

IP Link® Best Practices for Network Integration and Security

Table of Contents

Introduction	2
Passwords.....	4
ACL.....	5
VLAN.....	6
Protocols.....	6
Conclusion	9

Abstract

Extron IP Link technology enables AV devices to be controlled, monitored and accessed from any computer connected to the network. As with all IP enabled network devices, there are security concerns that need to be addressed. Developing and implementing a solid security policy to maximize the availability of the IP Link devices on your network will ensure uninterrupted monitoring and control of your AV systems.

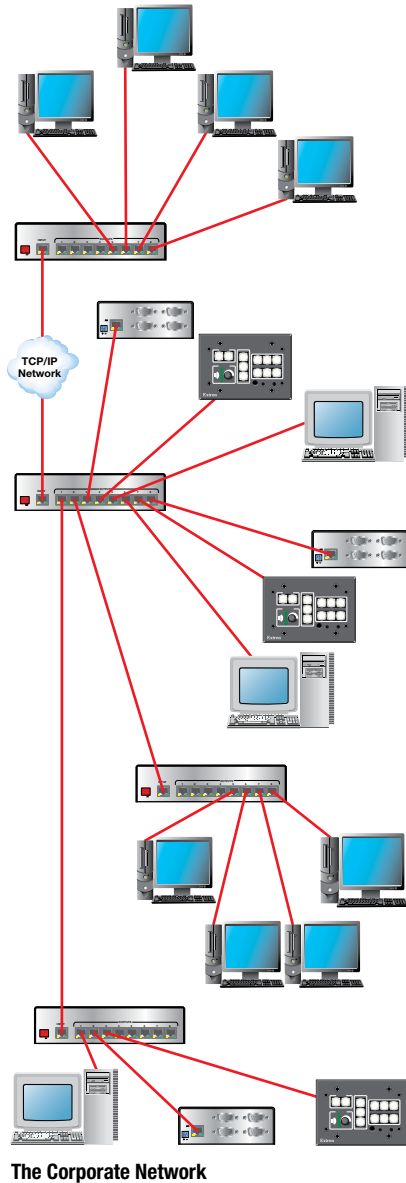
In this paper, we will provide an overview of several standard IT security practices that are compatible with Extron IP Link equipment. We also provide protocol and port information that may be needed by other network applications or appliances.

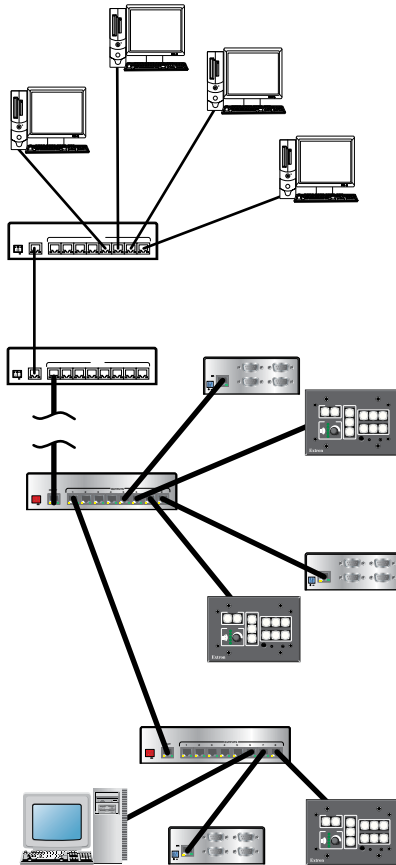
white paper

Introduction

For the IT department, security is the never ending search for a good nights sleep! Hackers are continuously looking for that open door. These “doors” are at all network levels and all levels of sophistication, from dumpster-diving to IP spoofing. There are opportunities at all levels to breach security; each level needs to cooperate to prevent unintended guests from gaining network access.

The Extron IP Link products connect and control A/V equipment and are another part of the network. The following describes how Extron’s products fit in with common security techniques. These security techniques may or may not be implemented by your IT Administrator. Security solutions are constantly changing to keep pace with network evolution.





Isolated A/V Network

Trusted and Untrusted

Security in one sentence is “Who do you trust?” IT is constantly defining who is trusted and what hoops need to be jumped through to achieve trusted status. Hackers are constantly looking for opportunities to become a trusted source. Users provide credentials such as passwords to gain trusted access; and computers are granted network access by being on selective address lists.

We are all aware of the benefits gained by having access to shared resources. However, these benefits are reduced as security concerns drive the IT administrator to control resources and limit access. Taken to the extreme, perfect security would be no access. While this extreme negates the purpose and benefit of a network it does suggest a variant, the Isolated A/V Network, which does provide security by limiting access.

The Isolated A/V Network

An isolated A/V network has its own hardware and creates a parallel network that is separate from the data network. This achieves a high level of security by severely limiting access. Extron network products will work in an isolated environment. The rest of this paper focuses on an integrated solution that balances the needs of security and access.

User Trusted Access

Procedures

We begin with procedures. They depend on the cooperation of the network user and are usually the first line of defense. There are procedures for locked doors to network cabinets and server rooms; keeping reset buttons and physical access to network appliances away from abusers. There are also constant reminders of security procedures such as “don’t open an email attachment from an unknown source” and “protect your password.” These procedures are just as critical, if not more so, than the latest security appliance.



Password Use

Passwords provide access for the user and verification to the network that the user is “trusted”. Procedures for password use, generation and protection are critical to network security. Normal password security procedures consist of not writing down passwords, shielding passwords from others, and changing passwords regularly.

IP Link products have two levels of password security: administrator and user. The administrator level permits complete access to all commands and ports, permitting configuration and maintenance of an IP Link system. The user level grants access to operational controls such as On/Off, video source, volume, and other commands needed for presentations.

Note: The factory default is no password is enabled. We strongly recommend that both the user and administrator passwords be assigned. If the administrator password is not set the user has unrestricted access. Any user could re-configure the system and even change or set passwords.

Password Creation

It is imperative to limit access to all network devices in order to protect them from both unintentional modification and malicious tampering.

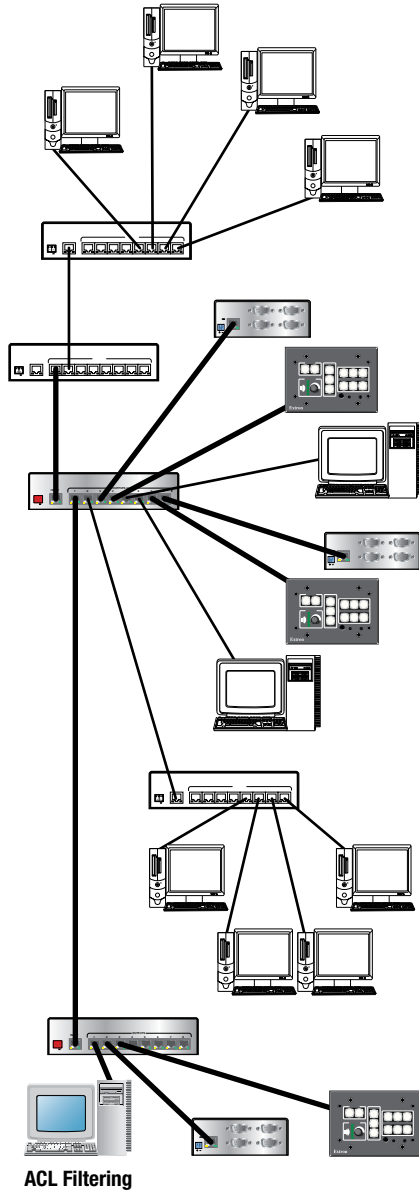
IP Link passwords are alphanumeric, case sensitive and have a length of up to 12 characters. Good security practices recommend that passwords be at least 8 characters in length, consisting of at least one upper case character and 1 numeric digit. When creating a password, switch letters with numbers, and avoid using dictionary words or industry acronyms. For instance, “Extr0nEl3c” is a stronger password than “extron” and is less likely to be guessed. Choose a password that can be remembered; otherwise, users might write it down, undermining security. It is recommended that you regularly change passwords: a good rule of thumb, change the administration password once a month and the user password 2-6 times a year. The longer a static password is in use and remains unchanged, the more likely it is to be compromised.

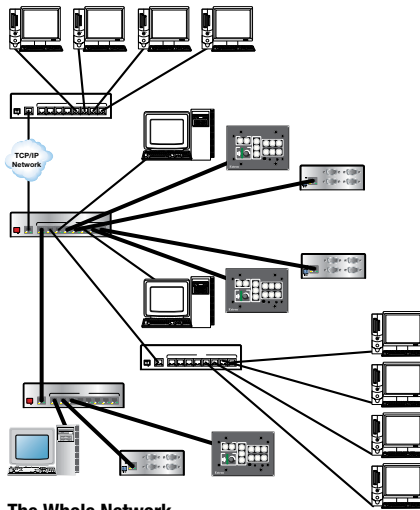
Network Controls for Trusted Access

Access Control List (ACL)

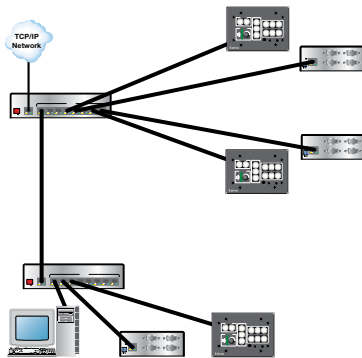
The ACL is strictly a look up table created by the administrator and you are either on the trusted list or not. ACLs filter IP packets entering and/or leaving a switch/router or server. The list can filter on layer 2 MAC addresses, or layer 3 IP addresses, or layer 3 and layer 4 together; defining an IP address and port number. ACLs can perform similar functions as a firewall. A firewall is a common security appliance which blocks malicious internet traffic from a local network.

Again, we are sorting clients and hosts into two bins; trusted and un-trusted. An AV ACL can be created with IP address of all IP Link devices and all GlobalViewer hosts. There can be additional ACL filtering by limiting access to the Telnet port from specific MAC and IP addresses. As an example Telnet traffic could be restricted to just the Ethernet connections within the A/V room and administrator computers.

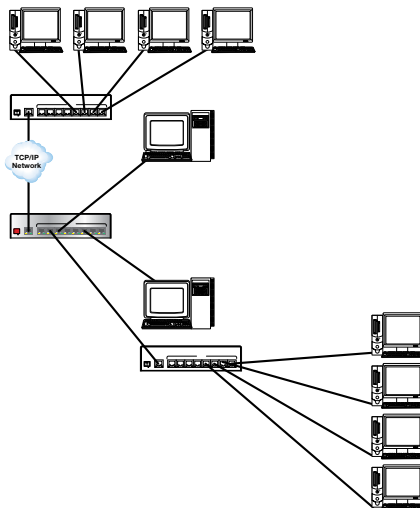




The Whole Network



VLAN A: The AV Network



VLAN B: The Rest of the Network

Virtual Local Area Network (VLAN)

A VLAN, as its name suggests, creates a private or virtual network within a network. The VLAN creates the concept, of the previously mentioned isolated A/V network, within the corporate network but without the drawbacks. Through administration controls, VLANs can access important shared resources and still maintain a community of trusted members.

VLANs are defined in the IEEE 802.1Q specification. They are configurable on network switches and routers that support the VLAN protocol. When implementing the IP Link technology, it is good practice to create a dedicated VLAN for IP Link devices.

Supporting Protocols and Port Specifications

Server Applications

The IP Link device hosts 2 server applications: Telnet for control and status and HTTP for the embedded Web server. The factory default is the standard Telnet port of 23 and port 80 for HTTP.

Changing the well known port 23 for Telnet and 80 for HTTP to any other “random” port number is a good security practice. Telnet and HTTP ports can be remapped to any other valid port between 1024 thru 65,535. Remapping the standard ports help deter automated attacks that scan well known ports looking for an opportunity to gain trusted access.

Note: Before changing the default port number verify that the new port number is not already in use by another application in your network.

Client Applications

The IP Link device supports 2 client applications. The IP Link device includes a DHCP - Dynamic Host Configuration Protocol client which allows the device to dynamically get its TCP/IP parameters - IP address, subnet mask and default gateway - from a DHCP server. The SMTP - Simple Mail Transfer Protocol client allows an administrator to set up monitoring processes which trigger an e-mail to be sent when certain conditions are met.

SMTP Authentication

IP Link devices can be programmed to automatically send e-mail notices. E-mail systems may be configured to reject incoming messages from an unauthorized source to prevent SPAM relay attacks. Because an IP Link device does not have an account in the internal system, some e-mail systems would reject any e-mail coming from the IP Link device and would consider it as SPAM. If the SMTP server supports it, the IP Link device can authenticate against the server prior to sending a message. If your SMTP server doesn't support authentication, one option is to create an account in your e-mail system for each IP Link device.

DHCP Client Support and Configuration

Every IP Link device includes an embedded DHCP client in the hardware that can be enabled through its Web server. By default, DHCP is turned off. Extron recommends that IP Link devices be given a static IP address for better management when using Extron Global Configurator Software. Global Configurator uses the IP address assigned to the IP device when compiling and configuring the XML and HTML files that are uploaded to the device. Any changes to the IP address of the IP Link device after configuration will require a recompiled GC project file.

When the DHCP client is enabled on an IP Link device, it will get its IP parameters from the DHCP service. Prior to enabling DHCP, make sure that a DHCP server is available on the network and that it is able to distribute IP addresses for the subnet where the IP Link device is installed.

The purpose of a DHCP server is to provide dynamic-addressing, each IP address is selected by the DHCP server in sequence from a list or range of addresses. It is probable that an IP Link device will not receive the same IP address every time it requests an IP address. To avoid this situation, the IP address for each IP Link device needs to be a static entry in the DHCP server. Typically, this can be accomplished by reserving a specific IP address based on the MAC address of the IP Link device.

Auto Discovery Ports

The Extron Device Manager application communicates using UDP ports 1230 and 1231 to monitor the IP Link device and is used for auto-discovery. These ports cannot be remapped. Please make sure that ports 1230 and 1231 are accessible through network appliances.

Direct Access Ports

Many of the IP Link products have unidirectional or bi-directional serial ports. Extron defines these as Direct Access Ports. Direct Access Ports are assigned unique TCP ports for direct communication. Factory defaults start at port 2001 and are assigned in ascending order as needed. The starting base port can be changed to any other available port number beyond 1024 or be turned off to reject connections all together.

Conclusion

Network security must be approached on a system level. IP Link devices require the normal security measures that IT deems necessary for any network connection: Passwords, ACLs, VLANs and port re-mapping put up significant barriers for the malicious intruder.

At the device level, IP Link products are inherently secure because they are dedicated appliances. They are not subject to many threats because they do not run a Windows Operating System. This eliminates many of IT's security concerns when integrating new products. For IP link devices, the security measure that needs compliance is password enforcement. Close that open door into the network, enforce both user and administrator passwords on IP Link devices.

Extron Electronics, headquartered in Anaheim, CA, is a leading manufacturer of professional AV system products including computer-video interfaces, switchers, matrix switchers, distribution amplifiers, video scalars, scan converters, signal processing devices, Ethernet control interfaces, and high resolution cables. Extron products are used to integrate video and audio into presentation systems for today's high tech boardrooms, presentation/training centers, university lecture halls, and other applications.

For additional information, please call an Extron Customer Support Representative at: 800.633.9876 (inside USA and Canada only) or 714.491.1500 for Extron USA; +800.3987.6673 (inside Europe only) or +31.33.453.4040 for Extron Europe; +800.7339.8766 or +65.6383.4400 for Extron Asia; +81.3.3511.7655 for Extron Japan.

www.extron.com

Copyright © 2009 All rights reserved.