HIRSCHMANN
A BELDEN BRAND

Mark Cooksley - **Product Manager**

Network Security in the Hirschmann Operating System

Improving Industrial Network Security - a Step by Step Guide

If you are a network administrator, there is something you can be sure of. Somebody wants to attack your network. Maybe just for fun, maybe to steal information, maybe to extort money. Or in the case of an industrial network, maybe to slow down your production process and make your company less competitive.

Effective network security is the countermeasure. Today everyone who is directly or indirectly involved with an industrial communications system needs to understand security. But it seems so complicated. Jargon. Buzzwords. Unfamiliar concepts. Actually, essential network security is easy to understand. You just need to get started with the learning process.

This document explains basic network security functions, and how you can deploy them to provide foundation level security for your network. If you own Hirschmann switches running HiOS software, then you already have some or even all of these functions. If not, the concepts are just as applicable to all Ethernet networks. Whenever you are ready to start enhancing your network security, the topics covered here will provide you with the knowledge you require to make well-founded decisions.

Table of Contents

Be certain.
Belden.

Protecting Your Network Infrastructure

Hardware is the foundation of your network. A secure, and therefore highly available network is essential to the success of your operation. So the first step on your security journey should be to protect your network infrastructure itself. With a few simple actions you can regulate access to your network devices. The hardened devices will then provide a solid foundation on which to build your secure Ethernet network.

Management Protocols

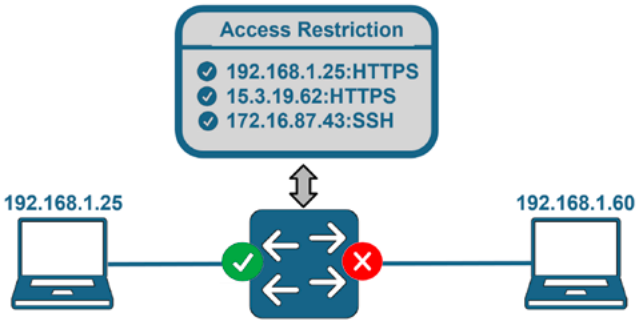
In the past Hirschmann's philosophy has been to make our products as simple as possible to use. This included maximizing the number of methods which can be used to connect to them. But today, security takes priority over ease of use. We still continue to support unsecure communication protocols such as SNMPv1 and v2, Telnet, and HTTP. But by default they are now disabled. Feel free to enable them, if this is required on your network. Encrypted protocols, such as HTTPS and Secure Shell are enabled. But even here a small amount of work is required to increase the effectiveness of the protocols.

Protocol	Allowed	Comments
SNMPv1	✗	
SNMPv2	✗	
SNMPv3	✓	
HTTP	✗	
HTTPS	✓	- Change the certificate - Change the port number
Telnet	✗	
SSH	✓	- Use RSA - Change the key - Set an idle timeout

Access your products the modern way, using secure encrypted protocols

IP Access Restriction

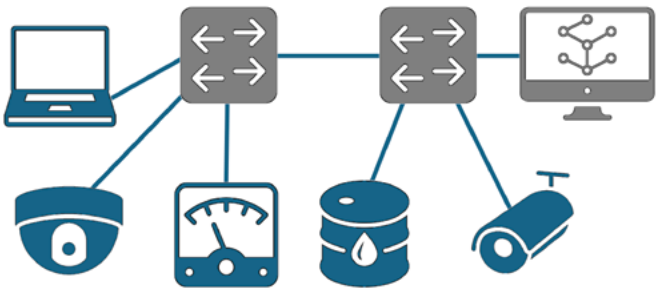
By default, your network infrastructure devices can be accessed from any PC attached to the network. This is convenient when commissioning your network. But for live operation it makes sense to limit access. A simple and effective way to achieve this is to restrict access to specified IP addresses, typically PCs under your control. Of course, IP addresses can be spoofed. But as we will see later, spoofing can be prevented. For even stronger security, this technique can be taken a step further. Specify which protocols can be used by each IP address. For example, allow SNMP from a management station, but maybe not from an engineering workstation.



Control which PCs can be used to access your network infrastructure

VLANs

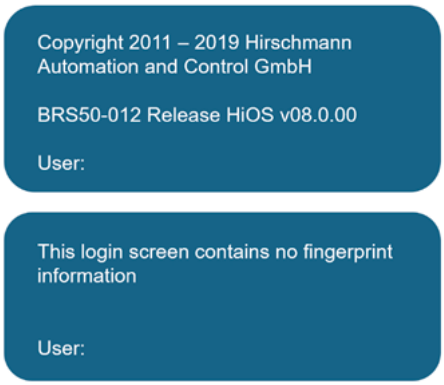
VLANs were developed to allow the creation of multiple independent logical networks running on a single physical network. Devices in one VLAN are unaware of devices in another. Or even that there is another. This makes VLANs an ideal tool for network security. HiOS allows you to create a VLAN for the management interface of each switch and the ports where the network management stations are connected. As a result, the switches and management stations can communicate, but they are hidden from the network users. Security is increased as end users connected to the network cannot see or communicate with the network infrastructure.



Hide your network from the connected users

Command Line Banner

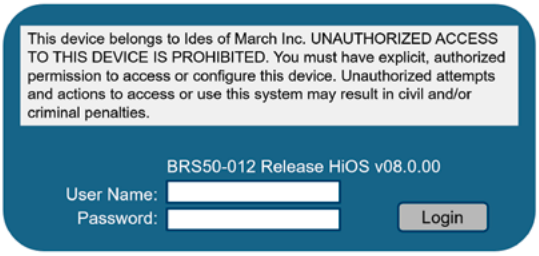
In the physical world, fingerprints have been used for more than 100 years to identify individual people. In cybersecurity, fingerprinting is a technique where an attacker gathers information about a device. This information is then used to facilitate an exploit against the device. In the example on the right, you can see a typical switch login screen. It contains a lot of information which could be useful for an attacker, such as device manufacturer, model number and software version. While this information is useful during network commissioning, for day to day network operation this data serves no purpose. So hide it, and remove a weapon from your attacker's armory.



Hide fingerprints to ensure device anonymity

Appropriate Use Banner

Appropriate Use Banners are typically displayed together with a device login screen. They are used to explain that any unauthorized attempt to access the device could result in severe legal consequences. Of course these banners cannot prevent an attack against the device. But they may deter an attacker. They could also assist your legal department in any subsequent legal action against an attacker.



Make sure that attackers understand the consequences of their actions

User Management

If all your employees are using the same login credentials, accountability is lost. One of the most effective things you can do to protect your network devices against unauthorized access is to set up user accounts. Log files make extensive use of user names to record who has done what. HiOS offers a number of predefined access roles, such as full read/write, read/write except security parameters, read-only plus saving log files, or pure read-only. If none of these fits your precise requirements, we can customize a role to match the responsibilities within your organization's structure.

User	Role	Password
Mark	Operator	*****
David	Auditor	*****
admin	Administrator	*****
user	Guest	*****

Ensure that your employees are accountable for their actions

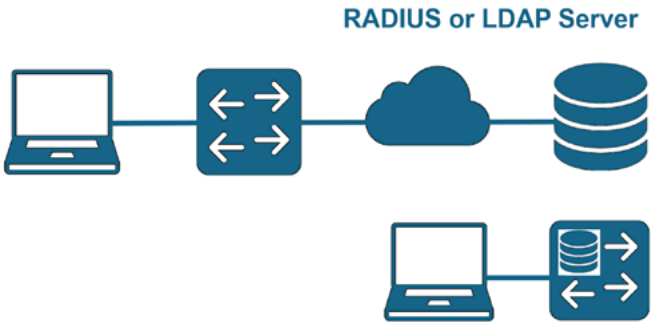
Password Policy

Today, every time you create an on-line account, your password must conform to a policy which describes length and characters. So it makes sense to have the same requirement for your switches. By demanding a minimum password length, as well as specific characters, you can increase security by compelling your users to use strong passwords. Attackers will try to guess the passwords. So you must limit the number of login attempts before the account becomes locked. Attackers who deliberately cause accounts to be locked are also creating a denial of service. So it makes sense to allow accounts to be enabled automatically after a period of time.

Conform to your corporate standard

User Device Login Authentication

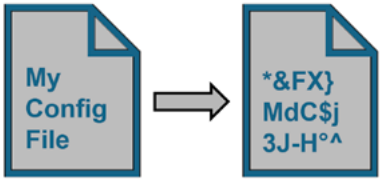
When your employees want to log in to your network devices, their credentials must be checked. HiOS offers several ways to authenticate your employees. The simplest way is to store user names and passwords in a database on each switch. But this has a potential disadvantage. If an employee leaves the company, or a new employee joins, the database on each switch must be updated. A second option would be to use RADIUS. This is a tried and trusted mechanism for storing credential in a central server. The technique is certainly scalable. A third option is to use LDAP to verify credentials. This is the same system which is used for your Windows login. So you can provide users with a single sign-on across your organization.



Select an authentication method which best suits the size of your network

Configuration File Encryption

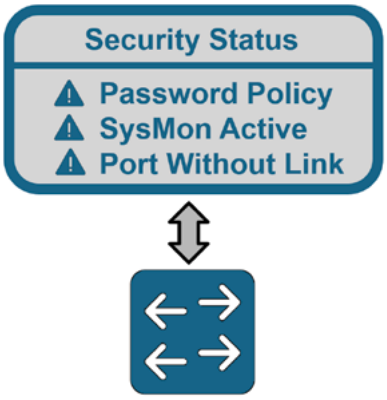
You need backups of your device configuration files, in case a device needs to be replaced. But what could happen if the configuration files fell into the wrong hands? Of course sensitive information such as passwords is encrypted. But there is still a lot of potentially interesting information in these files. The obvious answer is to encrypt the configuration files. And HiOS certainly offers this option. But that leads to a classic example of where it is not possible to have both security and convenience. Traditional device replacement using removable media will not work with encrypted configuration files. A device in factory default needs to be given a password to decrypt the file. So you need to make a decision. If you can be certain that the configuration files can be stored securely, then leave them in plain text. If not, encrypt them.



Secure your device configuration files

Security Status

Switches support many security mechanisms and it can sometimes be challenging to decide which mechanisms should be implemented on a switch. The HiOS Security Status function is here to help you. The Security Status configuration screen lists typical security functions which can be configured on a network. From this list, you can select which functions are important to your network. An alarm will be generated if one or more of your selected functions have not been activated.



Be notified of unsecure configurations

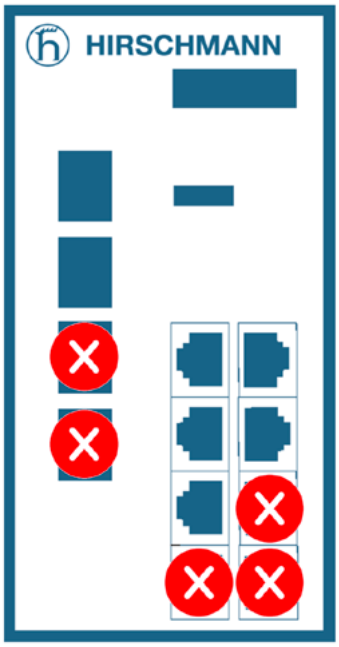
Enforcing Network Access Policy

Now that you have secured your network infrastructure, the next step is to decide which devices and which people are allowed to communicate on your network. This is known as Network Access Control. Clearly if you restrict network access to authorized users, you greatly reduce the opportunities for an outsider to attack your operation. HiOS on its own offers a range of configuration options to meet your requirements. But Network Access Control is becoming ever more sophisticated. As your demands become more complex, you may find that using HiOS devices together with external authentication software will provide you with the most granular solution.

Unused Ports

Ease of use is one of the main reasons that Ethernet became the dominant LAN protocol. If you want to get access to an Ethernet network, just plug your PC into an unused switch port, and you are good to go. In the past, this was perfect. Today, the connection of unauthorized devices is one of the main causes of security breaches. It is also one of the easiest to prevent. If your switch is in an accessible location, disable the unused ports. This will deny network access to any devices which are connected to these ports.

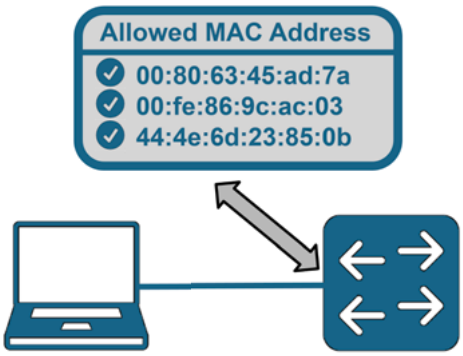
Prevent network access via unused switch ports



Port Security by MAC Address

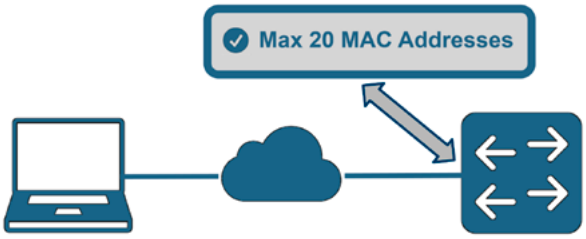
Imagine this scenario. A potential attacker tries to connect to your network by plugging his PC into unused ports on a switch. He is never able to establish communication, because the ports are disabled. So what will he try next? Probably he will unplug the cable from a working port, and connect his own PC. You need to ensure that he is still unsuccessful. Port Security defines which MAC addresses or VLANs can use a port. Packets received with an unknown source address are discarded. So in the described scenario, if you have deployed Port Security the attacker would still not get access to the network.

Restrict network access to defined MAC addresses



Port Security Against MAC Flooding

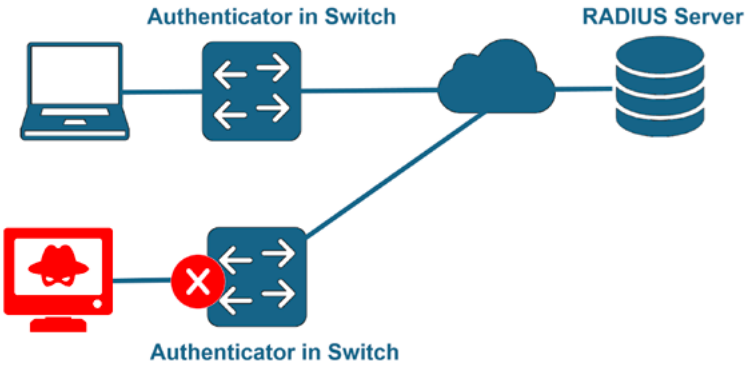
Port Security can also be used to restrict port access to a defined number of MAC addresses. In this case the number of addresses is relevant, not the specific addresses. So why would you want to do it? A number of network attacks are based upon the ability to fill up the Learned Address Table, also known as the Forwarding Database. This is done by transmitting a large number of data packets with different source addresses into the switch. When the Learned Address Table is full, packets subsequently received are flooded to all other ports on a switch. This facilitates the interception of communication which is running through the switch. MAC Flooding Prevention can also be used to prevent DHCP Starvation Attacks, which will be covered later.



Prevent the interception of communication through a switch

802.1X Port-based Network Access Control

Earlier we looked at using RADIUS authentication to allow a user to connect to a switch. A very similar technique is widely used to allow a device such as a PC to access a network. When a PC attempts to connect to a network, the switch uses a protocol called 802.1X to put the client on hold. The switch checks with an authentication server, such as a RADIUS server, whether the PC is allowed to connect to the network. The client is then allowed or denied network access. The client could also be assigned to a specific VLAN, for example a guest VLAN. Network Access Control using 802.1X is commonly used in IT networks today, and its deployment in OT networks is increasing.

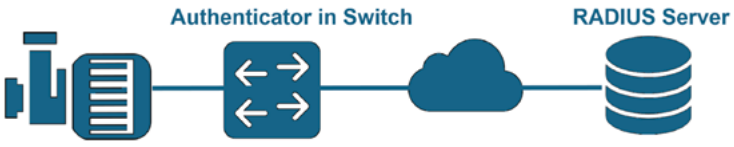


Enforce network access control using state of the art technology

MAC Authentication Bypass

802.1X authentication works well in modern networks, where all devices support the protocol. But in OT networks, many industrial devices do not support 802.1X. So does this mean that you cannot use authentication for network access at all? Actually, no. HiOS supports a feature called MAC Authentication Bypass. This allows authentication of older devices to be based on the client MAC address. It is not as secure as traditional authentication, because the client MAC address can be spoofed. But it is a big improvement compared with no authentication. Even better, HiOS enables you to mix 802.1X and MAC Authentication Bypass on the same switch, giving you the greatest flexibility.

Benefit from network access control, even with older client platforms

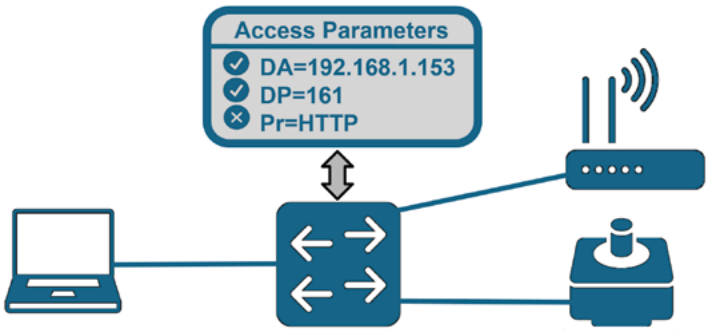


Deploying Access Control Lists

Most network security is based around permitting or denying something. Access Control Lists are an excellent example of this. Access Control Lists, or ACLs as they are commonly known, allow you to permit and deny traffic transmitted into or out of network interfaces, based on a range of criteria. ACLs operate at wire speed, with no impact on data throughput, which makes them ideal for use with high speed ports.

Basic Access Control Lists

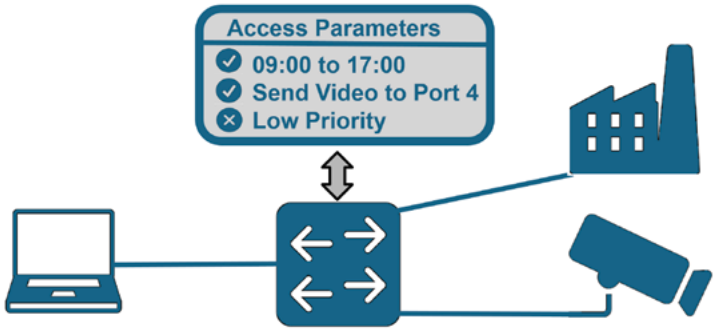
In HiOS, we have divided ACLs into two categories, called Basic and Advanced. Don't be fooled by the names. Basic has limited configuration options, but these options are extremely powerful. You can decide to permit or deny communication based on IP addresses or protocols. For example, "Device A cannot communicate with Device B". Or "Device A cannot communicate with this group of devices". Or "Device A can communicate with Device B, but only to send events". As you can see, even with only a few decision criteria, you can build up very flexible rules. For beginners to the deployment of ACLs, these building blocks are a great way to become familiar with the concept.



Create powerful communication rules with simple building blocks

Advanced Access Control Lists

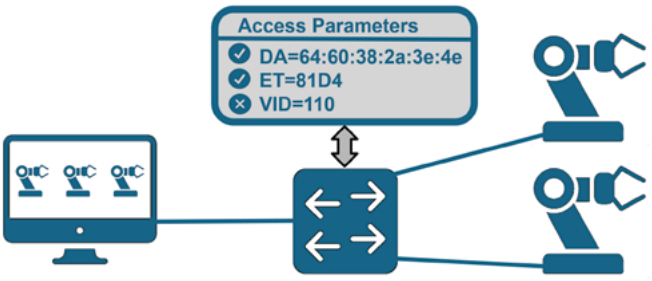
Once you become familiar with the concept of ACLs, it is time to consider how your network could benefit from the more advanced options. This document is not the right medium to discuss every possible option. There are just too many. But it is interesting to be aware of some commonly used configurations. You can permit or deny traffic based on its priority, the flags set in the headers, or whether the data has been fragmented into multiple packets. This would drop potentially malicious traffic. You can assign priority to incoming traffic. Great if your legacy devices cannot do this for themselves. Not all networks are in use 24 hours a day, so you can decide to apply the rules only at certain times. You can mirror the traffic to another port, for monitoring and analysis. You can even force specific traffic to a defined port, regardless of its intended destination.



Configure granular control of data flow

MAC-based Access Control Lists

So far we have looked at Access Control Lists for TCP/IP traffic. But on OT networks you will often find industrial protocols, and these protocols may not be based on TCP/IP. No problem. HiOS offers ACLs at Ethernet level. An Ethernet frame is much less complex than a TCP/IP packet, so there are fewer fields which can be used for filtering. This makes it simpler to create MAC level ACLs. Basic ACLs support filtering on MAC addresses. Advanced ACLs support filtering on VLANs, traffic type, time of day, and other criteria.



Deploy ACLs to control non-TCP/IP protocols

Firewalls vs. Access Control Lists

If you are familiar with firewalls, then you will recognize that firewall rules and Access Control Lists have a lot in common. For example, filtering on addresses or protocols. So what are the differences between firewalls and switches supporting ACLs? This is not a black and white topic, and there are many opinions. Let's examine some basics. Firewalls offer a function called Stateful Inspection. Put simply, Stateful Inspection will only allow data into your network if the data was requested from inside your network. Your home router with firewall probably works like this. It is a great function for use between networks. ACLs generally offer more filtering options, so they work better inside a network. Unlike firewall rules, ACLs are performed in hardware, so they operate at full speed and have no impact on your network performance.

Select the right technology for the job

Controlling Malicious Traffic

Denial of Service attacks can be conducted by attackers who possess only low skill levels. Although these attacks will not cause long-term harm, at best they are a nuisance, and at worst can cause a production failure and therefore financial loss. HiOS includes a range of tools to prevent disruption to your network communication caused by malicious network traffic.

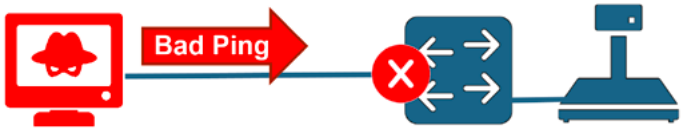
Denial of Service Prevention TCP/UDP (Legacy)

Denial of Service attacks can take many forms. One method is to attack the TCP/IP protocol stack on a device causing it to stop functioning. This can be done by sending the device data packets which do not conform to the standard. The receiving device does not know how to process the packet, so the protocol stack crashes. Another technique is to send a data packet to a device, using its own IP address as the source. The device then replies to itself, causing an endless loop. Modern protocol stacks are resilient to these techniques. But if you are supporting legacy devices on your network, such as older PLCs or I/Os, switches can filter out these malicious data packets.

Protect your legacy equipment

Denial of Service Prevention – ICMP

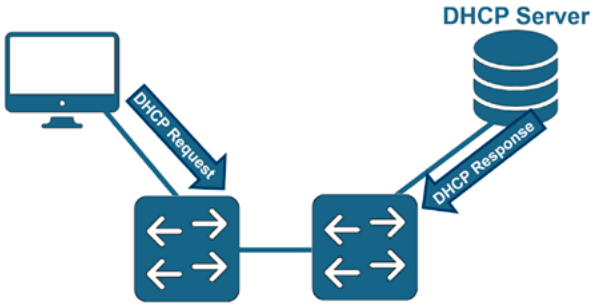
Internet Control Message Protocol, or ICMP, is used to diagnose errors on networks. The best known component of ICMP is Ping. While most of us use pings to detect device availability and response times across a network, pings can also be used for malicious purposes. A broadcast ping will be sent to all devices on a network, and many may reply. Sending a broadcast ping with the source address of another device on the network might result in a Denial of Service attack. Sending a ping with a very large payload can cause a buffer overflow in the recipient device, crashing the protocol stack. This is sometimes referred to as the Ping of Death. Again, modern devices are resilient to these kinds of attack. But you need to protect your older devices.



Filter out malicious network traffic

DHCP Server

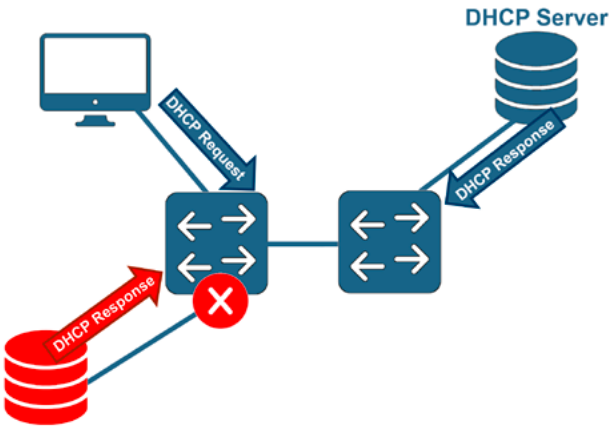
Dynamic Host Configuration Protocol, known as DHCP, is a network protocol used to provide IP addresses and other configuration parameters to end devices. If you attach your computer to a network in the office or at home, there is a very high chance that it will get its IP address via DHCP. In the past, DHCP was not commonly used on industrial networks. But as these networks get bigger, DHCP becomes an attractive option for simplified deployment. DHCP was never designed to be secure, and it forms the basis for many network attacks. If you use DHCP, you need to take some precautions.



Employ security functionality when using DHCP

DHCP Rogue Server Prevention

The easiest way to attack a network which is using DHCP is to add another DHCP server. The unauthorized server will hand out IP addresses which are not compatible with the network address plan, therefore disrupting communication. You can prevent this by only allowing DHCP servers to be attached to trusted ports, in other words ports which are directly under your control. Note that DHCP servers are often attached to networks by accident. For example, a user attaches another switch or a wireless access point to the network, without realizing that these devices have an active DHCP server. So attacks by rogue servers are often unintentional.



Protect your network against unauthorized DHCP servers

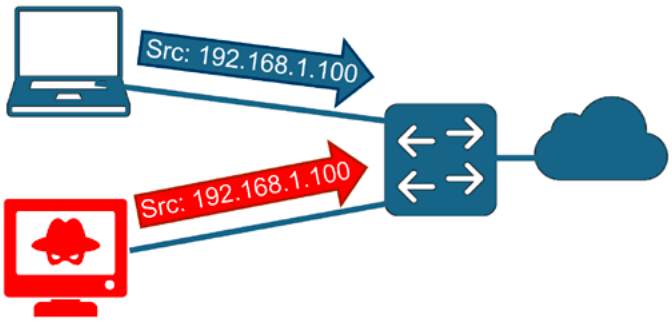
DHCP Starvation Attack Prevention

DHCP servers have a pool of available IP addresses. End devices are issued addresses from this pool. A simple Denial of Service attack involves the attacker requesting all the available IP addresses from the DHCP server. As a result, no addresses are available for genuine end devices. This is known as a Starvation Attack. Mitigating these attacks is not easy, but switches have the tools you require to block this malicious behavior.

Block attacks from DHCP Clients

Binding Tables

The Binding Table is a list of IP addresses and their corresponding MAC addresses. It is usually created via DHCP, but can also be created manually. The Binding Table is used to prevent many types of network attacks. Here are some examples. IP Address Hijacking involves the attacker requesting the DHCP server to release and reallocate an IP address which is currently being used by another device. IP Source Guard allows the switch to check that an incoming IP packet has been received on the port where the IP address is expected. Dynamic ARP Inspection will check that ARP Requests and Responses contain the correct IP/MAC address pairs, to prevent invalid ARP cache entries, known as ARP Cache Poisoning.

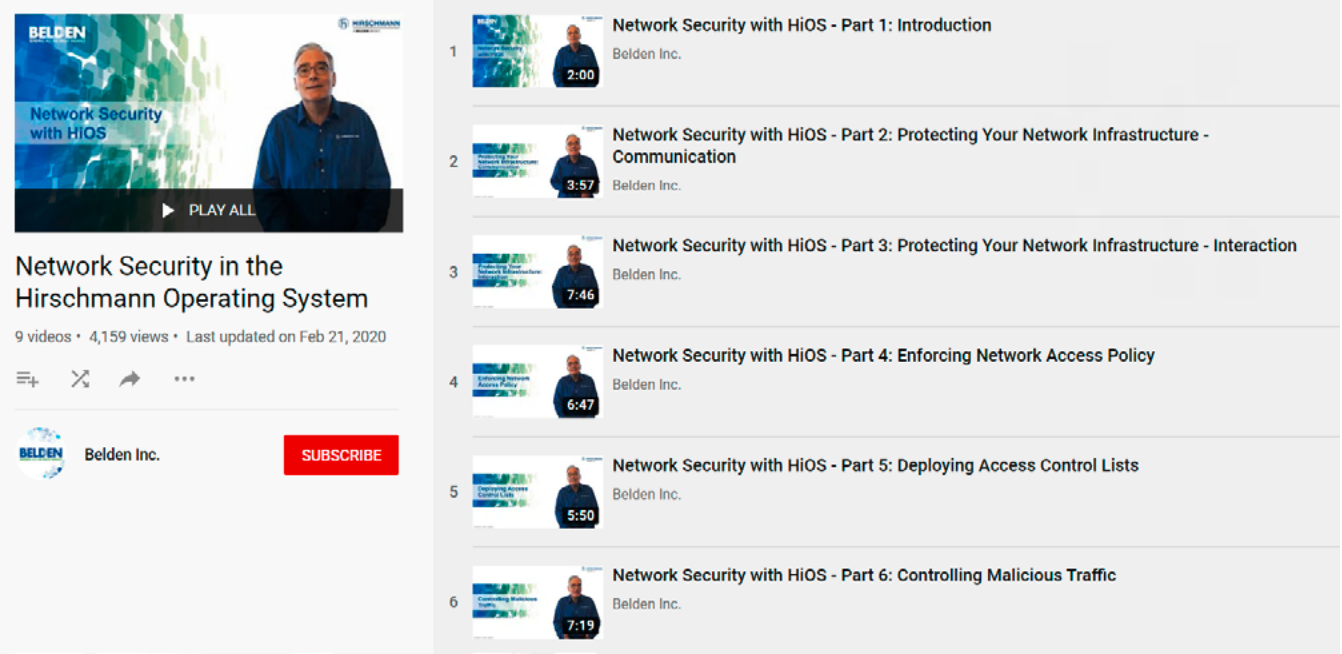


Use Binding Tables to prevent IP attacks

YouTube

Network Security Video Training @YouTube.

Visit our Belden Inc. YouTube channel and watch the training videos in the Network Security in the Hirschmann Operating System playlist.

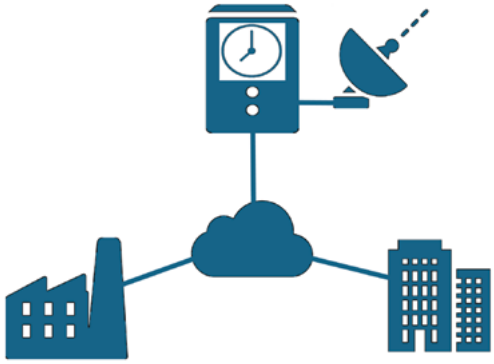


Logging Security Events

You cannot personally supervise your network 24 hours a day. Log files provide a record of activity which can help you to understand what took place in the past. This will allow you to detect threats and respond to security concerns. You can identify issues before they become problems. HiOS provides valuable logging functionality for day to day use. This can be enhanced by additional application software for short term forensic analysis or long term event correlation.

Time Server

Anyone who has ever tried to deduce meaningful information from a set of log files which have uncoordinated times and even dates, will tell you that it is an uphill struggle. But all managed switches have a Time Client, and most have a Time Server. Typically Network Time Protocol, or NTP, is used by firewalls, and Simple Network Time Protocol, or SNTP, is used by switches. Many industrial Ethernet switches offer other more accurate time protocols, but these are not required for general operation. Typically a time server will obtain the precise time from satellites. But log files do not require precise time. In fact they do not even require the correct time. Just synchronized time.



Time synchronization will make your log files meaningful

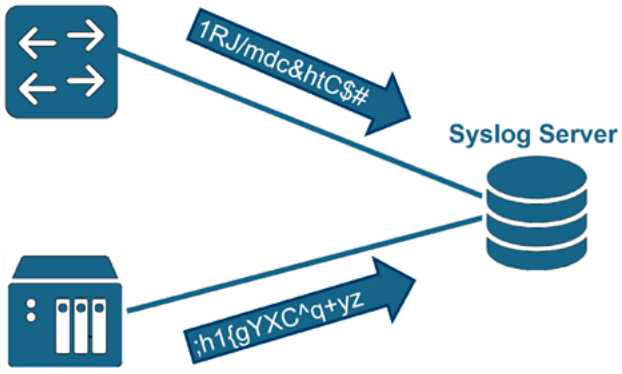
Audit Trail

Accountability is a major component of network security. In other words, who did what and when. This information is so vital, that regulatory authorities often insist that documentary evidence is available. Switches use volatile memory to store events, so this information is lost after a power cycle. External media can be used to store data persistently. But external memory media can be stolen, or its data can be erased. This method of data storage is just not persistent enough. The Audit Trail is truly permanent. The data cannot be deleted. It is stored in memory located inside the switch, which cannot be accessed. It meets the criteria for regulatory compliance. But please take note. If you borrow a switch for evaluation, bear in mind that the audit trail contains sensitive information which you cannot erase.

Permanent documentary evidence provides accountability

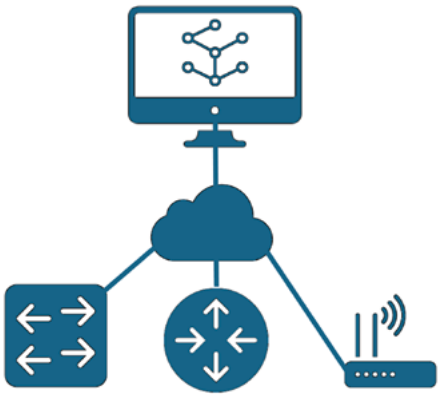
Encrypted Syslog

Syslog is an abbreviation for System Logging Protocol. It is used by network devices to send system messages to a centralized log server. The messages can be used for system-wide analysis. Syslog is a universal solution which has been in use for decades. Syslog messages can contain sensitive information about a network, which would be valuable to an attacker. Like other older protocols, it was never designed with security in mind and its messages are sent in plain text. Today, Syslog messages must be encrypted.



Raise your security level using encrypted Syslog messages

Network Management Software



Today's network management applications offer a wide range of security functionality. This is often specific to a hardware manufacturer. Fine-tuning the security functionality of your network infrastructure can be a time-consuming process, and it is easy to overlook some parameters, giving an entry path to an attacker. Network management software should provide a graphical overview of the security status of a network. Going one step further, you need the option to lock down your network with just a couple of clicks. The unauthorized connection of rogue devices is a major security risk. Your network management software will notify you and prompt for a response. If attackers can get access into your network devices, they will almost certainly change the configuration. For example, they will add their own login account to facilitate future attacks. Network management software can keep you aware of many potentially threatening scenarios.

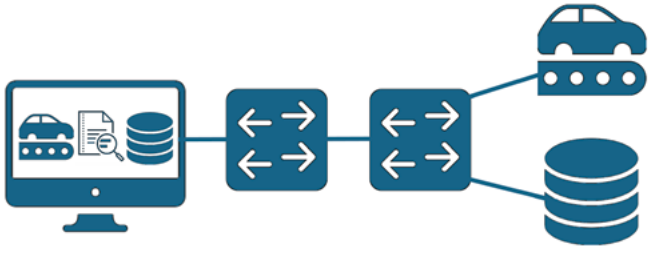
Use network management software to focus your security awareness

Syslog vs. Network Management Software

Although not strictly a security function, network administrators often ask about the relationship between Syslog servers and Network Management Systems, in terms of event handling. Syslog servers typically have a huge amount of data storage, which means that events can be recorded and analyzed over a long period of time. Syslog applications use a technique called Event Correlation. This involves analyzing the relationship between events, and then creating alarms based on user-defined rules. Network Management Systems usually save events over a short period, which make them ideal for highlighting information about what happened in the last day or two.

Both Syslog servers and Network Management Systems have their places in a modern network

Centralized Traffic Monitoring



Changes in network traffic patterns are a good indicator that something is amiss on your network. New devices appear. Devices which have never talked to each other before start communicating. Traffic loads increase. These are typical symptoms that you need to be aware of. Switches offer two methods of centrally collecting and analyzing data from remote parts of a network. sFlow randomly samples data packets and sends the samples to a central sFlow collector for analysis. Random samples are normally enough to detect irregular network activity. Remote Switch Port Analyzer, known as RSPAN, allows data from a remote switch to be copied across the network to a local destination port. As every packet is copied, this makes RSPAN an excellent tool to use in conjunction with Intrusion Detection Systems.

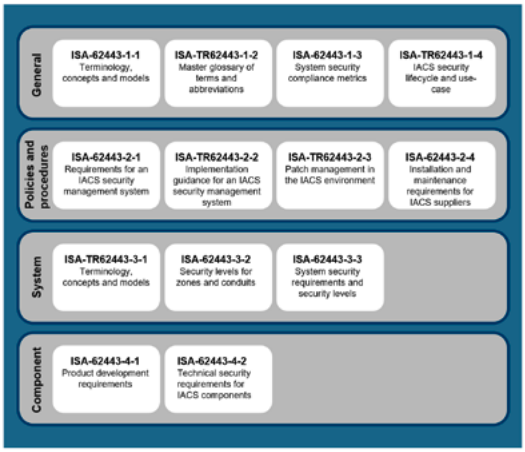
Analyze data at a central location

IEC 62443 – Independent Certification

You buy products every day. And you can be certain that each manufacturer will highlight the advantages of their products, while playing down the disadvantages. Network equipment manufacturers are no different. So how can you be certain that your switch is genuinely secure? The answer is certification. But this subject is a minefield. Every country has its own security certifications, and many industries do the same. Now there is a solution. IEC 62443 provides a certifiable framework to address security in Industrial Automation and Control Systems, across all industry sectors and critical infrastructure. Compliance with these standards is independently audited.

IEC 62443 – Security for Industrial Automation and Control Systems

Two standards are directly relevant to individual components, such as Ethernet switches. IEC 62443-4-1 is a process standard which defines a secure product development lifecycle, including security requirements definition, secure design, secure implementation including coding guidelines, verification and validation, defect management, patch management, and product end of life. IEC 62443-4-2 is a product standard which defines the cybersecurity technical requirements for components that make up an IACS, specifically the embedded devices, network components, host components, and software applications. Products can only be certified once the manufacturer has passed the development process certification.



Base your security posture on international standards

IEC 62443-4-2 Security Levels

IEC 62443-4-2 for products includes four security levels. A set of security functionality is defined for each level. This functionality is matched to the skills and motivation of an attacker. SL1 indicates that a device is resistant to unintentional mistakes made by your own employees. SL2 includes additional functionality designed to deter individual hackers who have low motivation. SL3 assumes that the attacker has knowledge of IACS systems, such as equipment and protocols, together with a malicious agenda. SL4 indicates that a device can withstand an attack by a nation state, together with all the resources that state may have. In reality, SL4 compliance is many years away, and SL3 is viewed as the optimal objective. Building your network using products that are IEC 62443 certified demonstrates your commitment to superlative cybersecurity.

Security Level	Skills	Motivation	Means	Resources
SL1 - Staff	None	Mistake	Non-intentional	Individual
SL2 - Cyber Crime, Hacker	Generic	Low	Simple	Isolated Individual
SL3 - Hacktivist, Terrorist	IACS specific	Moderate	Sophisticated (attack)	Hacker Groups
SL4 - Nation State	IACS specific	High	Sophisticated (campaign)	Multi-diciplinary teams

Select a Security Level to match the threat

Conclusion

As you have seen throughout this document, implementing network security is a process, not an action. It will happen over time. You have learned about different categories of threats to Ethernet networks, and the techniques you can implement to mitigate these risks. At this point you can now evaluate where you see the greatest challenges for your network, and plan the appropriate action.

Next Steps

So where do you go next in this process? As network attacks increase in sophistication, so do the mediation tools and strategies. Robust security must be extended to the field level. Defense in depth involves creating multiple layers of protection throughout a network, typically by using firewalls. Content Inspection allows you to permit or deny communication by looking deep into the contents of network traffic.
Network Access Control can provide precise permissions to users. If your organization is subject to regulatory compliance or industry best practices, applications exist to facilitate integrity monitoring and security configuration management. Passive scanning and agentless monitoring offer the greatest visibility into your industrial networks without disrupting live operations. Complete the process with real time threat monitoring. And remember, you are not alone. Trainers can help you to extend your knowledge, and Consultants can be with you at every step of the security process.

Continue to enhance the security of your network

Hirschmann EAGLE40
- industrial network firewall

Tofino Xenon
- industrial security appliance

tripwire®

Tripwire - cybersecurity solutions for industrial organizations

HIRSCHMANN
A BELDEN BRAND

About Belden

Belden Inc., a global leader in high quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis, USA, and has manufacturing capabilities in North and South America, Europe and Asia.

For more information, visit us at:
www.belden.com
www.beldensolutions.com
follow us on Linkedin and Facebook.

NETWORK-SECURITY-IN-THE-HIRSCHMANN-OPERATING-SYSTEM-Hirschmann-2020-06-Br-Cybr-Eng

Be certain.
Belden.