Предисловие

Версия документа v1.0

В следующем справочном руководстве приведены подробные сведения о работе NetworkHD с учетом безопасности связи и передовых методов работы в сети.

Версии прошивок

Протоколы безопасности были добавлены в продукты NetworkHD через обновление прошивки. Для реализации указанных в документе функций на оборудовании должны быть установлены следующие версии прошивки (или выше).

Модель	Версия прошивки
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 (Все модели)	V2.2.2
NHD-400-RX (Все модели)	V2.2.2
NHD-500-TX (Все модели)	V1.2.5
NHD-500-RX (Все модели)	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

Порты и Протоколы

В зависимости от приложения и действия, выполняемого NetworkHD, будут/могут использоваться различные протоколы связи. Ниже описываются различные методы связи и принципы их работы.

Чтобы просмотреть полный список портов, протоколов и мультикастовых адресов, используемых NetworkHD, см. «Руководство по установке» на каждое устройство.

Telnet

Telnet используется как открытый, незащищённый метод связи с API-каналом на NHD-CTL-PRO. Подключение к NHD-CTL-PRO через порт 23 позволит получить доступ к функциям, связанным с API, таким как управление или обратная связь от периферийного оборудования.

Telnet не может использоваться для прямого доступа к передатчикам и приемникам. Любая связь с конечной точкой осуществляется строго через фирменное соединение с NHD-CTL-PRO.

Telnet можно включить/отключить по мере необходимости для соответствия требованиям безопасности приложений. Использование Telnet также можно изменить с порта 23 (по умолчанию) на любой другой желаемый порт через веб-интерфейс NHD-CTL-PRO.

Telnet через TLS

Telnet через TLS работает аналогично Telnet, главное отличие — зашифрованное и аутентифицированное соединение. Использование TLS обеспечит защищённое соединение с API-каналом NHD-CTL-PRO. Telnet через TLS работает на порту 992.

Telnet через TLS не может использоваться для прямого доступа к передатчикам и приемникам. Любое взаимодействие с конечной точкой осуществляется строго через фирменное соединение с NHD-CTL-PRO

Использование порта Telnet через TLS также можно изменить с порта 992 (по умолчанию) на любой другой желаемый порт через веб-интерфейс NHD-CTL-PRO.

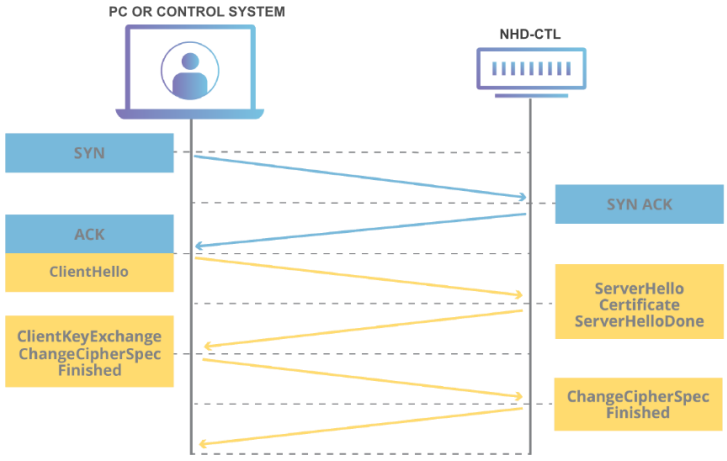
SSH

SSH можно использовать как 3-й метод доступа к API-каналу NHD-CTL-PRO. Подобно Telnet по TLS, SSH предлагает зашифрованное и аутентификационное соединение. SSH работает на порту 10022.

Использование порта SSH также можно изменить с порта 10022 (по умолчанию) на любой другой желаемый порт через веб-интерфейс NHD-CTL-PRO.

SSH работает через порт 22 на передатчиках, приемниках и NHD-CTL-PRO, однако это соединение заблокировано для использования WyreStorm и используется только в случае доступа к диагностике устройства или расширенному устранению неполадок.

Аутентификация API-подключения (TLS)



HTTP & HTTPS

Веб-серверы имеются в большинстве устройств NetworkHD. NHD-CTL-PRO содержит веб-сервер, на котором размещен интерфейс для управления, настройки и обслуживания передатчиков и приемников.

За исключением 600 серии, все передатчики используют веб-сервер для размещения потока предварительного просмотра MJPEG, доступ к которому можно получить через веб-браузер, приложение WyreStorm NetworkHD Touch или сторонние панели управления.

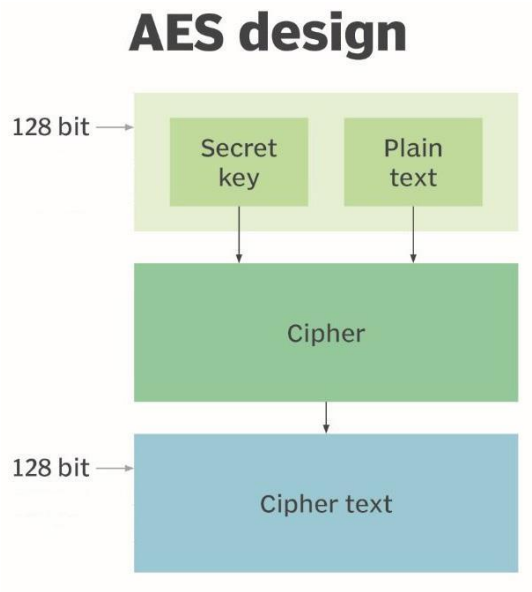
HTTP обеспечивает незашифрованный доступ к этим веб-серверам через порт 80. HTTPS обеспечивает зашифрованное соединение через порт 443.

HTTP можно включать/отключать по мере необходимости для соответствия требованиям безопасности приложения.

AES

Шифрование AES-128 реализовано во всех сериях NetworkHD. AES шифрует потоки аудио/видео и управляющие сигналы между передатчиками и приемниками, чтобы предотвратить перехват данных или несанкционированный доступ к ним. AES-128 использует шифрование и дешифрования данных с использованием криптографических ключей.

Шифрование AES не влияет на потоки предварительного просмотра видео на передатчиках, поскольку они генерируются через MJPEG по протоколу HTTP(s).



Пользователи и Пароли

NHD-CTL-PRO по умолчанию использует глобального пользователя-администратора с неограниченным доступом для управления и настройкой конечных точек через веб-интерфейс. Рекомендуется изменить пароль пользователя-администратора при первом входе в систему.

Дополнительные учетные записи пользователей могут быть созданы с ограниченным доступом к этому веб-интерфейсу. Этот ограниченный доступ обеспечивает только возможность матричного переключения, управления видеостенами или мультиоконным режимом. Никакие изменения конфигурации не могут быть внесены через учетные записи, не являющиеся администраторами.

В дополнение к пользователям веб-интерфейса, для подключений TLS и SSH к каналу API также требуются имя пользователя и пароль. Пароль для подключений TLS и SSH можно изменить со значения по умолчанию, если это необходимо для повышения безопасности.

802.1x & LDAP

LDAP

LDAP позволяет NHD-CTL-PRO, передатчикам и приемникам взаимодействовать с каталогом для аутентификации устройства. При настройке устройства NetworkHD будут проверять учетные данные по базе данных с разрешениями на доступ. Это используется в корпоративных сетевых средах с пользователями Active Directory.

LDAP можно настроить для работы с доменом (DN) или определенным идентификатором пользователя.

Поддерживаются как стандартные LDAP, так и LDAPS (или LDAP через TLS). LDAPS позволяет загружать подписанный сертификат и использовать его в процессе аутентификации.

802.1x

802.1x работает аналогично LDAP, но использует сервер RADIUS для аутентификации устройств. 802.1x можно использовать для NHD-CTL-PRO и отдельных передатчиков и приемников. 802.1x гарантирует, что устройствам, добавленным в сеть, разрешен доступ к этой сети.

802.1x поддерживает протоколы аутентификации EAP-MSCHAPV2 и EAP-TLS.

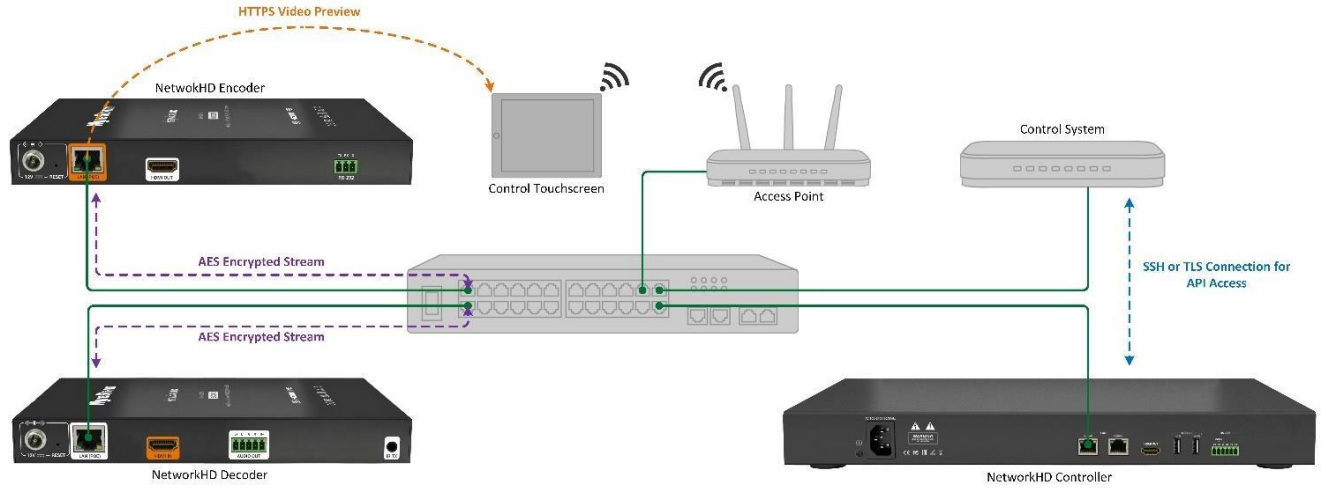
EAP-MSCHAPV2 требует имя пользователя и пароль для аутентификации устройства, тогда как EAP-TLS использует цифровые сертификаты.

Отключение незащищённых протоколов

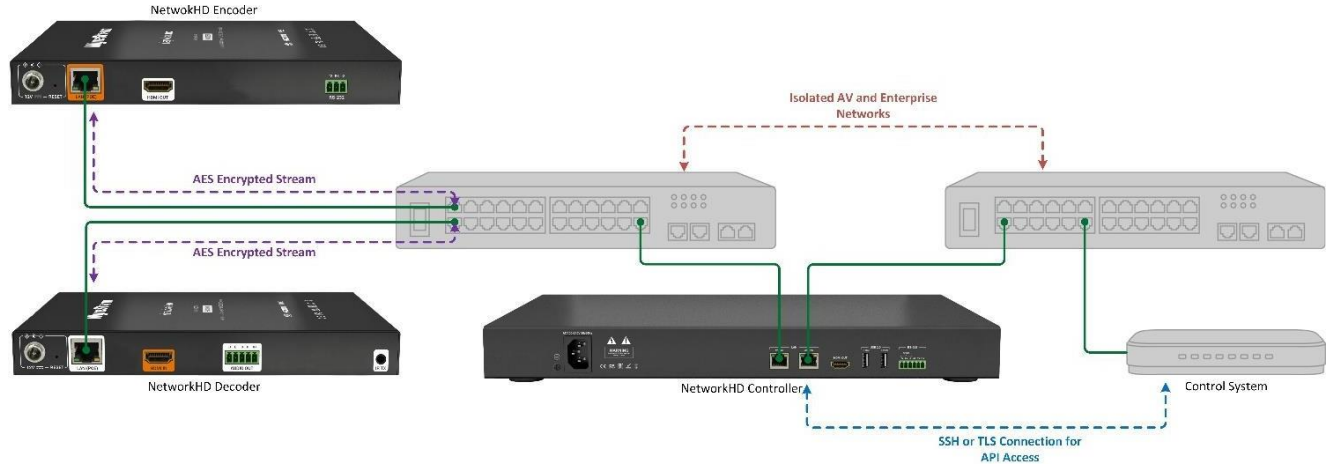
Лучше всего отключать незащищённые протоколы связи с устройствами NetworkHD. Это обеспечит наивысший уровень безопасности и шифрования контента. По умолчанию все незащищённые и защищённые протоколы включены. В тестовой среде или во время развертывания Telnet и HTTP могут быть удобным способом настройки и устранения неполадок в системе. Однако после завершения работы над системой лучше всего убедиться, что используются TLS, SSH и HTTPS.

Защищенные схемы систем

Интегрированная AV-сеть



Изолированная AV-сеть



LDAP/802.1x Network