firmware Versions

Secure protocols/communication were added to NetworkHD products via a firmware update. In order to realize these functions, the following firmware versions (or higher) must be installed on hardware.

Model	Firmware Version
NHD-110-TX	V7.3.4
NHD-110-RX	V7.2.6
NHD-110-RX-V2	V7.7.6
NHD-140-TX	V2.0.6
NHD-250-RX	V4.0.5
NHD-400-TX (ALL SKU VARIATIONS)	V2.2.2
NHD-400-RX (ALL SKU VARIATIONS)	V2.2.2
NHD-500-TX (ALL SKU VARIATIONS)	V1.2.5
NHD-500-RX (ALL SKU VARIATIONS)	V1.2.5
NHD-600-TRX	V1.3.2.6
NHD-600-TRXF	V1.3.2.6
NHD-610-TX	V1.3.2.6
NHD-610-RX	V1.3.2.6
NHD-CTL-PRO	V1.1.20

Ports & Protocols

Depending on the application and action performed by NetworkHD different communication protocols will/can be used. The following outlines the different communication methods and their responsibilities.

To view a comprehensive list of ports, protocols and multicast addresses use by NetworkHD refer to page 31 in the Technical Reference Guide.

Telnet

Telnet is used for an open and insecure method of communication to the API channel on the NHD-CTL-PRO. Connecting to the NHD-CTL-PRO on port 23 will allow access to send and receive API related actions, such as a matrix switch or to 2-way feedback from peripheral equipment.

Telnet cannot be used to access encoders and decoders directly. Any communication to an endpoint is strictly performed via a proprietary connection to the NHD-CTL-PRO

Telnet can be enabled/disabled as needed to meet application security requirements. Telnet port usage can also be changed from the default 23 to any port you wish via the NHD-CTL-PRO web interface.

Telnet over TLS

Telnet over TLS works in a similar way to Telnet, the main difference being an encrypted and authenticated connection. Using TLS will provide a secure connection to the NHD-CTL-PRO's API channel. Telnet over TLS operates on port 992.

Telnet over TLS cannot be used to access encoders and decoders directly. Any communication to an endpoint is strictly performed via a proprietary connection to the NHD-CTL-PRO

Telnet over TLS port usage can also be changed from the default 992 to any port you wish via the NHD-CTL-PRO web interface.

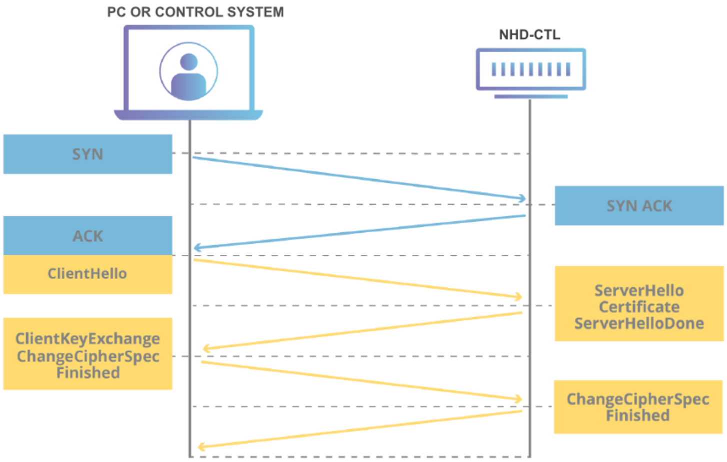
SSH

SSH can be used as a 3rd method for accessing the NHD-CTL-PRO's API channel. Similar to Telnet over TLS, SSH offers an encrypted and authentication connection. SSH operates on port 10022.

SSH port usage can also be changed from the default 10022 to any port you wish via the NHD-CTL-PRO web interface.

SSH also exists via port 22 on encoders, decoders, and the NHD-CTL-PRO, however this connection is locked for WyreStorm use only in the case of accessing device diagnostics or advanced troubleshooting.

API Connection Authentication (TLS)



HTTP & HTTPS

Web servers are found in most NetworkHD devices. The NHD-CTL-PRO contains a webserver which hosts an interface for management, configuration and maintenance of encoders and decoders.

With the exception of the 600 series, all other encoders utilize a web server to host an MJPEG preview stream which can be accessed via a web browser, the WyreStorm NetworkHD Touch app or 3rd-party control panels.

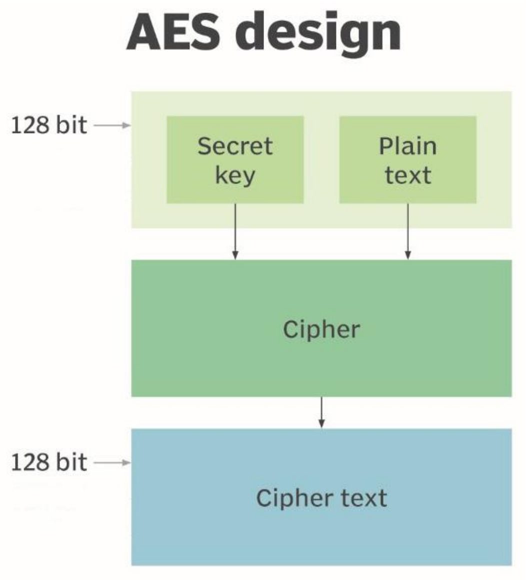
HTTP provides unencrypted access to these web servers on port 80. HTTPS will provide an encrypted connection via port 443.

HTTP can be enabled/disabled as needed to meet application security requirements.

AES

AES-128 encryption is implemented across all NetworkHD series. AES encrypts the A/V and control signal streams between encoders and decoders to prevent data from being intercepted or accessed without permission. AES-128 uses ciphers to encrypt and decrypt data using cryptographic keys.

AES encryption does not affect the video preview streams on encoders as those are generated via MJPEG through HTTP(s) protocol.



Users & Passwords

The NHD-CTL-PRO by default uses a global admin user with unrestricted access to manage and configure endpoints via its web interface. It is recommended to change the admin user’s password upon first login.

Additional user accounts can be created with limited access to this web interface. This limited access only provides the ability to matrix switch, control video walls or multiview. No configuration changes can be made via non-admin accounts.

In addition to the web interface users, TLS and SSH connections to the API channel also require a username and password. The password for TLS and SSH connections can be changed from their default if required for enhanced security.

802.1x & LDAP

LDAP

LDAP allows the NHD-CTL-PRO, encoders, or decoders to communicate with a directory to authenticate a device. When configured, the NetworkHD devices will verify credentials against a database with access permissions. This is commonly used in enterprise networking environments with active directory users.

LDAP can be configured to work with a domain (DN) or a specific user ID.

Both standard LDAP and LDAPS (or LDAP over TLS) are supported. LDAPS allows a signed certificate to be uploaded and used in the authentication process.

802.1x

802.1x works similar to LDAP but uses a RADIUS server to authenticate devices. 802.1x can be used for the NHD-CTL-PRO and individual encoders/decoders. 802.1x ensures that devices that are added to the network are permitted to have access to that network.

802.1x supports EAP-MSCHAPV2 and EAP-TLS authentication protocols.

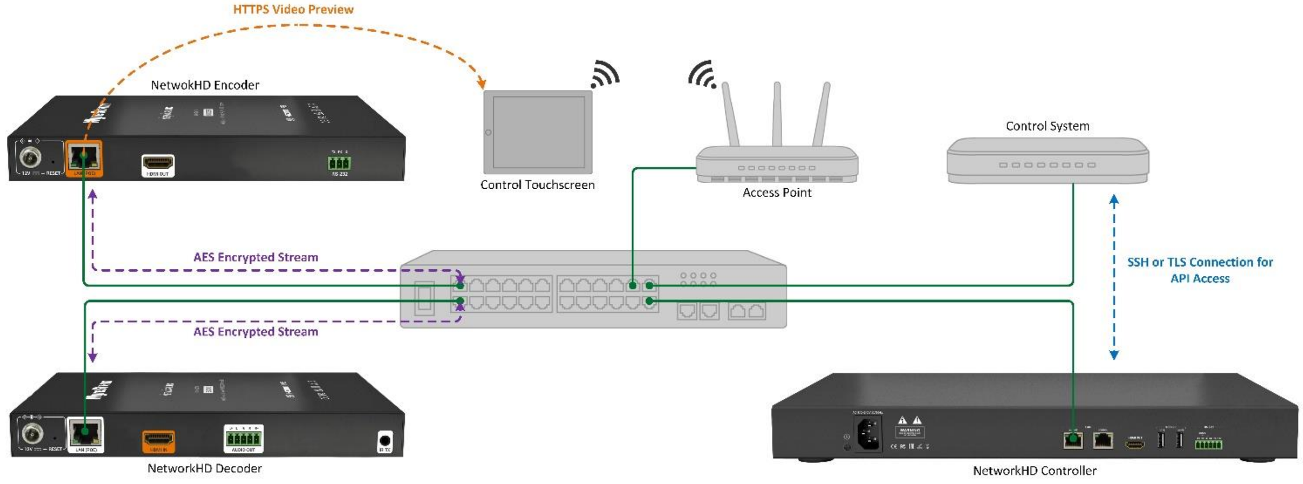
EAP-MSCHAPV2 requires a username a password to authenticate a device where EAP-TLS uses digital certificates.

Disabling Insecure Protocols

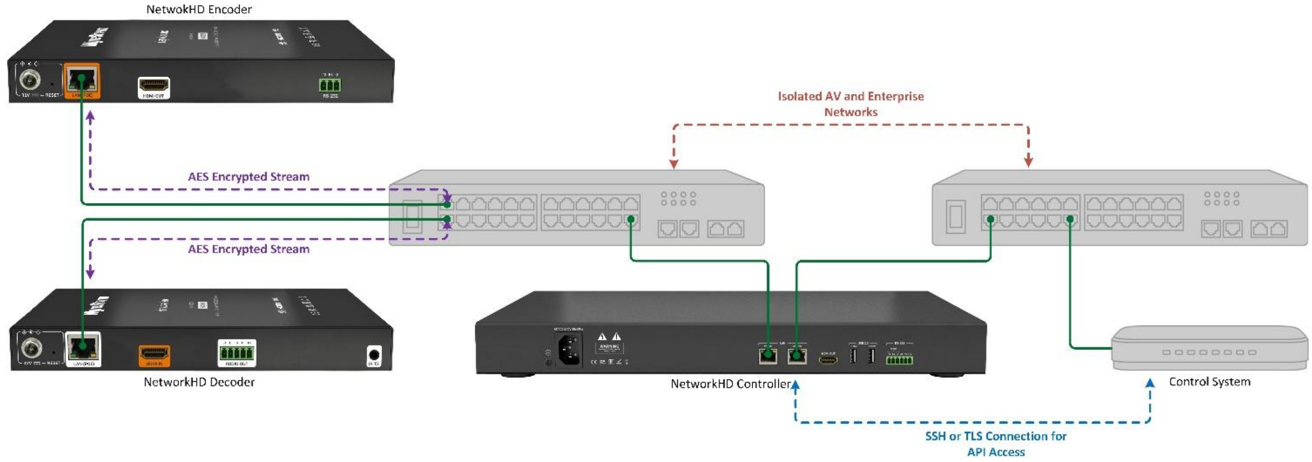
It is best practice to disable insecure communication protocols with NetworkHD devices. This will ensure the highest level of security and encryption of content. By default, all insecure and secure protocols are enabled. In a testing environment or during deployment, Telnet and HTTP can be a convenient way to configure and troubleshoot a system. However, upon finalizing a system it is best to ensure TLS, SSH and HTTPS are used.

Secure System Designs

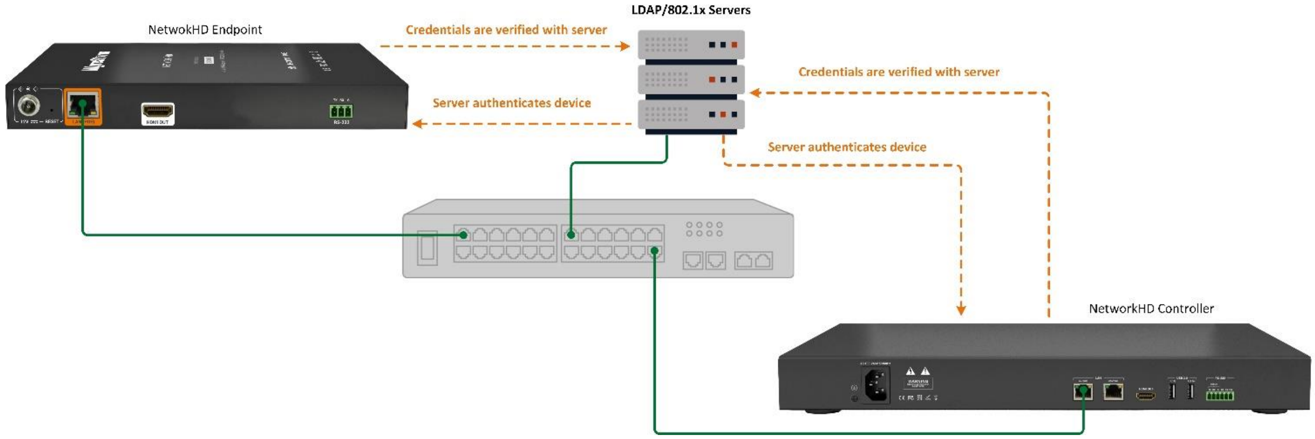
Integrated AV Network



Isolated AV Network



LDAP/802.1x Network


LDAP/802.1x Servers
NetwokHD Endpoint
Credentials are verified with server
Server authenticates device
Credentials are verified with server
Server authenticates device
NetworkHD Controller