

How Can I ...

Utilize Security Features of Cisco Industrial Ethernet Switches in the Control Network?

System Technical Note
Cybersecurity

[Design
your architecture



Important information

People responsible for the application, implementation and use of this document must make sure that all necessary design considerations have been taken into account and that all laws, safety and performance requirements, regulations, codes, and applicable standards have been obeyed to their full extent.

Schneider Electric provides the resources specified in this document. These resources can be used to minimize engineering efforts, but the use, integration, configuration, and validation of the system is the user's sole responsibility. Said user must ensure the safety of the system as a whole, including the resources provided by Schneider Electric through procedures that the user deems appropriate.

Notice

This document is not comprehensive for any systems using the given architecture and does not absolve users of their duty to uphold the safety requirements for the equipment used in their systems, or compliance with both national or international safety laws and regulations.

Readers are considered to already know how to use the products described in this document.

This document does not replace any specific product documentation.

The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

Failure to follow these instructions will result in death or serious injury.

WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

Failure to follow these instructions can cause death, serious injury or equipment damage.

CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

Failure to follow these instructions can result in injury or equipment damage.

NOTICE

NOTICE is used to address practices not related to physical injury.

Failure to follow these instructions can result in equipment damage.

Note: Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction, operation and installation of electrical equipment, and has received safety training to recognize and avoid the hazards involved.

Before you begin

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions and government regulations etc. In some applications more than one processor may be required when backup redundancy is needed.

Only the user can be aware of all the conditions and factors present during setup, operation and maintenance of the solution. Therefore only the user can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, the user should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual also provides much useful information.

Ensure that appropriate safeties and mechanical/electrical interlocks protection have been installed and are operational before placing the equipment into service. All mechanical/electrical interlocks and safeties protection must be coordinated with the related automation equipment and software programming.

Note: Coordination of safeties and mechanical/electrical interlocks protection is outside the scope of this document.

START UP AND TEST

Following installation but before using electrical control and automation equipment for regular operation, the system should be given a start up test by qualified personnel to verify the correct operation of the equipment. It is important that arrangements for such a check be made and that enough time is allowed to perform complete and satisfactory testing.

WARNING

EQUIPMENT OPERATION HAZARD

- Follow all start up tests as recommended in the equipment documentation.
- Store all equipment documentation for future reference.
- Software testing must be done in both simulated and real environments.

Failure to follow these instructions can cause death, serious injury or equipment damage.

Verify that the completed system is free from all short circuits and grounds, except those grounds installed according to local regulations (according to the National Electrical Code in the USA, for example). If high-potential voltage testing is necessary, follow recommendations in the equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment
- Close the equipment enclosure door
- Remove ground from incoming power lines
- Perform all start-up tests recommended by the manufacturer

Operation and adjustments

The following precautions are from NEMA Standards Publication ICS 7.1-1995 (English version prevails):

Regardless of the care exercised in the design and manufacture of equipment or in the selection and rating of components; there are hazards that can be encountered if such equipment is improperly operated.

It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer's instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer's instructions and the machinery used with the electrical equipment.

Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

WARNING

UNEXPECTED EQUIPMENT OPERATION

- Only use software tools approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can cause death, serious injury or equipment damage.

Intention

This document is intended to provide a quick introduction to the described system. It is not intended to replace any specific product documentation, nor any of your own design documentation. On the contrary, it offers information additional to the product documentation on installation, configuration and implementing the system.

The architecture described in this document is not a specific product in the normal commercial sense. It describes an example of how Schneider Electric and third-party components may be integrated to fulfill an industrial application.

A detailed functional description or the specifications for a specific user application is not part of this document. Nevertheless, the document outlines some typical applications where the system might be implemented.

The architecture described in this document has been fully tested in our laboratories using all the specific references you will find in the component list near the end of this document. Of course, your specific application requirements may be different and will require additional and/or different components. In this case, you will have to adapt the information provided in this document to your particular needs. To do so, you will need to consult the specific product documentation of the components that you are substituting in this architecture. Pay particular attention in conforming to any safety information, different electrical requirements and normative standards that would apply to your adaptation.

It should be noted that there are some major components in the architecture described in this document that cannot be substituted without completely invalidating the architecture, descriptions, instructions, wiring diagrams and compatibility between the various software and hardware components specified herein. You must be aware of the consequences of component substitution in the architecture described in this document as substitutions may impair the compatibility and interoperability of software and hardware.

CAUTION

EQUIPMENT INCOMPATIBILITY OR INOPERABLE EQUIPMENT

Read and thoroughly understand all hardware and software documentation before attempting any component substitutions.

Failure to follow these instructions can result in injury or equipment damage.

This document is intended to describe Cisco switch security in the control network and the steps necessary to implement those features.

WARNING

UNEXPECTED EQUIPMENT OPERATION, LOSS OF CONTROL, LOSS OF DATA

The system owners, designers, operators, and those maintaining equipment utilizing Cisco security features must read, understand, and follow the instructions outlined in this document, "*How can I Utilize Security Features of Cisco Industrial Ethernet Switches in the Control Network?*".

Failure to follow these instructions can cause death, serious injury or equipment damage.

This document is intended to describe Cisco switch security in the control network and the steps necessary to implement those features. Failure to implement these features may result in network disruption.

DANGER

HAZARD OF ELECTRIC SHOCK, BURN OR EXPLOSION

- Only qualified personnel familiar with low and medium voltage equipment are to perform work described in this set of instructions. Workers must understand the hazards involved in working with or near low and medium voltage circuits.
- Perform such work only after reading and understanding all of the instructions contained in this bulletin.
- Turn off all power before working on or inside equipment.
- Use a properly rated voltage sensing device to confirm that the power is off.
- Before performing visual inspections, tests, or maintenance on the equipment, disconnect all sources of electric power. Assume that all circuits are live until they have been completely de-energized, tested, grounded, and tagged. Pay particular attention to the design of the power system. Consider all sources of power, including the possibility of back feeding.
- Handle this equipment carefully and install, operate, and maintain it correctly in order for it to function properly. Neglecting fundamental installation and maintenance requirements may lead to personal injury, as well as damage to electrical equipment or other property.
- Beware of potential hazards, wear personal protective equipment and take adequate safety precautions.
- Do not make any modifications to the equipment or operate the system with the interlocks removed. Contact your local field sales representative for additional instruction if the equipment does not function as described in this manual.
- Carefully inspect your work area and remove any tools and objects left inside the equipment.
- Replace all devices, doors and covers before turning on power to this equipment.
- All instructions in this manual are written with the assumption that the customer has taken these measures before performing maintenance or testing.

Failure to follow these instructions will result in death or serious injury.

The STN collection

The implementation of an automation project includes five main phases: Selection, Design, Configuration, Implementation and Operation. To help you develop a project based on these phases, Schneider Electric has created the Tested, Validated, Documented Architecture and System Technical Note.

A Tested, Validated, Documented Architecture (TVDA) provides technical guidelines and recommendations for implementing technologies to address your needs and requirements. This guide covers the entire scope of the project life cycle, from the Selection to the Operation phase, providing design methodologies and source code examples for all system components.

A System Technical Note (STN) provides a more theoretical approach by focusing on a particular system technology. These notes describe complete solution offers for a system, and therefore support you in the Selection phase of a project. The TVDAs and STNs are related and complementary. In short, you will find technology fundamentals in an STN and their corresponding applications in one or several TVDAs.

Development environment

Each TVDA or STN has been developed in one of our solution platform labs using a typical PlantStruxure architecture.

PlantStruxure, the process automation system from Schneider Electric, is a collaborative architecture that allows industrial and infrastructure companies to meet their automation needs while at the same time addressing their growing energy efficiency requirements. In a single environment, measured energy and process data can be analyzed to yield a holistically optimized plant.

Table of contents

1.	Introduction	13
1.1.	<i>Purpose</i>	13
1.2.	<i>Customer Challenges</i>	14
1.3.	<i>Prerequisites</i>	16
1.4.	<i>About this document</i>	16
1.5.	<i>Glossary</i>	16
2.	Selection	17
2.1.	<i>Selection Criteria</i>	17
2.2.	<i>Where is Security Required?</i>	17
2.3.	<i>Safeguarding the Device – Device Hardening</i>	18
2.4.	<i>Safeguarding Network Data</i>	19
3.	Design	35
4.	Implementation	37
4.1.	<i>Management Plane</i>	37
4.2.	<i>Control Plane</i>	44
4.3.	<i>Data Plane</i>	49
5.	Validation	71
5.1.	<i>General Operational Tests</i>	71
5.2.	<i>Security Feature Tests</i>	75
5.3.	<i>Performance Criteria</i>	78
6.	Conclusion	79
7.	Appendix	81
7.1.	<i>Glossary</i>	81
7.2.	<i>Bill of Material and Software</i>	83
7.3.	<i>Reference Documents</i>	84
7.4.	<i>Security Functions outside the scope of this document</i>	84

1. Introduction

1.1. Purpose

This System Technical Note (STN) provides guidelines to help you implement security features that are resident in equipment added to a control network, where that network also includes Cisco switches. Use the information presented by this document in combination with previously published STNs and TVDAs that focus on cybersecurity:

- STN – *How Can I Reduce Vulnerability to Cyber Attacks?*
- TVDA – *How can I Reduce Vulnerability to Cyber Attacks in the Control Room?*
- TVDA – *How Can I Reduce Vulnerability to Cyber Attacks in the Functional Unit?*

This document complements these earlier publications and is written specifically for customers that have Cisco switches in the control network.

Schneider Electric recommends a defense-in-depth approach to cybersecurity. The defense-in-depth approach, conceived by the United States National Security Agency (NSA), layers the network with security features, appliances, and processes.

As shown in Figure 1, the Schneider Electric defense-in-depth approach integrates a set of related process and system components to provide higher levels of security in a PlantStruxure network.

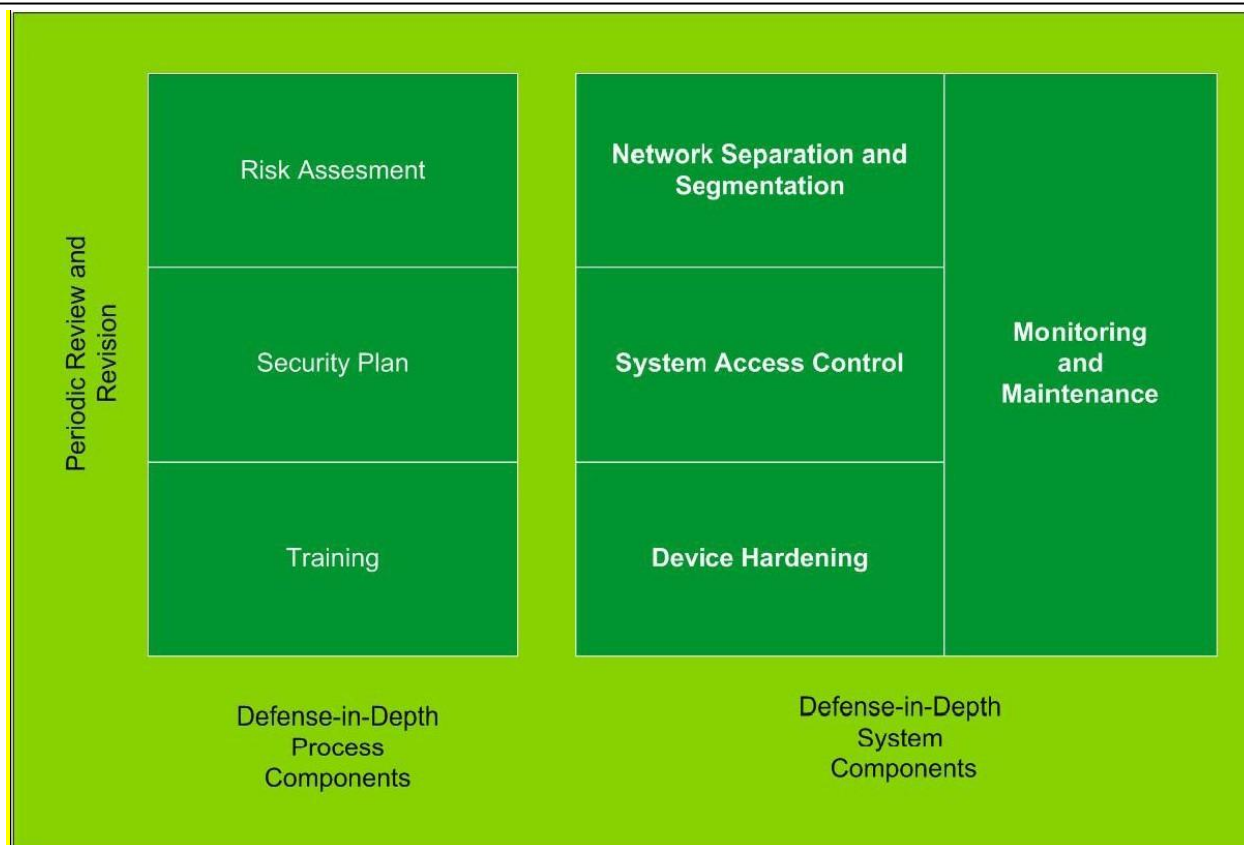


Figure 1: PlantStruxure Network Defense-in-Depth Components

1.2. Customer Challenges

Attempting to secure an industrial automation (IA) network can be a daunting process. As network complexity increases, so do points of vulnerability. Security is no longer a secondary consideration in the world of industrial controls. It is as important as safety or high availability. Industrial control systems, based on computer technology and industrial-grade networks, have been in use for decades. Earlier control system architectures were developed using proprietary technologies and were isolated from the outside world. In many cases, physical perimeter security was deemed adequate, while cybersecurity was not a significant concern.

Today many control systems use open or standardized technologies – such as Microsoft Windows operating systems and Ethernet TCP/IP – to reduce costs and improve performance. Many systems also employ direct communications between control and business systems to improve operational efficiency and more cost-effectively manage production assets.

This technical evolution exposes control systems to vulnerabilities previously thought to threaten only office and business computers. Control systems are now vulnerable to cyber attacks from both inside and outside the industrial control system network.

Security challenges for the control environment include:

- Diverse physical and logical boundaries.
- Multiple sites that span large geographic areas.
- Adverse effects of security implementation on process availability.
- Increased exposure to worms and viruses migrating from business systems to control systems as communication between these systems becomes more frequent.
- Increased exposure to malicious software from USB devices, vendor and service technician laptops, and the enterprise network.
- Direct impact on the control systems and network devices.

No longer are fences and security guards adequate to safeguard industrial assets. Companies must be diligent in the steps they take to help secure their systems. A successful cyber attack can result in lost production, damaged company image, or environmental disaster. The controls industry and its customers need to apply cybersecurity lessons learned from the IT world.

1.3. Prerequisites

You will benefit from a basic knowledge of these product and applications:

- Ethernet switching and routing
- Cisco industrial Ethernet products
- Network security concepts

1.4. About this document

This document describes a set of features you can use to help secure the control network in PlantStruxure architectures. These features are available in Cisco switches and routers. The features mentioned in the document are specific to Cisco switches. We recommend that you incorporate the guidelines set forth in this document into your overall security policy, which should be well documented and understood by personnel who design, implement, and maintain operational technologies (OT). Policies such as hardening devices, securing access, and encrypting and isolating traffic are the main considerations.

1.5. Glossary

A glossary (section 7.1.) is available in the appendix of this document. Please refer to it whenever necessary.

2. Selection

2.1. Selection Criteria

Several alternative security technologies can be used in different scenarios and architectures. This section discusses technologies, which are available in Cisco equipment, that enhance security of the PlantStruxure control network. Not all security options and technologies offered by Cisco equipment are included in this paper. Only those technologies that are most relevant to industrial implementations are discussed.

NOTE: Schneider Electric recommends that you implement all the features described in this section on your Cisco switches.

2.2. Where is Security Required?

Depending on the situation, security may be required at different levels of physical and logical segments of the network. Of course, there are some general guidelines that should be implemented in every case, like device hardening by using passwords and disabling unused services. In addition, other measures can be taken to help prevent unauthorized access to the network devices or to the data itself. The next sections cover two topics: device hardening, and features of the Cisco IE switches that help protect data.

Using the defense-in-depth strategy, security is required across the entire PlanStruxure architecture. The architectures that follow the PlantStruxure scheme are scalable, and operate from simple to complex network architectures. The diagram below demonstrates the PlantStruxure architecture:

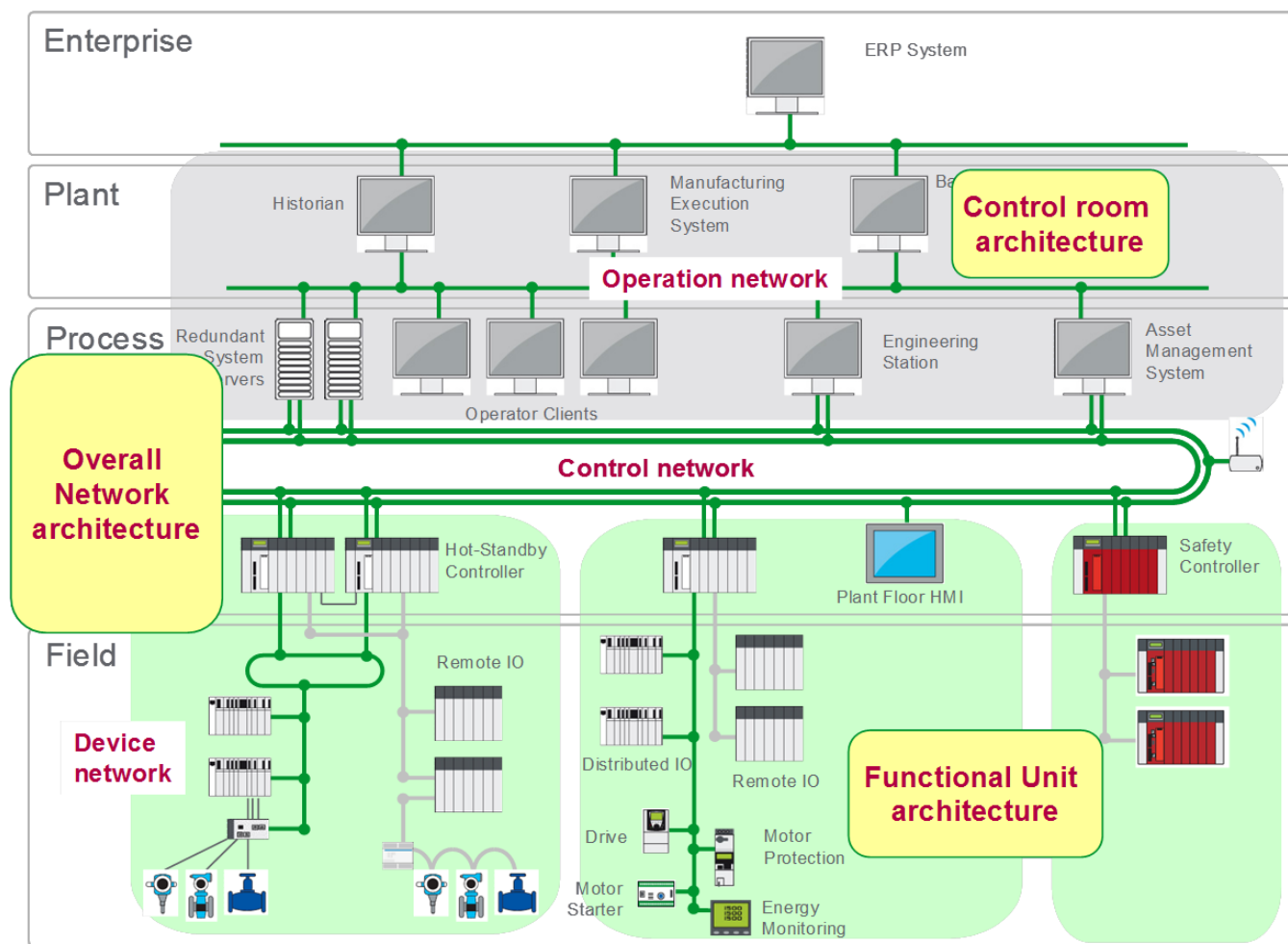


Figure 2: PlantStruxure architecture concept

2.3. Safeguarding the Device – Device Hardening

Device hardening includes any measure that denies access to the Cisco switch by someone unauthorized to do so. The goals of device hardening include: the prevention of unauthorized changes to the device configuration, and the denial of access to the data that is transmitted.

Implement the following basic steps, regardless of the network architecture, to help harden the devices:

- Assign usernames and passwords. Cisco devices introduce the added feature of privilege levels, which makes it possible to grant different degrees of access to different users. Cisco devices include 15 levels with level 15 granting full access, and level 1 granting only basic access to view - but not edit - configuration parameters.
- Match the assigned usernames and passwords to a specific access method. For example, accessing a switch through the console, or via a remote command line interface (CLI) or web access, can require different username and password combinations.

Authentication, therefore, has to be separately configured for each of these different methods of access.

- Disable all unused ports. All ports that are not used and are not connected to any device should be administratively shut down.
- Disable all unused services. Devices have many legacy services running by default. They are also known as “small servers”. The ones that are not used should be disabled as they present a possible point of entry.
- Enable encryption for remote access to the switch. For HTTP access using the device manager, use SSL to encrypt the traffic. For remote CLI access, use secure shell (SSH), but avoid using telnet. To modify parameters or features of the device, require a user to enter an “enable” command to edit configuration settings. An elevated “enable” password should be required to restrict access even from the console port.
- Configure an access-list in all access types (VTY, HTTP) to permit management access only from specific hosts.
- Help protect management traffic. There are many ways do this, which will be discussed later. Management traffic uses the native VLAN to transfer data related to management protocols such as STP, OSPF, etc.
- Prune VLAN traffic. By default, when a port is configured as TRUNK, all the VLANs that exist in the switch database are allowed to pass through the port. A better approach is to permit only necessary, specific VLAN traffic to pass through each trunk port.

2.4. Safeguarding Network Data

This section identifies features that help protect data in the control network from unauthorized network access, unintended network disruption such as a network operator error, and direct attacks from hackers.

2.4.1. Protocol Authentication

Today's plant networks generally rely on static routing. Static routing is implemented using manually entered data to create a route table for the device, which references this data when forwarding data packets. While simple to configure, static routing is most effective in a small network such as a plant network. As devices or functional units are added to the network, dynamic routing such as OSPF and HSRP may be alternatives that provide redundancy coupled with reduced network maintenance. Because static routers do not share information with each other, you need to manually enter topology changes to each router. Dynamic routing protocols such as OSPF exchange information between the routers, so any topology change is managed by the routers working in concert. In addition, OSPF offers authentication mechanisms that can help secure the PlantStruxure control network.

Authentication should not only be used for device hardening with the help of passwords, but also in protocols applied to the network. Most protocols – like OSPF, HSRP, even the new versions of SNMP – support password protected authentication, which should always be used.

Authentication can help prevent an attacker from creating neighbor relationships with network elements and read or manipulate the network data or configurations.

Authentication usually implies the use of a password to access the device itself, but many protocols that transport information among devices also support authentication. An example is the Open Shortest Path First (OSPF) routing protocol, which uses MD5 authentication. MD5 authentication helps prevent an attacker from joining the OSPF area and influencing the routing updates. An example is shown in the following figure:

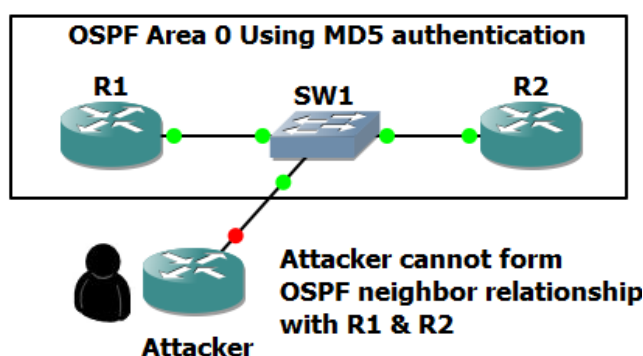


Figure 3: OSPF protocol with MD5 authentication

In this example, the OSPF packets are encrypted using a password. When the attacker tries to establish a neighbor relationship with R1 and R2, the two routers will reject the attacker's packet because the hash produced with MD5 will not match the expected hash.

The OSPF protocol, defined in RFC 2328, is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System. OSPF is a link-state protocol. A link is considered to be an interface on the router. The state of the link is a description of that interface and of its relationship to its neighboring routers. A description of the interface would include the IP address of the interface, the mask, the type of network it is connected to, the routers connected to that network, etc. The collection of all these link-states forms a link-state database.

OSPF uses an algorithm – the Dijkstra algorithm – to build and calculate the shortest path to all known destinations. The algorithm by itself is quite complicated. The following is a very high level, simplified way of looking at how the algorithm is used.

Upon initialization or in response to any change in routing information, a router generates a link-state advertisement. This advertisement represents the collection of all link-states on that router. All routers exchange link-states by means of flooding. Each router that receives a link-state update stores a copy in its link-state database and then propagates the update to other routers.

After the database of each router is updated, the router uses the Dijkstra algorithm to calculate a shortest path tree to all destinations. The destinations, the associated cost, and the next hop to reach those destinations form the IP routing table.

If no changes in the OSPF network occur, such as cost of a link or a network being added or deleted, OSPF is very quiet. When changes occur, they are communicated through link-state packets, and the Dijkstra algorithm is used to calculate the shortest path.¹

2.4.2. VLANs

Traffic separation is an indispensable part of a security strategy. Devices that need to communicate to each other frequently, like devices in a functional unit, should be grouped together. VLANs separate the broadcast domains at layer 2 by restricting a communication to the VLAN. One VLAN cannot “see” traffic from another VLAN.

- As depicted in the following figure, this means that PACs in VLAN 10 cannot communicate with PACs in VLAN 20. Also, the attacker in the guest VLAN cannot communicate with PACs in either VLAN 10 or 20. If inter-VLAN communication is desired, for example between VLANs 10 and 20, it can be accomplished with the use of a router. A router can further control communication flow by means of an access list, which will be examined in the next section.

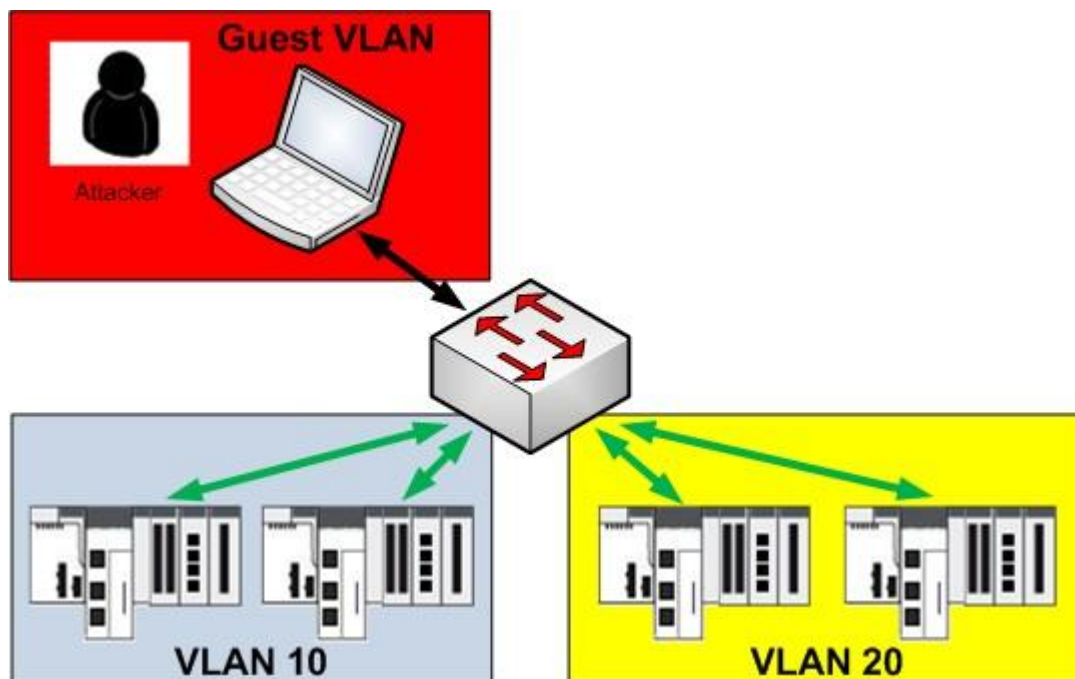


Figure 4: VLAN traffic separation

¹ <http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>

In addition, management of the devices should be implemented through the use of a separate management VLAN. Cisco switches use a specific VLAN for inter-switch communication. Transmissions of link state information, spanning- tree topology notifications, and routing information are sent via this management VLAN. This management VLAN is referred to as the Native VLAN and, in Cisco devices, is VLAN 1 by default. No process control or functional unit VLAN should be assigned the reserved name of VLAN1.

2.4.3. Access Lists

Access lists give advanced control over traffic flow. With an access list, firewall-like rules can be created on a layer 3 switch or on a router to block or allow traffic between hosts or networks. Access lists contain a sequence of permit or deny statements; the layer 3 switch or router examines each packet to determine if it meets the stated criteria. The statements are sequentially processed. Each statement is assigned a number, and the statements are processed in ascending order.

Access lists perform packet filtering to control which packets move through the network and where they go. Such control can help limit network traffic and restrict the access of users and devices to the network. Access lists have many uses, and therefore many commands accept a reference to an access list in their command syntax. Access lists can be used to do the following:

- Filter incoming packets on an interface.
- Filter outgoing packets on an interface.
- Restrict the contents of routing updates.
- Limit debug output based on an address or protocol.
- Control virtual terminal line access.
- Identify or classify traffic for advanced features, such as congestion avoidance, congestion management, and priority and custom queuing.²

Access lists are applied on an interface for inbound or outbound traffic. Because there are two kinds of interfaces (routed and switched virtual interface), there are also different kinds of access lists. Although the configuration between access lists that are attached to a physical interface is a little different than the ones applied to VLANs, the logic behind them is the same.

² http://www.cisco.com/c/en/us/td/docs/ios/12_2s/feature/guide/fsaclseq.html

Access lists can be configured as either:

- Standard access lists, that match traffic only according to the source IP address.
- Extended access lists, that offer advanced matching criteria based on source and destination addresses, protocol type and port number.

Used in concert with VLANs, access lists control traffic flow at layer 3. As shown in Figure 5, below, if inter-VLAN communication between VLAN 10 and 20 is desired, the router can be configured to allow traffic to be routed between networks 192.168.1.0 and 192.168.2.0 and block all other traffic. This helps prevent other traffic, like traffic from the guest VLAN, to be routed to the PAC VLANs.

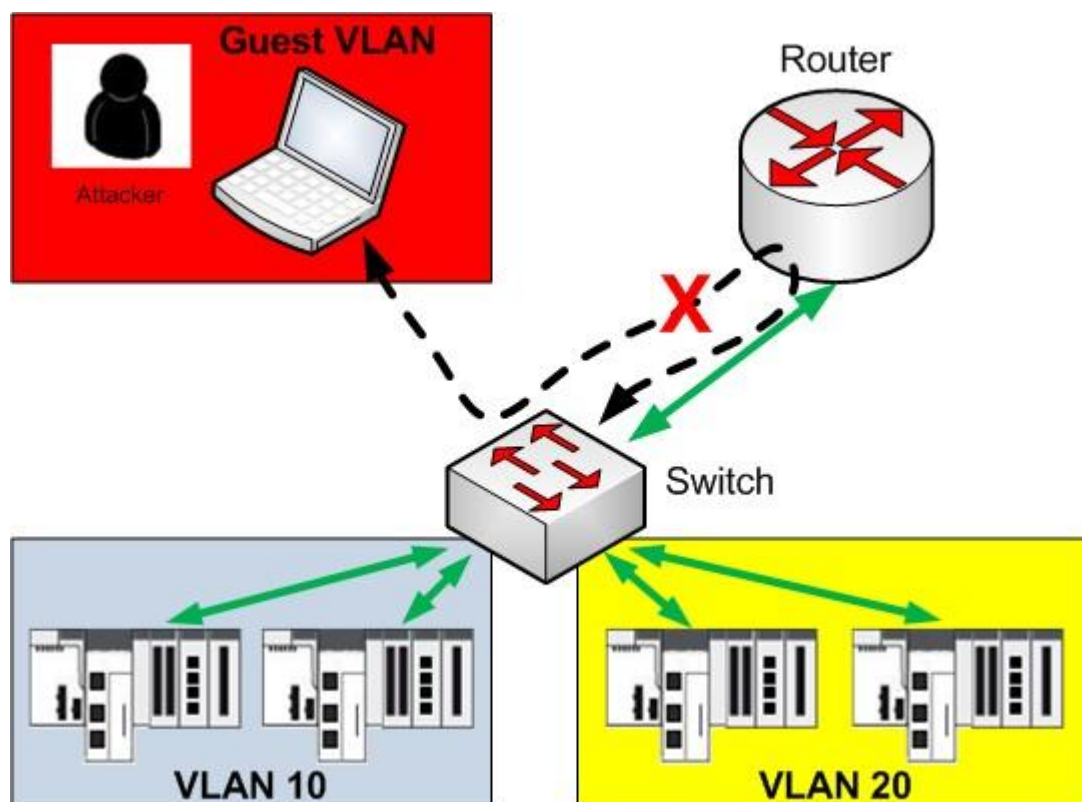


Figure 5: Access list control of VLAN traffic flow

2.4.4. Encryption

Encryption is the “masquerading” of data as it traverses the network. Encryption helps prevent an attacker from accessing the actual data if they successfully “hack” the network. This is performed by using a mathematical formula to encrypt and then decrypt the data. In the design described in this paper, a site to site VPN connection is configured to emulate a process network that is physically distant from both the control station and the SCADA.

Encryption is also used if the physical medium cannot be easily safeguarded or the connection is accomplished through the public internet. In these scenarios, all the traffic between the control and process network should be encrypted to help prevent unauthorized access to the transmitted information.

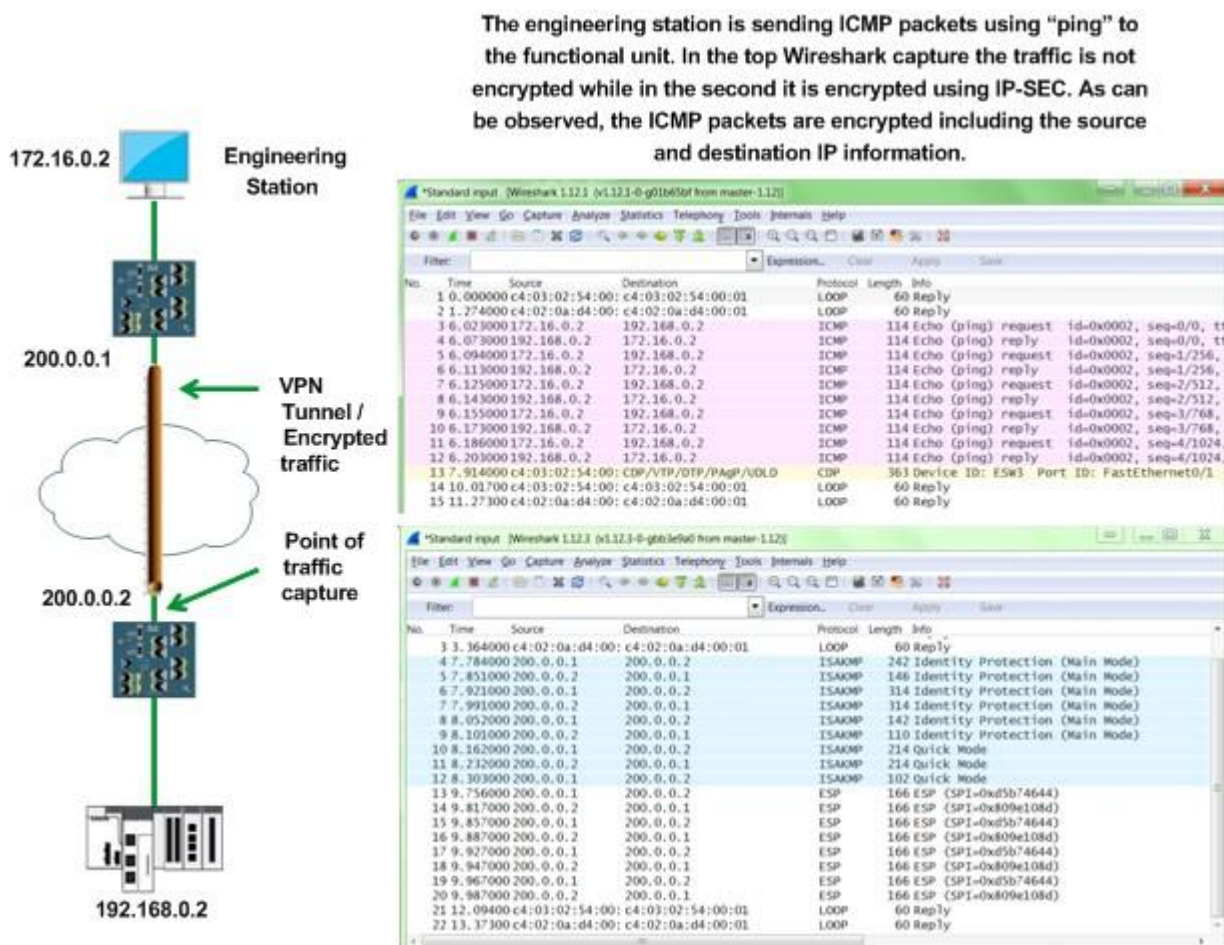


Figure 6: Encrypted versus non-encrypted Ethernet packets

Cisco uses the Internet Engineering Task Force (IETF) IPSec framework as its encryption standard. This framework acts at the network level (Layer 3) and implements the following standards:

- IPSec
- Internet Key Exchange (IKE)
- Data Encryption Standard (DES)
- MD5 (HMAC variant)
- SHA (HMAC variant)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

IPSec services provide a robust security solution that is standards-based. IPSec also provides data authentication and anti-replay services in addition to data confidentiality services. Data authentication provides two verification functions: that the data has not been altered, and that the information has been sent by the originator.

Anti-replay services allow the receiver to reject old or duplicate packets to safeguard itself against a “replay attack”. A replay attack occurs when valid data is maliciously repeated or delayed. Anti-replay services help prevent eavesdropping by a hacker to obtain a user’s confidential information such as a private key or password.

IPSec is documented in a series of Internet Drafts, all available at:

<http://www.ietf.org/html.charters/ipsec-charter.html>

2.4.5. Port Security

Port security is a technology used in Cisco switches that helps prevent attackers from connecting to an open switch, then using a spoofed MAC address to masquerade as a known device. Port security also helps stop MAC flooding attacks. Switches use a MAC forwarding table to map MAC addresses to specific switch ports and forward frames only over the appropriate ports without flooding the traffic to all ports. Often this table can be configured for maximum capacity of 2 addresses per port. In the absence of port security, a hacker can transmit a large number of fake MAC addresses, filling the table and flooding the network. This can cause extreme network performance degradation.

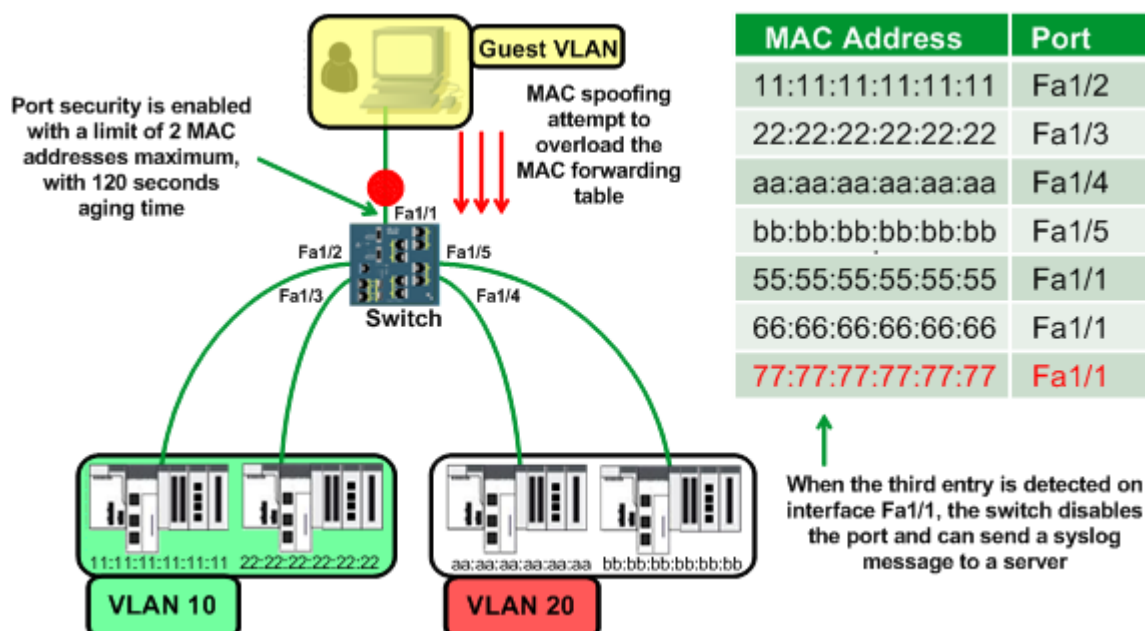


Figure 7: Limiting port access to known MAC addresses

Pre-approved MAC addresses are stored in the address table. When the switch port exceeds the number of assigned MAC addresses, a security violation is recorded. The violation can trigger a pre-configured responsive action. The possible actions are:

- Protect – unknown source address is dropped.
- Restrict – unknown source address is dropped; a syslog message is recorded; an SNMP trap is sent, and the violation counter increments.
- Shutdown – interface becomes disabled; the Port LED turns off; a syslog message is recorded; an SNMP trap is sent, and the violation counter increments.
- Shutdown VLAN – the VLAN under attack is disabled, and the port continues to function.

In an IA network the recommendation would be to shutdown the port. Most IA networks have a very specific and controlled configuration. Any violations to that configuration should be flagged immediately.

Entries are placed in the address table via 3 different mechanisms:

- Static secure MAC address – manually configured in the address table and stored in the running configuration.
- Dynamic secure MAC address – dynamically configured in the address table and removed when the switch restarts.
- Sticky secure MAC address – dynamically learned or manually configured in the address table and the running configuration. On a restart the port does not need to dynamically configure.

Implement port security for a switch port that experiences little or no end device changes. A switch port dedicated to process automation is a good example of this, as field devices and control network systems rarely change.

2.4.6. MAC Move Notifications

The MAC move function sends a notification, usually to a syslog server (more on this later in this document), when a device is detected to have connected to a port other than the port to which the device was originally connected. Use MAC Move notifications to help prevent an unknown user or a hacker from gaining to access the network over different switch ports. When this situation is detected, a security violation is triggered. Similar to the Port Security feature, the possible actions are:

- Protect – unknown source address is dropped.
- Restrict – unknown source address is dropped; a syslog message is recorded; an SNMP trap is sent, and the violation counter increments.
- Shutdown – interface becomes disabled, the Port LED turns off; a syslog message is recorded; an SNMP trap is sent, and the violation counter increments.
- Shutdown VLAN – the VLAN under attack is disabled, and the port continues to function.

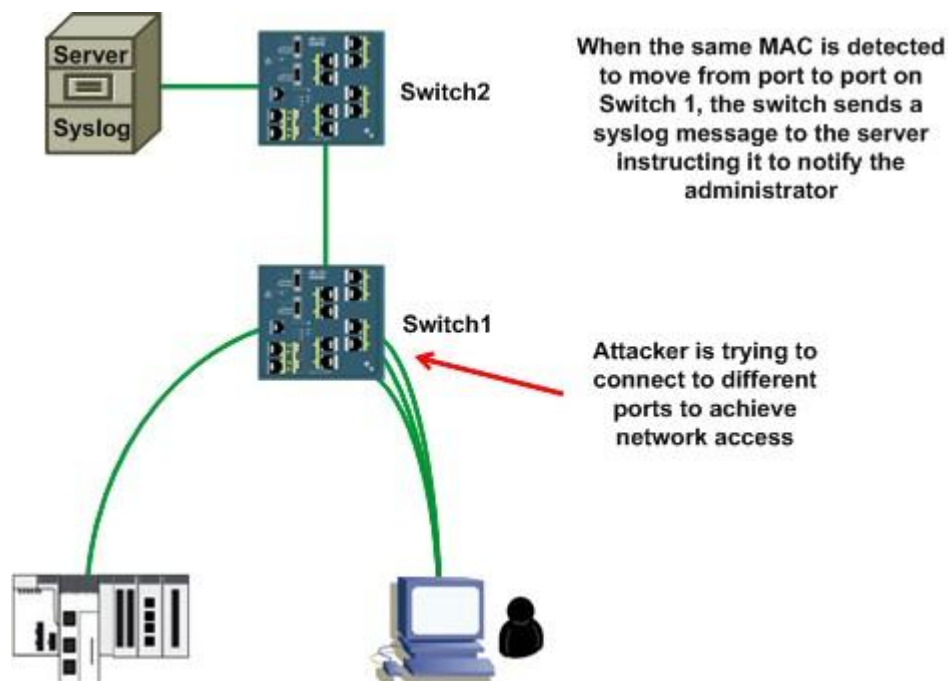


Figure 8: Switch sends MAC move notification of attempts to connect via different ports

2.4.7. Storm Control

Storm control is a traffic control mechanism in Cisco switches. The switch can be configured on a per-port basis to block unicast, broadcast, multicast, or any combination of traffic above a configurable threshold. Ports that are connected to broadcast sensitive devices such as a PAC can be configured to use this feature. Storm control does not block any management traffic, thus does not affect the operation of the switches.

CPU overload on a switch can occur when it is flooded with Address Resolution Protocol (ARP) packets. Storm control can be enabled to set a threshold for the percent of packets received or the bits per second received. When that threshold is reached or exceeded, the switch drops all packets received on that port for 30 seconds. After that the rate is again measured and storm control is reapplied if the threshold is reached. The port can also be disabled permanently or for a set amount of time. Configuration also permits a trap to be sent to an SNMP manager.

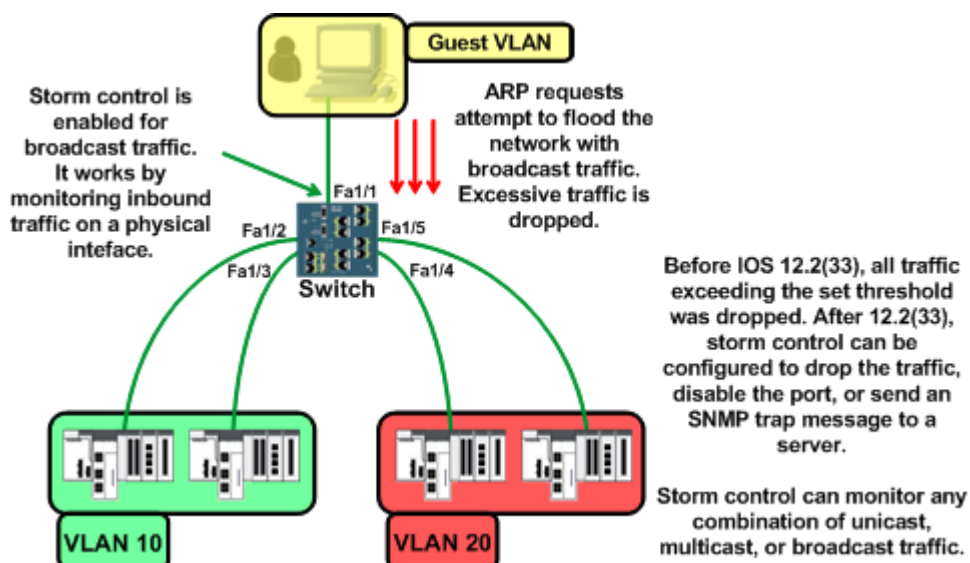


Figure 9: Using storm control to repel an ARP flooding attack

2.4.8. Blocked / Protected Ports

Switch ports designated as “protected” cannot communicate with each other; they can only communicate with ports designated as “unprotected”. This can be useful; for example, when connecting devices (such as PACs and cameras) to a single switch that have no need to communicate to each other. The performance degradation from intentionally or accidentally created excess broadcast traffic can be limited using this feature.

The limitation of this technology is that the protected status of ports has only a local significance: it applies to the local switch, but does not extend to other switches. A protected port on switch A can communicate with a protected port on switch B.

Protected ports work on unicast, broadcast or multicast traffic. Forwarding of packets between protected and unprotected ports continues as usual. This is a helpful feature for a switch where one port carries security information such as bandwidth intensive video, while another port carries IA traffic. In this case if both are protected ports, they never see the other's traffic.

By default, the switch floods packets with unknown destination MAC addresses out of all ports. If unknown unicast and multicast traffic is forwarded to a protected port, there could be possible security issues. To help prevent unknown unicast or multicast traffic from being forwarded from one port to another, you can block a port (protected or unprotected) from flooding unknown unicast or multicast packets to other ports.³

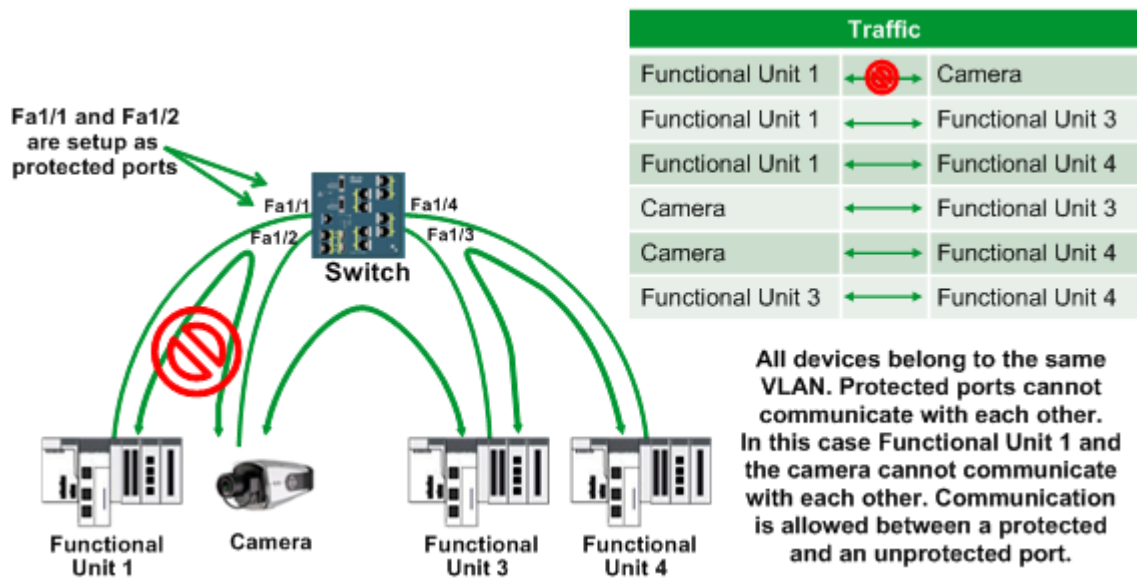


Figure 10: Protected ports segregate functional units 1 & 2

2.4.9. Loop Guard / BPDU Guard / BPDU Filter / Root Guard

These features are designed to mitigate attacks against the Spanning Tree Protocol. Bridge Protocol Data Units (BPDUs) are layer 2 advertisements that are sent on the ports between interlinked switches. BPDUs help maintain the integrity of the network by helping to prevent the creation of loops that can cripple the network. By default they are sent every 2 seconds.

An unintentional change to the network or a hacker's attempt to disrupt the network by invoking topology changes could cause a loop, thereby rendering the network inoperable. The following features are designed to guard against such attacks.

- Loop Guard: When enabled, it stops the blocked port in the RSTP ring from transitioning to a forwarding state in response to an error detected on another switch and thereby

³ Cisco IE 2000 Switch Software Configuration Guide Cisco Press, July 2012 p32-4

creating a network loop. The port is designated to be in *loop inconsistent* state and continues to block traffic.

- BPDU Guard: Enabled on access ports that shouldn't receive BPDU packets. If a packet is received, the port is disabled.
- BPDU Filter: Causes the switch to drop BPDU packets received by the interface configured with BPDU Filter. Use this feature along with Loop Guard to help prevent creating a loop in the network.
- Root Guard: Designed to safeguard the integrity of the network and keep the root bridge in control. It is configured on a per port basis. In the example below, root guard is enabled on the root bridge port and all the other switch ports that are participating in the RSTP ring. If packets with lower priority are received, signaling a change of the root bridge, the port is set to **err-disabled** state until the BPDUs are no longer received

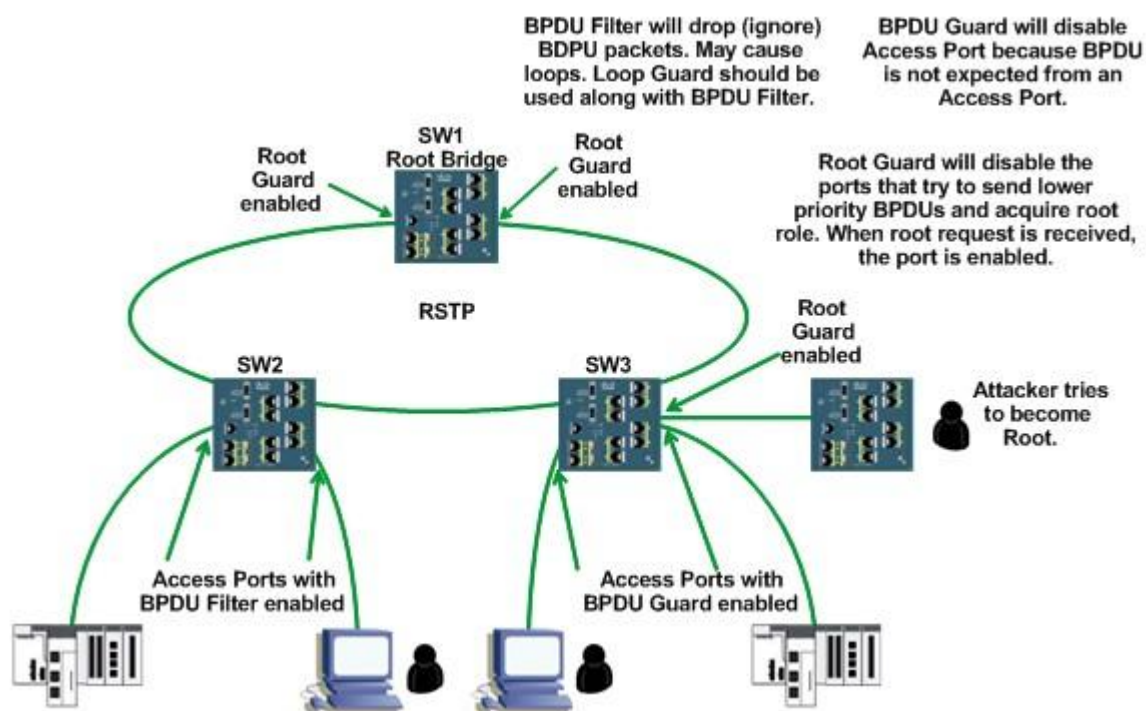


Figure 11: Guarding against attacks on the Spanning Tree Protocol

2.4.10. Logging

Maintaining a record of all events is an indispensable element of security implementation. Logging facilitates an accounting of all actions taken or attempted, including access attempts and configuration changes. Logging is the recommended way to detect unauthorized access, attack patterns, and failed access attempts. It can provide valuable forensics information in the event of a successful attack by a hacker. Devices perform logging by sending all events to a logging server. In this document, syslog will be the protocol of choice for logging with Syslog Watcher software.

Logging of security events is a prerequisite to monitoring and maintaining the IA network. Logging provides a timestamp for events, which can be displayed on a monitor or an HMI. Some logging software tools can trigger responsive events, such as notification to the operation staff by email, phone or pager.

Syslog is an IETF RFC2524 standard. Each syslog message includes a facility code and a severity indicator. The facility code is standardized in IETF RFC3164.

Syslog applies the user datagram protocol (**UDP**) as its underlying transport layer mechanism. The UDP port assigned to syslog is **514**.

The total length of the packet, including message, cannot exceed **1024** bytes. There is no minimum syslog message length.

Each syslog message includes one of the following severity level indicators:

- 0 = **Emergency**: system is unusable
- 1 = **Alert**: action must be taken immediately
- 2 = **Critical**: critical condition
- 3 = **Error**: error condition
- 4 = **Warning**: warning condition
- 5 = **Notice**: normal but significant condition
- 6 = **Informational**: informational messages
- 7 = **Debug**: debug-level messages

The definition of severity levels – other than Emergency and Debug – are determined by, and specific to, the application written for the device by its vendor, which in this example is Cisco. By default, all messages are sent to the physical console of a device. Cisco devices can be configured to send all syslog events to a syslog server. Cisco uses a message format that is compatible with a standard Unix platform. In the example architecture, there are Microsoft Windows based software applications – such as SMNPSoft Syslog Watcher – that also support syslog messages. These packages are very robust and feature numerous capabilities for monitoring and maintenance.

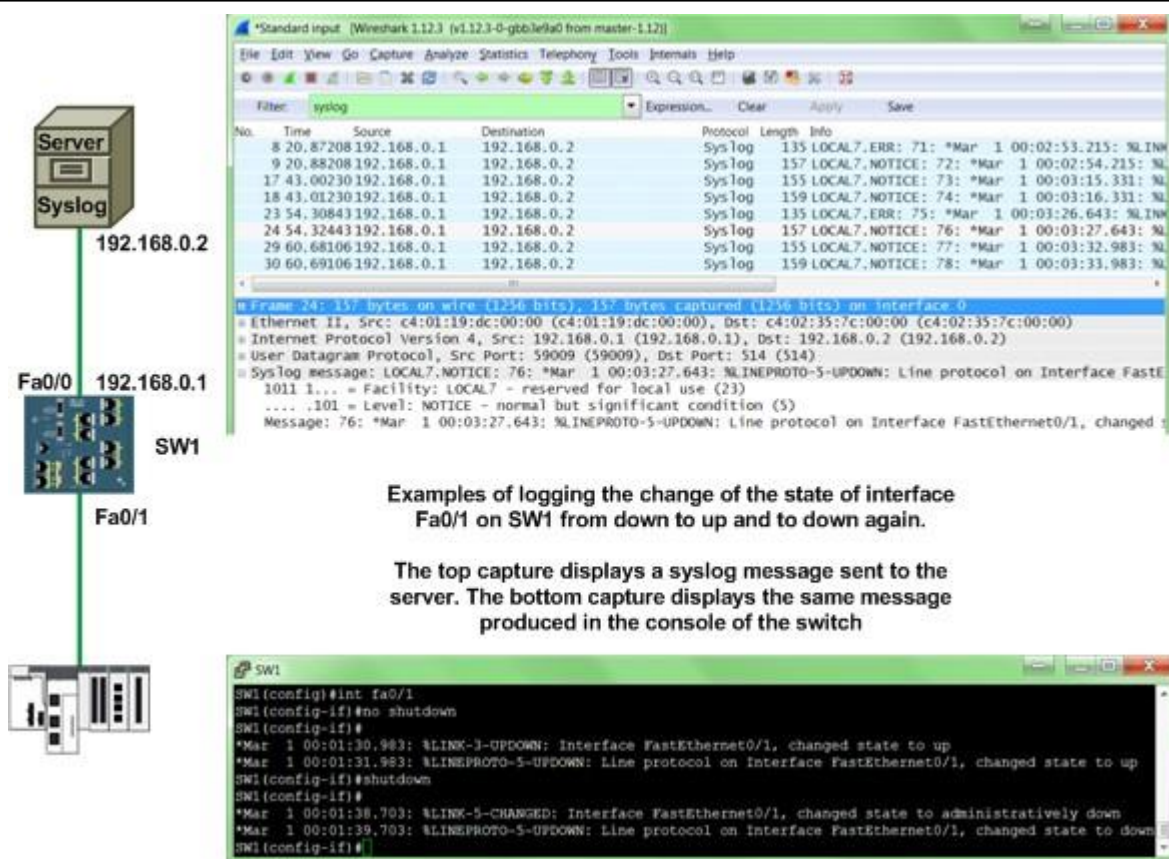


Figure 12: Logging events

2.4.11. NTP

Network Time Protocol (NTP) is an IETF RFC1305 standard that provides time synchronization for network devices. NTP is an important element of cybersecurity, because it provides an accurate timestamp for logging of network events to the syslog server. This is vital in a network forensic situation when determining the exact sequence of events that occurred on the PlantStruxure control network. Time synchronization establishes accuracy among device clocks on an Ethernet system. For example, the clock of one client may be synchronized either with another server, a referenced time source such as a radio or satellite receiver, or a GPS time server. Typical time service configurations use redundant servers and diverse network paths to establish high accuracy and reliability. Time service accuracy can be within a millisecond on LANs and within tens of milliseconds on WANs. Use the time synchronization service for:

- Event recording (for example, tracking a sequence of events).
- Event synchronization (for example, triggering simultaneous events).
- Alarm and I/O synchronization (for example, time stamping alarms).

The time synchronization service offers:

- Periodic time corrections obtained from the reference standard, for example, the NTP server.
- Automatic switchover to a backup time server if the normal server ceases to function.
- Local time zone configurable and customizable settings (including daylight saving time adjustments)

The protocol uses UDP packets on port number 123.

The National Institute of Standards and Technology provides a list of Internet Time Servers at the following link: [List of available time servers](#). This page also provides information about the protocol and a Windows application to use when synching your computer to an internet time server.

The Modicom M580 can be used as a NTP server or a client. It has a resolution time of 1ms.

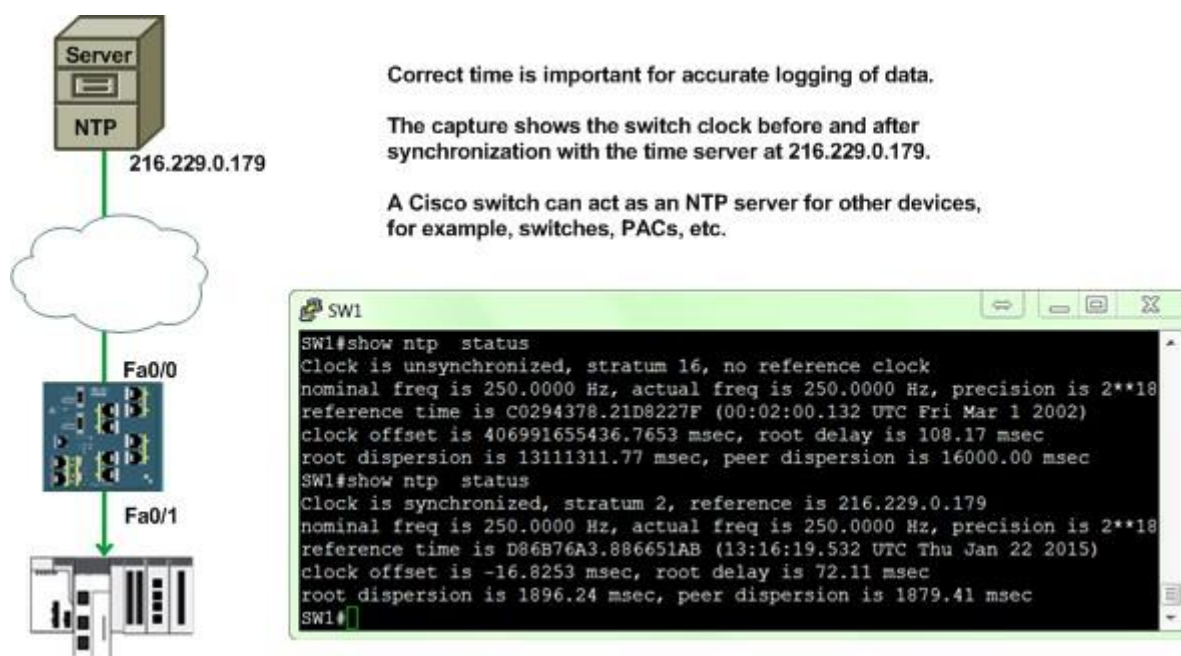


Figure 13: NTP service

2.4.12. DHCP Snooping / Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) determines the validity of an ARP packet based on a trusted database. It uses the database created by the DHCP snooping feature on the switches. It then associates a trust state with each interface on the switch.

In a typical network configuration, all ports connected to end devices are untrusted and all switch-to-switch ports are configured as trusted. With this configuration, all ARP packets entering the

network from a given switch bypass the security check. No additional validation is performed at any other place in the network⁴.

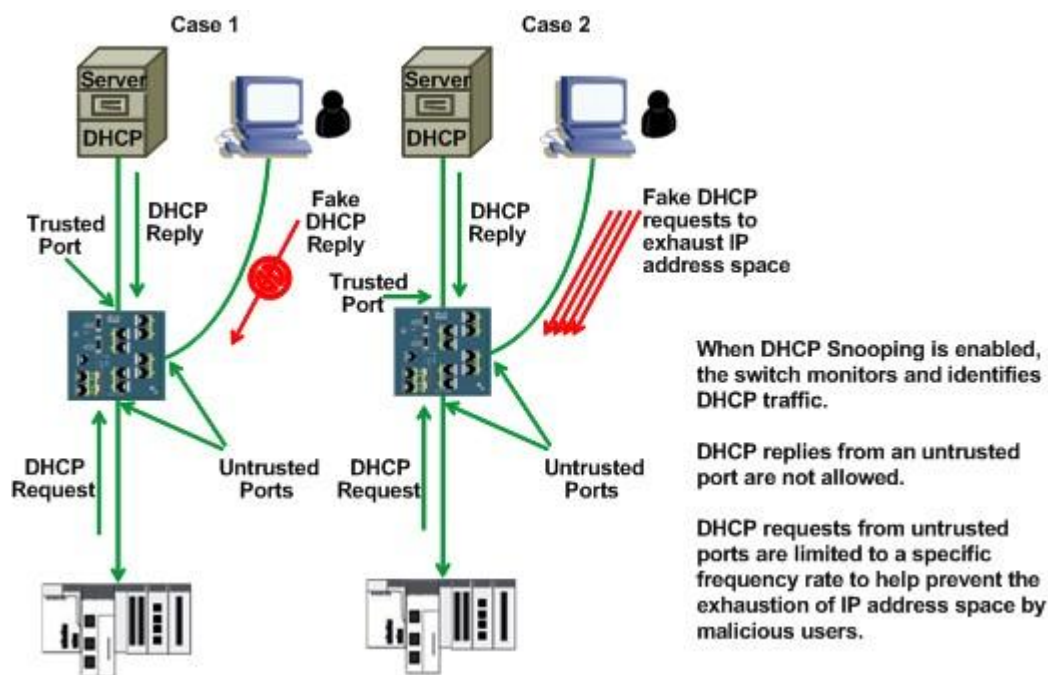


Figure 14: DHCP snooping

DHCP snooping is a technique used against attacks on the DHCP function. There are usually two kinds of attacks. The first is the attacker emulating a DHCP server and providing false gateways in order to capture the traffic. This is commonly referred to a **man in the middle** attack. Data collected may contain sensitive information such as user names, passwords, etc.

The second is an attacker faking DHCP requests until a legitimate DHCP server has depleted its pool of addresses, thereby preventing legitimate devices from acquiring IP addresses. When DHCP snooping is enabled on the switch, it will detect DHCP request packets as they pass through the switch. Ports are then configured as trusted or untrusted. The ports facing the DHCP server are configured as trusted, while all the rest are configured as untrusted. Only trusted ports are allowed to reply to DHCP requests, while untrusted ports are only allowed to send DHCP requests at a controlled rate.

⁴ Cisco IE 2000 Switch Software Configuration Guide Cisco Press 2012 p 29-3

3. Design

The diagram below is the selected architecture for this document. The two Cisco IE3000 layer 3 switches have routing enabled and use the industry standard Open Shortest Path First (OSPF) routing protocol. OSPF is a link state protocol that uses link state advertisements to update other routers in the network as to its status.

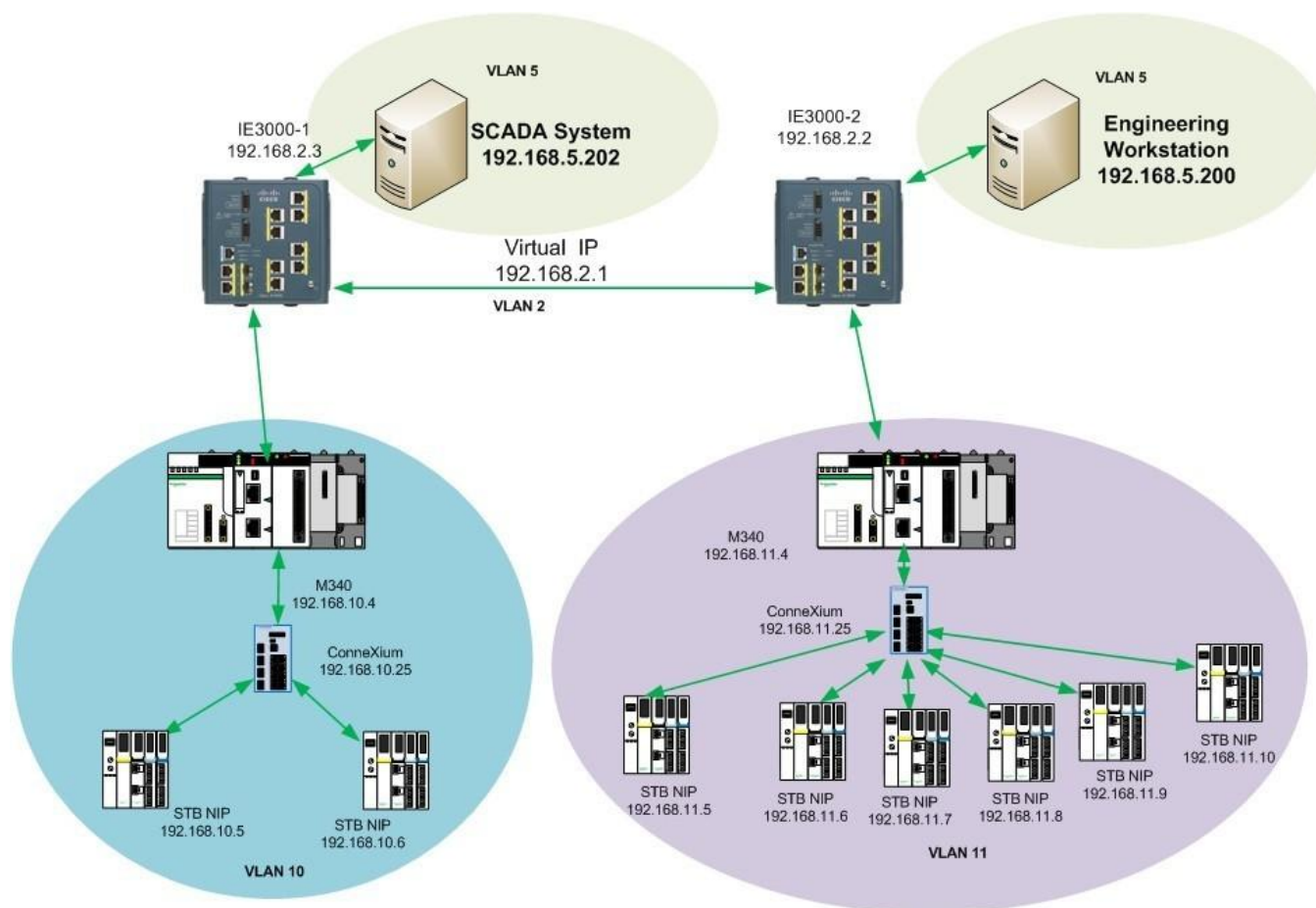


Figure 15: Network Design

In addition to running OSPF, the two Cisco IE3000 switches function as a redundant router set by implementing Cisco proprietary Hot Standby Routing Protocol (HSRP). Both OSPF and HSRP were explained in detail in the STN *How Can I Design a Transparent PlantStruxure Network Incorporating Cisco Industrial Ethernet Devices?* The architecture also includes two Schneider Electric M340 PACs running on separate VLANs. The PACs are attached to separate IE switches in the control room. Each PAC is then connected to a Schneider Electric ConneXium switch in the device network. These switches are also connected to the Advantys STB modules in the functional units. One switch is connected to two devices, the other to six.

The STBs are programmed to read I/O from the field devices. The PACs are programmed to scan the STBs for data.

All of the security testing was performed on the Cisco control network switches and the process area.

For the site-to-site encryption implementation, an additional Cisco switch was added that connects to one of the HSRP switch pair. The added Cisco switch at the remote location also connects to a group of ConneXium switches.

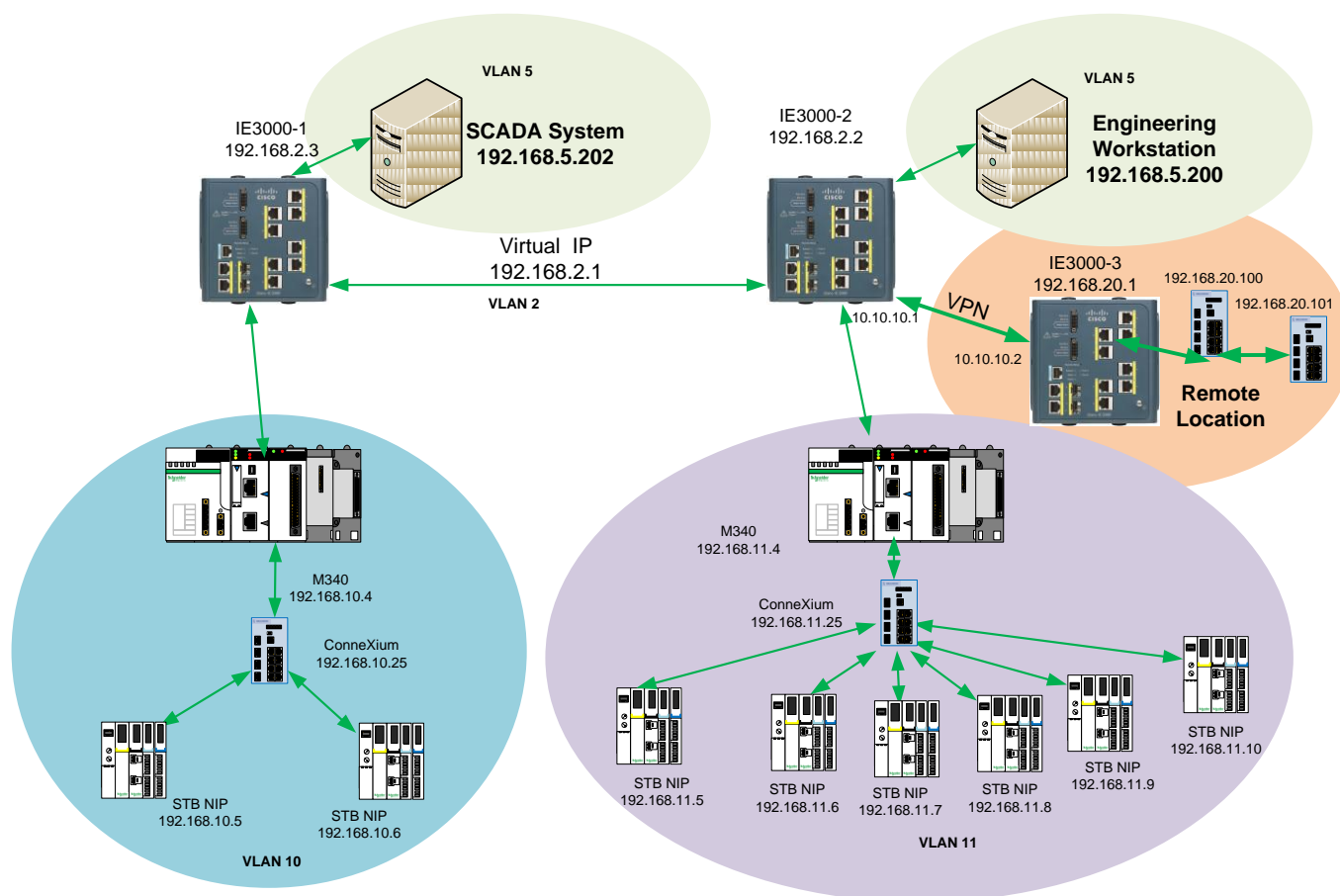


Figure 16: Network Design for Encryption

Many of the design guidelines were obtained from the *Cisco Guide to Harden Cisco IOS Devices*. Document ID: 13608 Updated June 13, 2014. This is available is available on the Cisco web site at:

<http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

This STN does not encompass all the options identified in the hardening guide, but reflects some recommendations for use in the industrial control network.

4. Implementation

In Cisco's view, the network consists of three sets, or planes, of functions: the management plane, the control plane, and the data plane. Each plane provides different functionality that needs to be safeguarded.

Management Plane – manages traffic sent to the Cisco device. The management plane is made up of applications such as secure shell (SSH) and simple network management protocol (SNMP).

Control Plane – processes the traffic that is paramount to the functionality of the network infrastructure. The control plane consists of applications and protocols that operate between network devices. These include routing protocols such as OSPF or Border Gateway Protocol BGP, and redundancy protocols such as Hot Standby Router Protocols (HSRP) or Resilient Ethernet Protocol (REP).

Data Plane – forwards the data through a network device.⁵

This document follows the Cisco functional plane strategy.

4.1. Management Plane

The management plane includes password management, informational banners, encrypted management sessions, control access via console, and command line and web browsers. It discusses applications and protocols to be disabled. It demonstrates recommended practices for logging and network management. It also addresses the implementation of NTP.

4.1.1. Password Management

Passwords are used to control access to devices or resources. Local passwords configured on the switch are safeguarded by the following mechanisms.

The “**enable secret**” command sets a password for administrative rights to the device. It is entered from the command line interface (CLI).

Here is an example from the switch configuration:

```
enable secret 5 $1$YFvD$PRTZSe28fL8j3uLFrQon1
```

```
enable password secret
```

⁵ *Guide to Hardening Cisco Devices*, Cisco Press, June 03, 2014 p.4

Note that the secret password is masked by the following text:

```
$1$YFvD$pRXTZSe28fL8j3uLFrQon1
```

Someone who gains unauthorized access to the device or to a printout of the configuration will not see the actual password. The password encryption service is a feature that directs the IOS software to encrypt the password. The command is as follows:

service password-encryption

Here is an example from the switch configuration:

service password-encryption

```
enable secret 5 $1$sp81$BPICAgQB55fPdrqsYlmgZ1
```

```
enable password 7 04480E051D2458
```

An additional feature of the Cisco IOS software is enhanced password security. This feature provides for the configuration of MD5 hashing for passwords. MD5 is a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321. MD5 is an algorithm used to verify data integrity by means of a 128-bit message digest. This digest is created from data that is input when the username is created. The command is as follows:

```
username greg privilege 15 secret 5 $1$RDyH$Dd.AmgwmOiKiFR//Nmsvt
```

Again the password is not in clear text.

Implementation of an authentication, authorization and accounting (AAA) server is another highly recommended strategy, which is not covered in this document. In the absence of an AAA server, the password encryption steps, described above, are recommended to help provide secure access to the device.

4.1.2. Informational Banners

An informational banner notifies a user, innocent or malicious, of that user's attempt to access a secure site. In the absence of informational banners, it may be impossible to prosecute a malicious intruder in some legal jurisdictions. Here is a sample from our switch configuration:

```
banner motd ^C
```

```
This is a secure site. Only authorized users are allowed.
```

```
Unlawful access to this system may be subject to civil and criminal penalties.
```

```
This system is monitored and all logs may be used as evidence in court.
```

```
^C
```

It is a recommended practice not to identify the device, or ownership.

4.1.3. Encrypted Management Sessions

Encrypted management sessions provide an alternative to sending clear text messages across the network when connected to a device. Terminal sessions using telnet are not recommended.

If Telnet is enabled, you can use the following commands to disable it:

```
Active-Router#  
Active-Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Active-Router(config)#line vty 0 4  
Active-Router(config-line)#transport input ssh  
Active-Router(config-line)#exit
```

Figure 17: Disabling Telnet

SSH is configured on the network devices. SSH allows authenticated users encrypted access to the device CLI. SSH was configured via the following command to the switch:

```
Enter configuration commands, one per line. End with CNTL/Z.  
Active-Router(config)#ip domain-name NCC.net  
Active-Router(config)#crypto key generate rsa modulus 2048  
The name for the keys will be: Active-Router.NCC.net
```

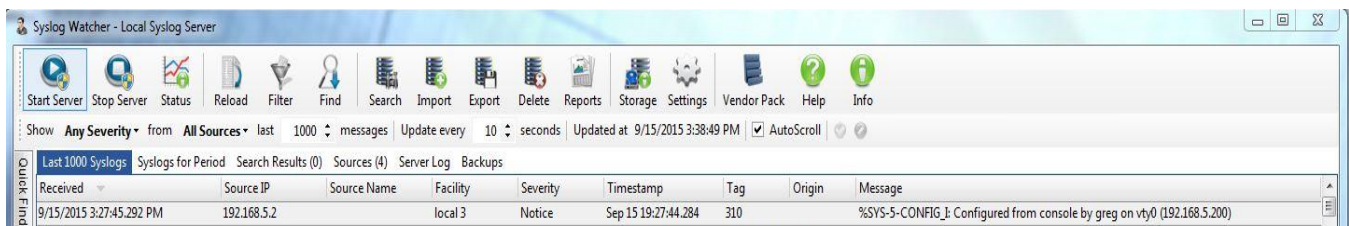
```
% The key modulus size is 2048 bits  
% Generating 2048 bit RSA keys, keys will be non-exportable...  
[OK] (elapsed time was 57 seconds)
```

```
Active-Router(config)#ip ssh time-out 60  
Active-Router(config)#ip ssh authentication-retries 3
```

```
Active-Router(config)#ip ssh source-interface fa1/1  
Active-Router(config)#line vty 0 4  
Active-Router(config-line)#transport input ssh  
Active-Router(config-line)#ip scp server enable
```

First a domain name is set on the devices. This is necessary for the generation of the encryption key. The next command generates the cryptography key. The **ip ssh time-out** step specifies a 60 second timeout to the connection; the next step permits 3 attempts to enter the password before the device disconnects the session.

On our switch, SSH can be connected only through the network management station attached to port fa1/1. The **ip scp server enable** command allows the use of the secure copy protocol (SCP) so an encrypted secure connection can be used to copy device configurations or software images. The following is an example of a syslog showing user “greg” accessing the switch via SSH:



Received	Source IP	Source Name	Facility	Severity	Timestamp	Tag	Origin	Message
9/15/2015 3:27:45.292 PM	192.168.5.2		local 3	Notice	Sep 15 19:27:44.284	310	%SYS-5-CONFIG-I: Configured from console by greg on vty0 (192.168.5.200)	

Figure 18: Syslog User Access Example

4.1.4. Console, Terminal and Web Access

The console port of the switch can also be disabled. The commands to do this are:

```
line aux 0
Transport input none
Transport output none
no exec
exec-timeout 0 1
no password
```

Remote terminal access can also be disabled. The commands to do this are:

```
line vty 0 4
Transport input none
```

Web access can be disabled. Cisco IOS devices have the ability to use a standard web service via HTTP or a secure web service via HTTPS. Either of these services can be disabled with a simple command:

```
no ip http server
```

Or

```
no http secure-server
```

4.1.5. Disable Unused Services

Unused services are disabled. The list of unused services includes:

- IP finger – no response to a finger request
- IP BOOTP server – the bootstrap protocol
- DHCP – the dynamic host configuration protocol
- MOP – the maintenance operation protocol
- IP domain-lookup – the domain name system (DNS)
- Service pad – the X.25 service
- Service Config – configuration via trivial file transfer protocol (TFTP)

Most of these services are disabled from the CLI by entering a **"no"** statement and then the name of the service, except for IP BOOTP server. That command is:

```
ip dhcp bootp ignore
```


4.1.6. Logging

Logging is an indispensable element of network security. It provides valuable information for network diagnostics. Time stamped messages are triggered when ports or interfaces changed state, and also shows when devices were accessed via remote terminals. It also flags detected system errors. Logging can act as a powerful debugging tool. The network syslog server employed in this design is a free product called Syslog Watcher, which is available from [SNMPSOFT](http://www.snmpsoft.com).

The download is a Microsoft Windows executable file that is a simple install. When starting the application, connect to the local server by selecting **Manage Local Syslog Server**.

It also has the capability to connect to Syslog Watcher running on remote devices.



Figure 19: Initializing Syslog Watcher

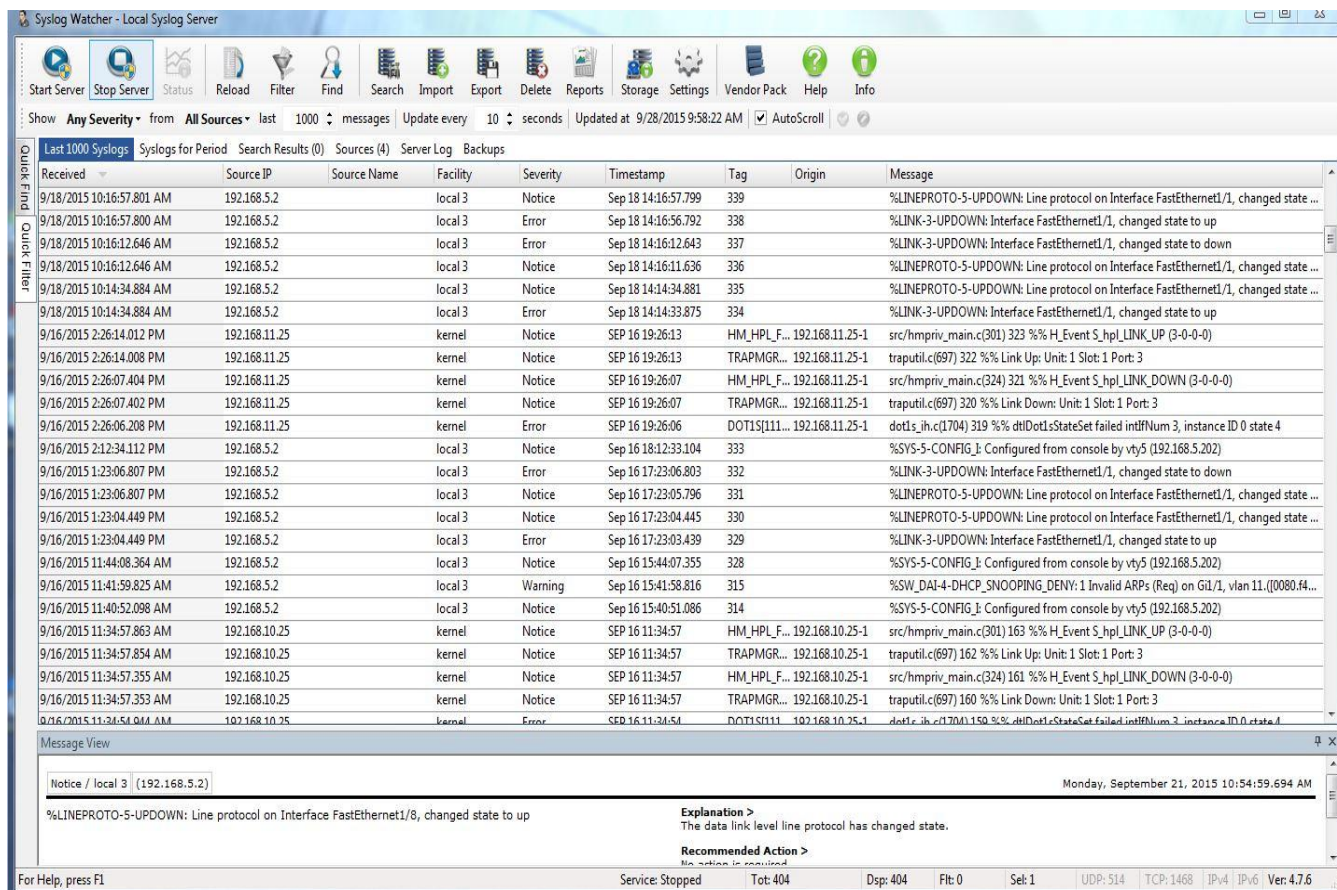
The next step is to configure logging on the switches. Here is a screenshot of the commands to enable logging and indicating where to send the switch log events.

```
!
logging facility local3
logging 192.168.5.202
!
```

Figure 20: CLI Enabling and Directing Logging

As you can see, in this configuration log files are sent to the Syslog Watcher at TCP/IP address of 192.168.5.202.

Here is a screenshot of Syslog Watcher running in the network:



Received	Source IP	Source Name	Facility	Severity	Timestamp	Tag	Origin	Message
9/18/2015 10:16:57.801 AM	192.168.5.2		local 3	Notice	Sep 18 14:16:57.799	339		%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/18/2015 10:16:57.800 AM	192.168.5.2		local 3	Error	Sep 18 14:16:56.792	338		%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
9/18/2015 10:16:12.646 AM	192.168.5.2		local 3	Error	Sep 18 14:16:12.643	337		%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down
9/18/2015 10:16:12.646 AM	192.168.5.2		local 3	Notice	Sep 18 14:16:11.636	336		%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/18/2015 10:14:34.884 AM	192.168.5.2		local 3	Notice	Sep 18 14:14:34.881	335		%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/18/2015 10:14:34.884 AM	192.168.5.2		local 3	Error	Sep 18 14:14:33.875	334		%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
9/16/2015 2:26:14.012 PM	192.168.11.25		kernel	Notice	SEP 16 19:26:13	HM_HPL_F...	192.168.11.25-1	src/hmpriv_main.c(301) 323 %% H_Event S_hpl_LINK_UP (3-0-0-0)
9/16/2015 2:26:14.008 PM	192.168.11.25		kernel	Notice	SEP 16 19:26:13	TRAPMGR...	192.168.11.25-1	traputil.c(697) 322 %% Link Up: Unit: 1 Slot: 1 Port: 3
9/16/2015 2:26:07.404 PM	192.168.11.25		kernel	Notice	SEP 16 19:26:07	HM_HPL_F...	192.168.11.25-1	src/hmpriv_main.c(324) 321 %% H_Event S_hpl_LINK_DOWN (3-0-0-0)
9/16/2015 2:26:07.402 PM	192.168.11.25		kernel	Notice	SEP 16 19:26:07	TRAPMGR...	192.168.11.25-1	traputil.c(697) 320 %% Link Down: Unit: 1 Slot: 1 Port: 3
9/16/2015 2:26:06.208 PM	192.168.11.25		kernel	Error	SEP 16 19:26:06	DOT1S[111...	192.168.11.25-1	dot1s_1h.c(1704) 319 %% dot1sStateSet failed intflNum 3, instance ID 0 state 4
9/16/2015 2:12:34.112 PM	192.168.5.2		local 3	Notice	Sep 16 18:12:33.104	333		%SYS-5-CONFIG_I: Configured from console by vty5 (192.168.5.202)
9/16/2015 1:23:06.807 PM	192.168.5.2		local 3	Error	Sep 16 17:23:06.803	332		%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down
9/16/2015 1:23:06.807 PM	192.168.5.2		local 3	Notice	Sep 16 17:23:05.796	331		%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/16/2015 1:23:04.449 PM	192.168.5.2		local 3	Notice	Sep 16 17:23:04.445	330		%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/16/2015 1:23:04.449 PM	192.168.5.2		local 3	Error	Sep 16 17:23:03.439	329		%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
9/16/2015 11:44:08.364 AM	192.168.5.2		local 3	Notice	Sep 16 15:44:07.355	328		%SYS-5-CONFIG_I: Configured from console by vty5 (192.168.5.202)
9/16/2015 11:41:59.825 AM	192.168.5.2		local 3	Warning	Sep 16 15:41:58.816	315		%SW_DAI-4-DHCP Snooping_DENY: 1 Invalid ARPs (Req) on Gi1/1, vlan 11.((0080.f4...
9/16/2015 11:40:52.098 AM	192.168.5.2		local 3	Notice	Sep 16 15:40:51.086	314		%SYS-5-CONFIG_I: Configured from console by vty5 (192.168.5.202)
9/16/2015 11:34:57.863 AM	192.168.10.25		kernel	Notice	SEP 16 11:34:57	HM_HPL_F...	192.168.10.25-1	src/hmpriv_main.c(301) 163 %% H_Event S_hpl_LINK_UP (3-0-0-0)
9/16/2015 11:34:57.854 AM	192.168.10.25		kernel	Notice	SEP 16 11:34:57	TRAPMGR...	192.168.10.25-1	traputil.c(697) 162 %% Link Up: Unit: 1 Slot: 1 Port: 3
9/16/2015 11:34:57.355 AM	192.168.10.25		kernel	Notice	SEP 16 11:34:57	HM_HPL_F...	192.168.10.25-1	src/hmpriv_main.c(324) 161 %% H_Event S_hpl_LINK_DOWN (3-0-0-0)
9/16/2015 11:34:57.353 AM	192.168.10.25		kernel	Notice	SEP 16 11:34:57	TRAPMGR...	192.168.10.25-1	traputil.c(697) 160 %% Link Down: Unit: 1 Slot: 1 Port: 3
9/16/2015 11:34:54.944 AM	192.168.10.25		kernel	Error	SEP 16 11:34:54	DOT1S[111...	192.168.10.25-1	dot1s_1h.c(1704) 150 %% dot1sStateSet failed intflNum 3, instance ID 0 state 4

Message View

Notice / local 3 (192.168.5.2) Monday, September 21, 2015 10:54:59.694 AM

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/8, changed state to up

Explanation >
The data link level line protocol has changed state.

Recommended Action >
No action is required.

For Help, press F1 Service: Stopped Tot: 404 Dsp: 404 Flt: 0 Seb: 1 UDP: 514 TCP: 1468 IPv4: IPv6 Ver: 4.7.6

Figure 21: Syslog Watcher in Operation

Cisco also recommends not logging monitor and console sessions. Enter the global configuration commands ***“no logging console”*** ***“no logging monitor”*** from the CLI to disable this feature.

4.1.7. Simple Network Management Protocol (SNMP)

SNMP is a valuable network management tool. SNMP is an interoperable protocol used by almost every network vendor. SNMP version 1 and 2 are very insecure and provide no password protection or encryption. SNMP version 3 fixed those problems. SNMP v3 has three primary configuration options:

1. No auth – no authentication or encryption of any SNMP packets.
2. Auth – authentication of the Ethernet packet without encryption.
3. Priv – both encryption and authentication of the SNMP packets.

To configure SNMP v3 from the CLI, configure an SNMP server group, then configure a user for that group. From the configuration mode of the CLI the commands are the following:

snmp-server group PRIVGROUP priv

snmp-server user snmpv3user PRIVGROUP v3 auth md5 authpassword 3des privpassword

To verify the configuration, issue a show command to display the user:

```
Active-Router#sho snmp user

User name: snmpv3user
Engine ID: 800000090300381C1A8CCC83
storage-type: nonvolatile          active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP

Active-Router#
```

Figure 22: SNMP Show Command Output

Schneider Electric ConneXium Network Manager supports the use of SNMP v3.

4.1.8. Network Time Protocol (NTP)

NTP configured in the switch network synchronizes the system clock of the devices. [Mienberg Global](#) provides a free Microsoft Windows based NTP server. The simple install process creates an NTP windows service and can point to any NTP server in the internet or, as in our case, within the control network. Here is a screenshot of the service:

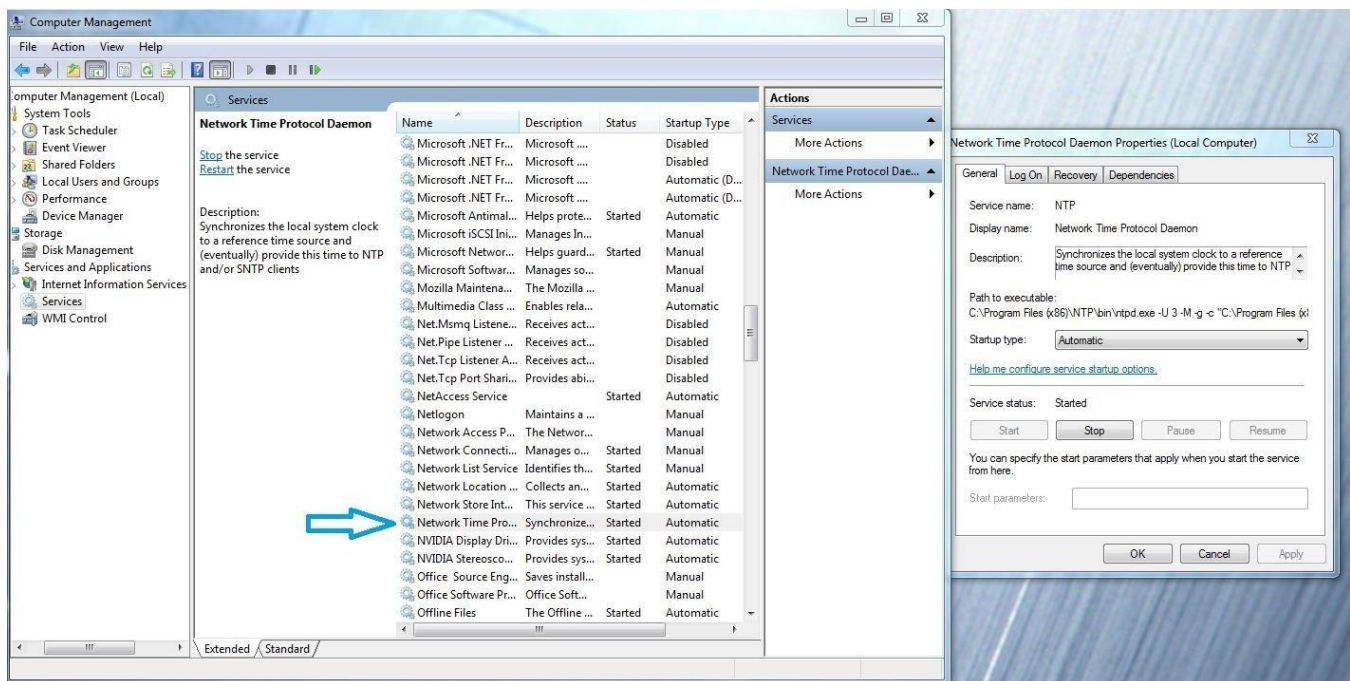


Figure 23: NTP Server

After the NTP server is installed, enable NTP on the switches. To demonstrate the different ways to configure these options, the CLI, Cisco Network Assistant (CNA) and the Cisco Configuration Professional (CCP) tools were used in this control network implementation. CNA is a free tool available from Cisco. It is a Microsoft Windows or Apple MAC software application that provides an easy to use graphical interface. CCP is demonstrated later in this document.

Here is a screenshot of NTP configured on the switches via CNA:

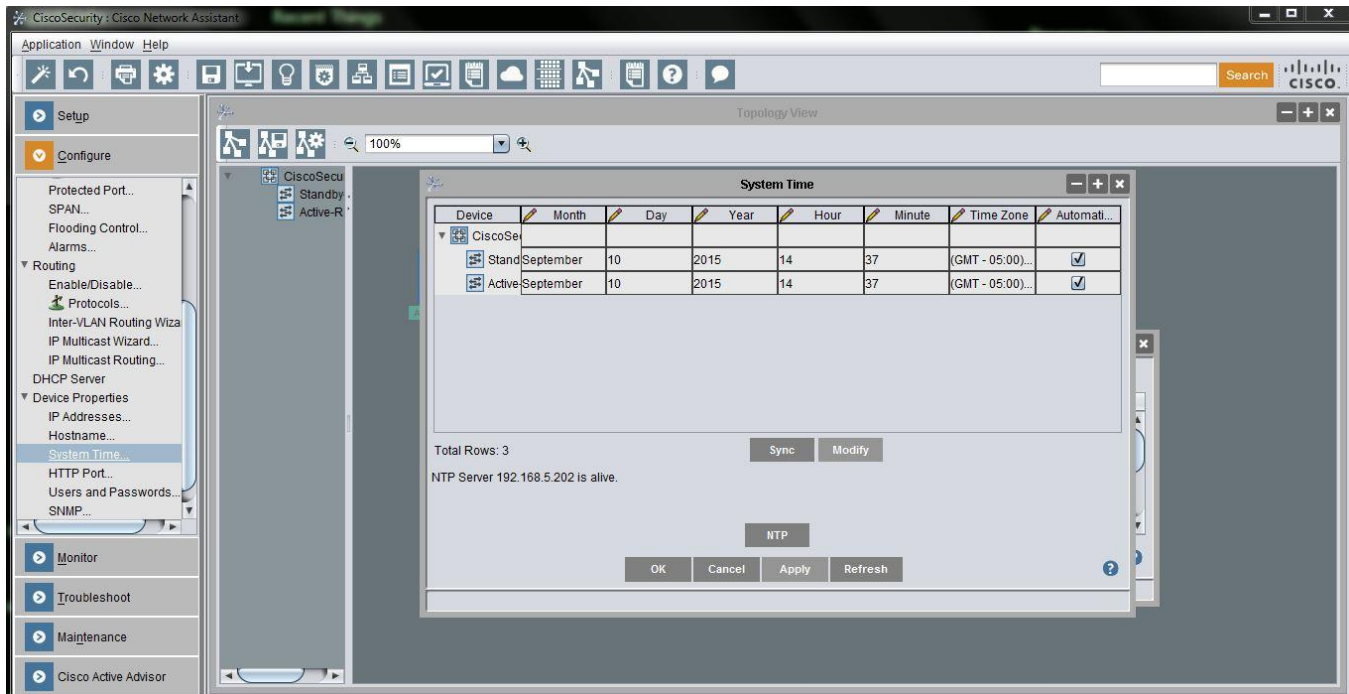


Figure 24: Cisco Network Assistant

4.2. Control Plane

The control plane focuses on applications and protocols that impact network devices. OSPF implemented in our network is a key control plane protocol. First Hop redundancy protocols, such as Hot Standby Router Protocols (HSRP), are also used in the control network to provide high availability. Other features like infrastructure access control lists (ACL) and routing protocol authentication are also implemented in the control network.

4.2.1. OSPF and HSRP

OSPF, which is configured in this network, is an example of a routing protocol between two routing enabled layer 3 switches. PlanStruxure control networks generally incorporate static routing. By contrast, OSPF is a link state protocol that provides additional features – including automatic topology determination – that do not exist in static routing. As the Internet of Things (IOT) continues to expand, more and more devices will be network enabled. This will increase the complexity of most networks, so that manually entering static link routes becomes a daunting task. OSPF is a feature-rich routing protocol that may benefit control networks both today and in the future. Most IT organizations use link state protocols such as OSPF. As the world of IT and OT converge, running OSPF – the most commonly used link state protocol – may provide a seamless secure bridge between IT and OT.

HSRP provides router redundancy thus eliminating a single point of failure in the PlantStruxure control network. Static routing provides no redundancy. For more information on OSPF and HSRP, refer to the detailed explanations in the STN *How Can I Design a Transparent PlantStruxure Network Incorporating Cisco Industrial Ethernet Devices?*

Here is the switch configuration for OSPF:

```
!
router ospf 1
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.5.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
```

Figure 25: OSPF Configuration

Below is a validation that OSPF is operating correctly:

```
Standby-Router#sho ip ospf
Routing Process "ospf 1" with ID 192.168.11.3
Start time: 00:00:33.546, Time elapsed: 4w4d
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
  Number of interfaces in this area is 4
  Area has no authentication
  SPF algorithm last executed 6d04h ago
  SPF algorithm executed 14 times
  Area ranges are
  Number of LSA 6. Checksum Sum 0x037D9B
  Number of opaque link LSA 0. Checksum Sum 0x000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
```

Figure 26: Verifying OSPF Operation

The following figures present the active and standby switch configurations for HSRP:

```
?
interface Vlan1
no ip address
?
interface Vlan2
ip address 192.168.2.2 255.255.255.0
standby 2 ip 192.168.2.1
standby 2 priority 105
standby 2 preempt
?
interface Vlan5
ip address 192.168.5.2 255.255.255.0
standby 2 priority 105
standby 5 ip 192.168.5.1
standby 5 priority 105
standby 5 preempt
standby 10 priority 105
standby 10 preempt
?
interface Vlan10
ip address 192.168.10.2 255.255.255.0
standby 10 ip 192.168.10.1
standby 10 priority 105
standby 10 preempt
?
interface Vlan11
ip address 192.168.11.2 255.255.255.0
standby 11 ip 192.168.11.1
standby 11 priority 105
standby 11 preempt
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5
?
```

Figure 27: Active Router

```
?
interface Vlan1
no ip address
?
interface Vlan2
ip address 192.168.2.3 255.255.255.0
standby 2 ip 192.168.2.1
standby 2 preempt
?
interface Vlan5
ip address 192.168.5.3 255.255.255.0
standby 5 ip 192.168.5.1
standby 5 preempt
?
interface Vlan10
ip address 192.168.10.3 255.255.255.0
standby 10 ip 192.168.10.1
standby 10 preempt
?
interface Vlan11
ip address 192.168.11.3 255.255.255.0
standby 11 ip 192.168.11.1
standby 11 preempt
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 02240B481F0901700D
?
```

Figure 28: Standby Router

This is the command to verify if HSRP is functioning:

```
Active-Router#sho standby
Vlan2 - Group 2
  State is Active
    2 state changes, last state change 6d05h
  Virtual IP address is 192.168.2.1
  Active virtual MAC address is 0000.0c07.ac02
  Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.272 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.2.3, priority 100 (expires in 11.536 sec)
  Priority 105 (configured 105)
  Group name is "hsrp-V12-2" (default)
Vlan5 - Group 5
  State is Active
    1 state change, last state change 6d05h
  Virtual IP address is 192.168.5.1
  Active virtual MAC address is 0000.0c07.ac05
  Local virtual MAC address is 0000.0c07.ac05 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.560 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.5.3, priority 100 (expires in 9.744 sec)
  Priority 105 (configured 105)
  Group name is "hsrp-V15-5" (default)
Vlan10 - Group 10
  State is Active
    2 state changes, last state change 6d05h
  Virtual IP address is 192.168.10.1
  Active virtual MAC address is 0000.0c07.ac0a
  Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.600 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.3, priority 100 (expires in 8.544 sec)
  Priority 105 (configured 105)
  Group name is "hsrp-V110-10" (default)
Vlan11 - Group 11
  State is Active
    1 state change, last state change 6d05h
  Virtual IP address is 192.168.11.1
  Active virtual MAC address is 0000.0c07.ac0b
  Local virtual MAC address is 0000.0c07.ac0b (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.968 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.11.3, priority 100 (expires in 10.160 sec)
  Priority 105 (configured 105)
  Group name is "hsrp-V111-11" (default)
Active-Router#
```

Figure 29: Verifying HSRP Operation

4.2.2. OSPF Message Authentication

Using password authentication between the switches helps prevent a malicious user from introducing false routing information into the control network. Applying the MD5 hash authentication process, routing updates are no longer in clear text. However, MD5 is still susceptible to brute force and dictionary attacks if simple passwords are used.

The switches are configured with MD5 authentication. In Figure 29 above, the last 2 lines of the interface VLAN 11 demonstrate how this is configured.

Here is a command to determine the state of password authentication:

```
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 02240B481F0901700D
```

Figure 30: Verifying Password Authentication

Here is the output of the command:

```
Active-Router#sho ip ospf int
Vlan11 is up, line protocol is up
Internet Address 192.168.11.2/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.11.2, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
0 1 no no Base
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 192.168.11.3, Interface address 192.168.11.3
Backup Designated router (ID) 192.168.11.2, Interface address 192.168.11.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 oob-resync timeout 40
 Hello due in 00:00:04
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 4/4, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 9 msec
Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 192.168.11.3 (Designated Router)
Suppress hello for 0 neighbor(s)
Message digest authentication enabled ←
Youngest key id is 1
```

Figure 31: Password Authentication Verification Command Output

4.2.3. Access Control List

Access control list (ACL) operation can be very simple or quite complex. The example network has a simple ACL that calls for SSH to be used to access and configure the device from the CLI. Telnet has already been disabled on the device. The CLI is set to accept only SSH (port 22) for access. The ACL specifies that SSH can be initiated from VLAN 5, which is where the network management station is set up. Here is the ACL:

```
Active-Router(config)#
Active-Router(config)#access-list 10 permit 192.168.5.0 0.0.0.255
Active-Router(config)#line vty 0 4
Active-Router(config-line)#access-class 1 in
Active-Router(config-line)#exit
```

Figure 32: Password Authentication Verification Command Output

The access list permits devices in VLAN 5 (subnet 192.168.5.0/24) to connect to the switch via SSH. The Cisco access list contains the hidden last line **ip deny any any** that denies access by any other device or VLAN not in the permitted subnet.

More complex ACLs can be written to identify a specific address of a device, or a control policy can be created to accomplish the same result.

4.3. Data Plane

Securely moving data between network devices is the responsibility of the data plane. There are many features and configuration options available in the Cisco IOS software. Implementation of these features was accomplished by various means. CNA was used in the previous Cisco based STNs.

CCP is a web based router tool and, although not designed for switches, it can be used to simplify switch configuration. It offers smart wizards and advanced configuration support to assist in configuring and deploying switches. It is a free tool available from Cisco at:

<https://software.cisco.com/download/release.html?mdfid=281795035&softwareid=282159854&release=3.2&relind=AVAILABLE&rellifecycle=&reltype=latest>.

Here is a screenshot of the tool discovering the control network switches:

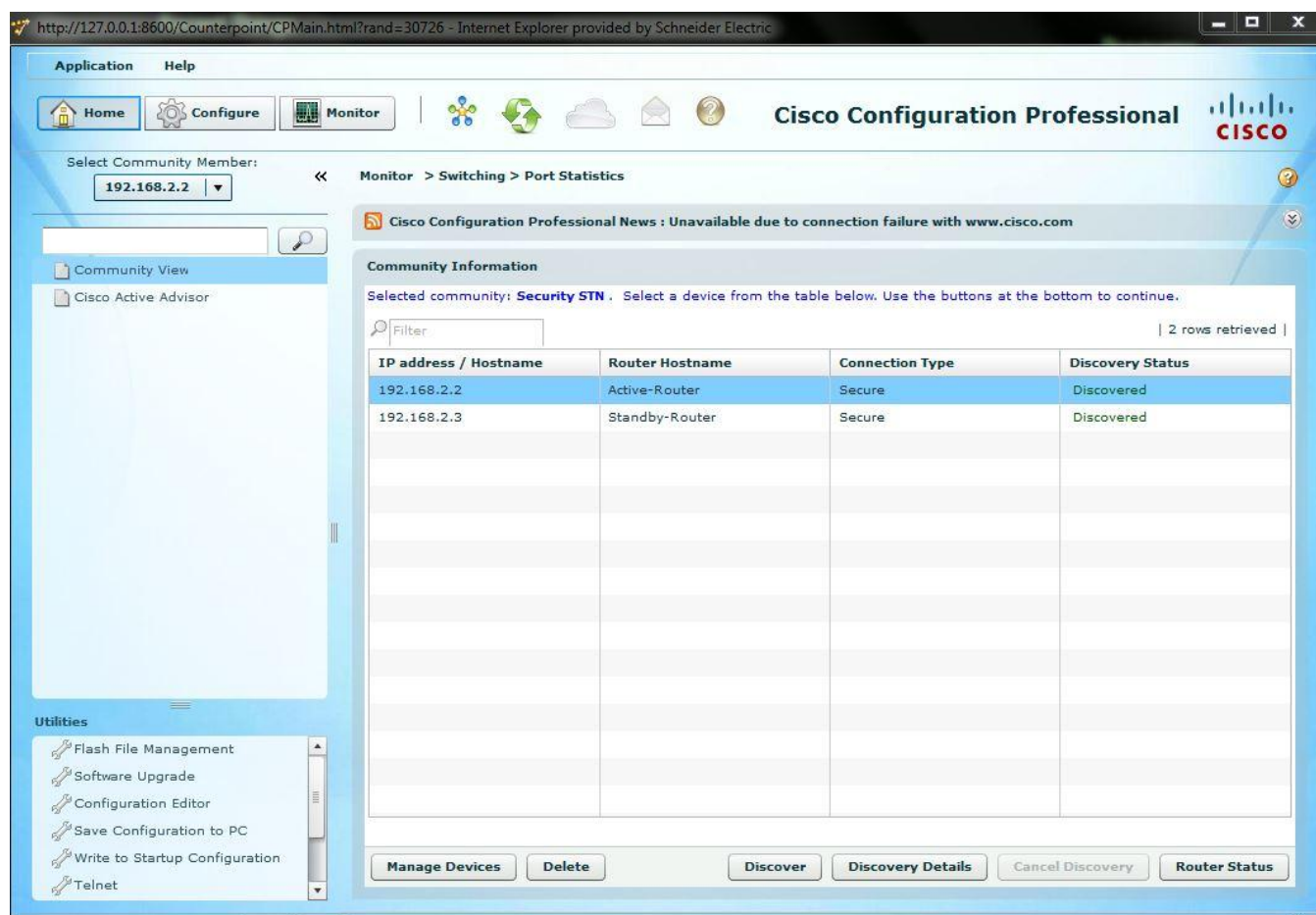
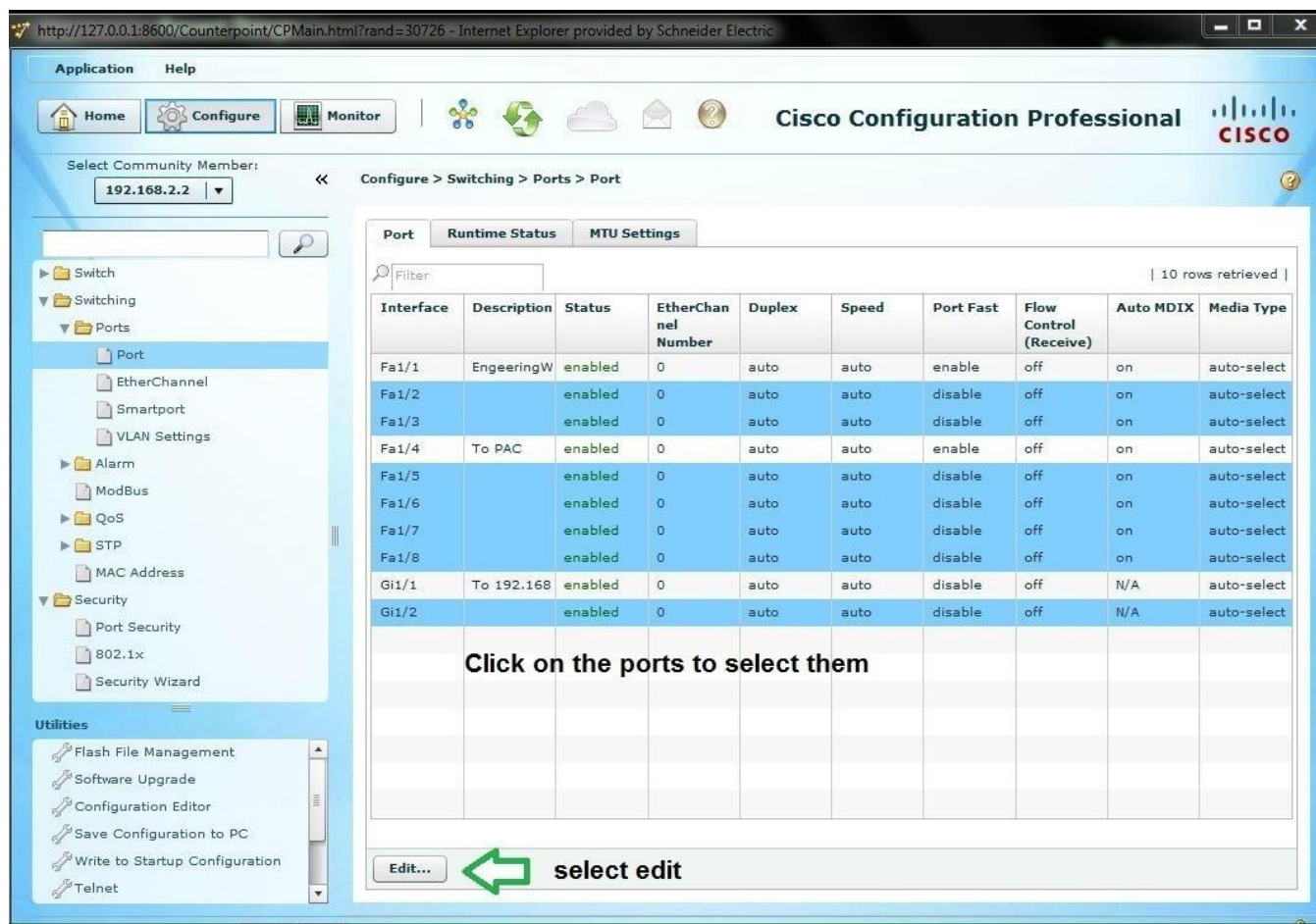


Figure 33: Cisco Configuration Professional GUI

4.3.1. Disabling Unused Ports

Ports that are not used should be disabled to help prevent a malicious user from gaining access to the control network. CCP provides an easy-to-use interface for disabling unused ports:



Click on the ports to select them

select edit

Figure 34: Selecting Unused Ports in CCP

The next screen allows you to select the “disable” button and click OK.

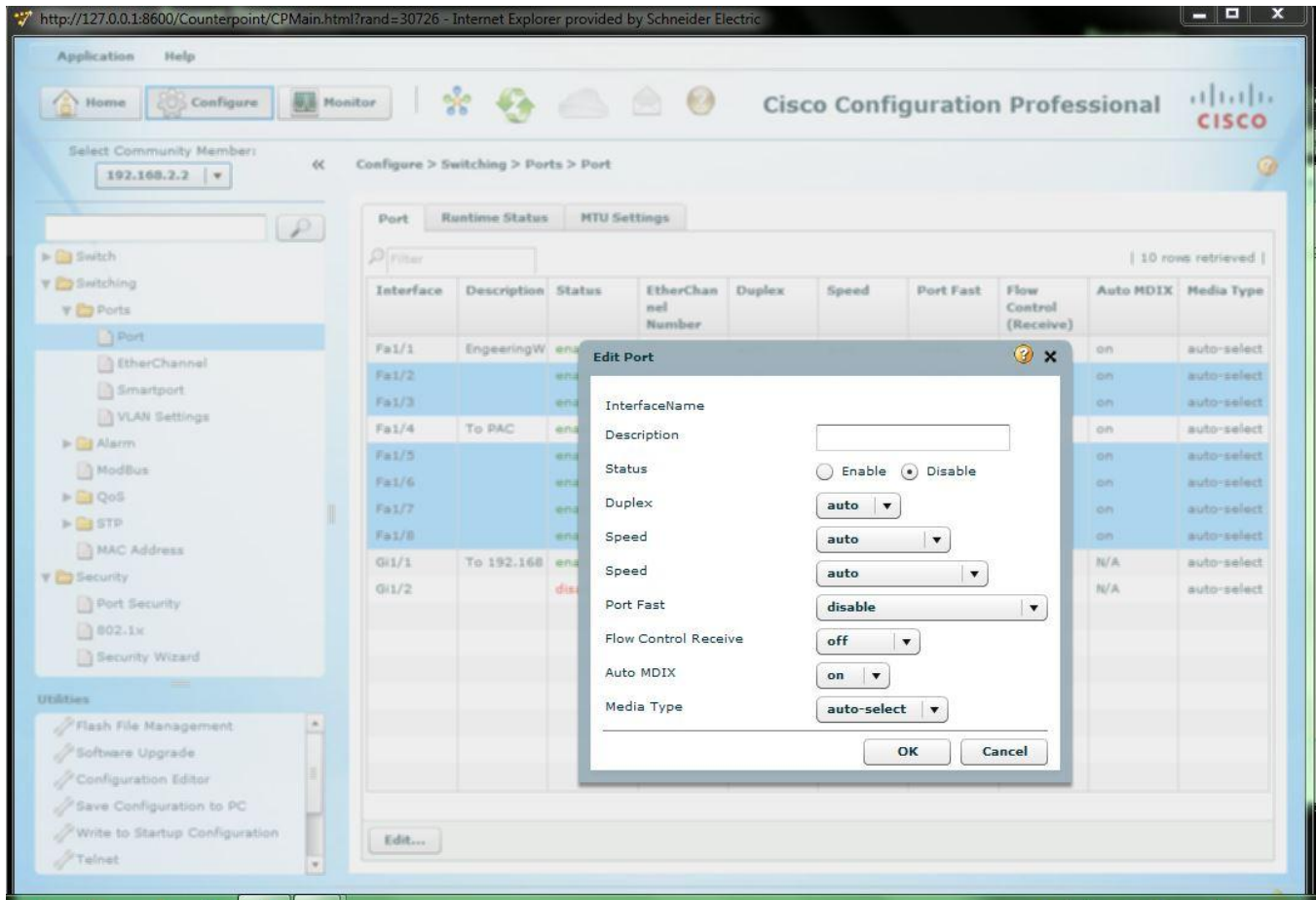
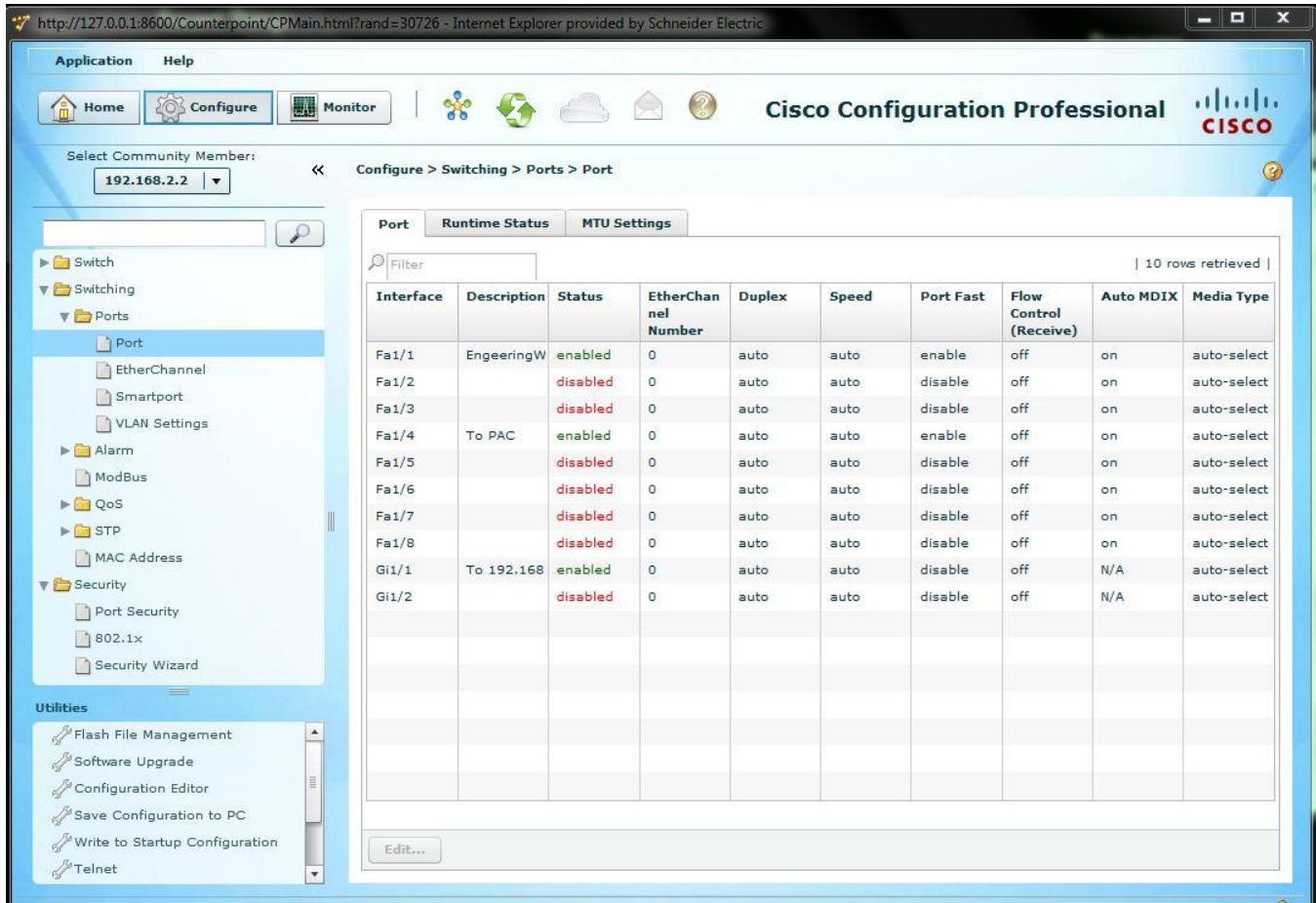


Figure 35: Disabling Selected Ports in CCP

Here are the results showing that the selected ports have been disabled.



The screenshot shows the Cisco Configuration Professional (CCP) interface. The top navigation bar includes 'Application' and 'Help' menus, and a 'Cisco Configuration Professional' header. The left sidebar shows a tree view of configuration options, with 'Ports' selected. The main area displays a table of port configurations under the 'Port' tab. The table has columns for Interface, Description, Status, EtherChannel Number, Duplex, Speed, Port Fast, Flow Control (Receive), Auto MDIX, and Media Type. The 'Status' column shows 'enabled' in green and 'disabled' in red. The 'Description' column shows 'EngineeringW' for Fa1/1 and 'To 192.168' for Gi1/1.

Interface	Description	Status	EtherChannel Number	Duplex	Speed	Port Fast	Flow Control (Receive)	Auto MDIX	Media Type
Fa1/1	EngineeringW	enabled	0	auto	auto	enable	off	on	auto-select
Fa1/2		disabled	0	auto	auto	disable	off	on	auto-select
Fa1/3		disabled	0	auto	auto	disable	off	on	auto-select
Fa1/4	To PAC	enabled	0	auto	auto	enable	off	on	auto-select
Fa1/5		disabled	0	auto	auto	disable	off	on	auto-select
Fa1/6		disabled	0	auto	auto	disable	off	on	auto-select
Fa1/7		disabled	0	auto	auto	disable	off	on	auto-select
Fa1/8		disabled	0	auto	auto	disable	off	on	auto-select
Gi1/1	To 192.168	enabled	0	auto	auto	disable	off	N/A	auto-select
Gi1/2		disabled	0	auto	auto	disable	off	N/A	auto-select

Figure 36: Displaying Port Status

As you can see, the CCP tool provides many configuration options. Some of these will be implemented later in this document.

In addition to disabling the ports, you can use RJ45 port locks to physically help secure the ports. Here is an example of installed port locks:

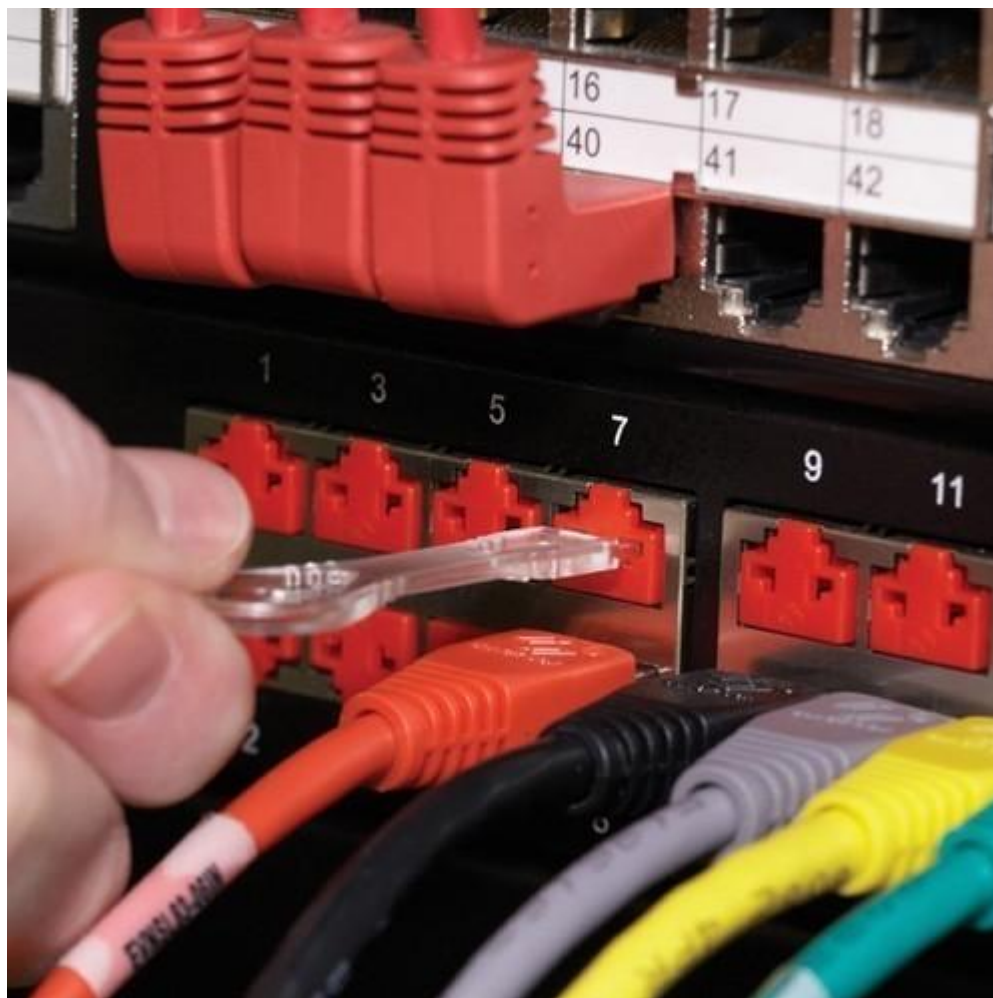


Figure 37: RJ45 Port Lockout

The clear instrument is the key that locks the plastic port block into place. Port locks are available from network hardware warehouses.

4.3.2. VLANs

VLANs are implemented in the control network. As mentioned in section 2.4.2. , they provide a separate broadcast domain for each VLAN. This helps create a secure operating environment because traffic traverses to another VLAN only when required. VLANs are implemented using the CNA tool. The creation of VLANs using CNA was explained in the STN *How Can I Design a Transparent PlantStruxure Network Incorporating Cisco Industrial Ethernet Devices?*.

Here is a screenshot of the control network VLANs:

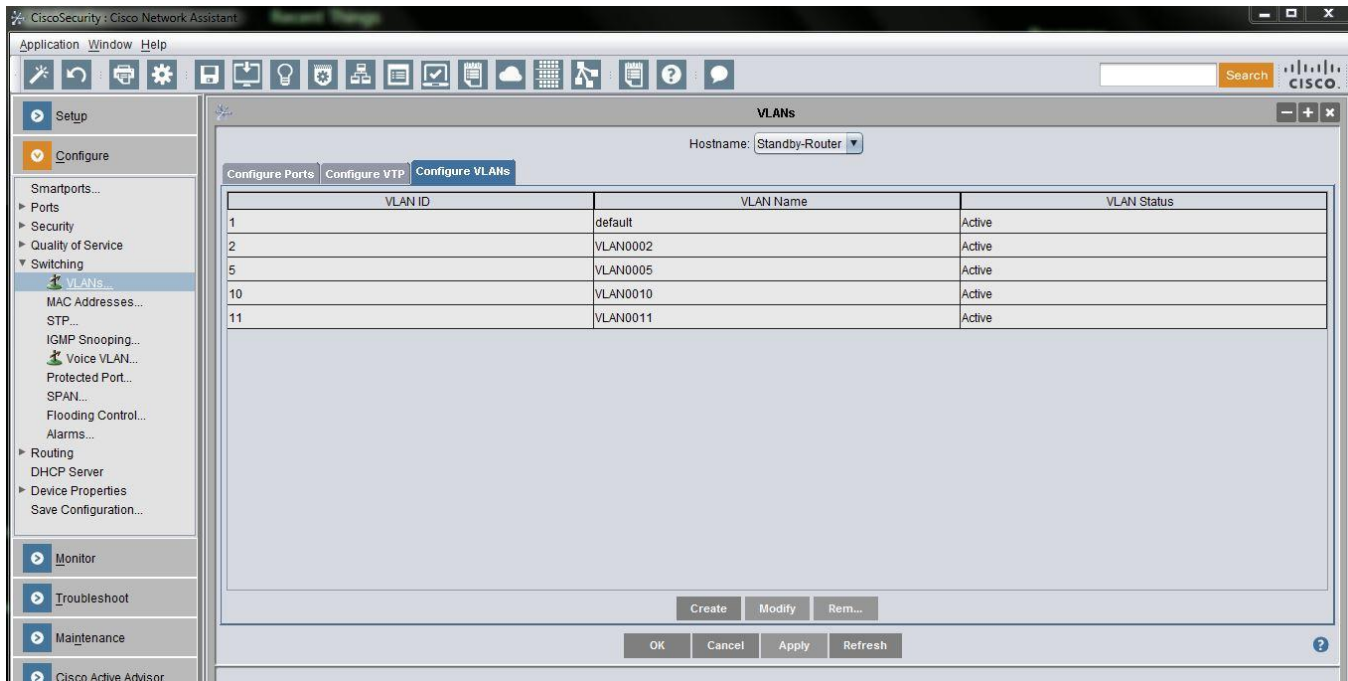


Figure 38: CNA Tool Displaying VLANs

4.3.3. Controlling Data Flow via Access List

Access lists were implemented in the control plane portion (section 4.2.3.) of this document.

Access lists can also be used to filter traffic that is addressed to the control network.

Internet control message protocol (ICMP) is a valuable tool for troubleshooting network problems. Malicious attackers can use tools such as **ping** and **traceroute** to gain access to and exploit the network.

A gate-keeping ACL, which determines whose ICMP packets are accepted and rejected, is called a transit ACL (tACL).

A tACL allows only ICMP messages from a “trusted network”, which in this control network is VLAN 5. All other subnets are denied access via ICMP ping and traceroute. Here is the ACL:

```
Active-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Active-Router(config)#ip access-list extended ACL-TRANSIT-IN
Active-Router(config-ext-nacl)#permit icmp host 192.168.5.0 any
Active-Router(config-ext-nacl)#deny icmp any any
Active-Router(config-ext-nacl)#exit
Active-Router(config)#
```

Figure 39: Creating a tACL

4.3.4. IP Source Guard

Cisco's IP source guard uses DHCP snooping to dynamically configure a port access control table so that it denies traffic from any IP address not included in the IP source binding table, which is controlled and maintained by DHCP. IP source guard helps prevent the spoofing of an IP address by a malicious user.

The DHCP service is disabled on our control network switches. However, it is enabled on the M340 PACs that provide IP addresses to the downstream Advantys STB devices. The first 2 lines of the CLI below globally enable DHCP snooping on the VLANs supporting the Advantys STB devices. The **ip verify source** command line enables IP source guard on the interface for the M340 PAC.

```
Standby-Router(config)#ip dhcp snooping
Standby-Router(config)#ip dhcp snooping vlan 10-11
Standby-Router(config)#int fa1/4
Standby-Router(config-if)#ip verify source
Standby-Router(config-if)#ip dhcp snooping trust
Standby-Router(config-if)#exit
Standby-Router(config)#ip arp inspection vlan 10-11
Standby-Router(config)#exit
Standby-Router#
```

Figure 40: Enabling IP Source Guard

In the lab control network, we have implemented a situation where DHCP packets are traversing the network, but where there is no match in the IP source binding table.

This situation exists because the PAC to Advantys STB communication is downstream from the switch. Ordinarily this design would generate syslog detected error notifications. But because the command line **ip dhcp snooping trust** is added, no such notifications are generated. The trust flag tells the device that if it detects a DHCP message coming from this DHCP-enabled interface, it has not detected an error.

4.3.5. Dynamic ARP Inspection (DAI)

DAI is used to mitigate ARP poisoning attacks from a malicious user. Similar to IP source guard, DAI uses DHCP snooping as the mechanism to validate MAC and IP addresses. Invalid matches are discarded and a syslog event is generated.

9/16/2015 10:28:13.645 AM	192.168.5.3	local 3	Notice	Sep 16 14:28:12.637	6832	%SYS-5-CONFIG: Configured from console by vty5 (192.168.2.2)
9/16/2015 10:28:02.799 AM	192.168.5.3	local 3	Warning	Sep 16 14:28:01.791	6831	%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/1, vlan 11. ([381c.1a...
9/15/2015 9:55:11.162 AM	192.168.5.2	local 3	Notice	Sep 15 13:55:11.159	191	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/15/2015 9:55:11.162 AM	192.168.5.2	local 3	Error	Sep 15 13:55:10.153	190	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
9/14/2015 4:08:53.198 PM	192.168.5.3	local 3	Notice	Sep 14 20:08:52.190	112	%LINK-5-CHANGED: Interface FastEthernet1/2, changed state to administratively down
9/14/2015 4:08:39.535 PM	192.168.10.25	kernel	Notice	SEP 14 16:08:39	TRAPMGR...	traputil.c(697) 140 %% saSNTPTrap: saNetSNTPOperStatus: 1
9/14/2015 4:08:36.298 PM	192.168.11.25	kernel	Notice	SEP 14 21:08:36	TRAPMGR...	traputil.c(697) 312 %% saSNTPTrap: saNetSNTPOperStatus: 1
9/14/2015 4:08:23.041 PM	192.168.5.3	local 3	Notice	Sep 14 20:08:23.039	111	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/14/2015 4:08:23.041 PM	192.168.5.3	local 3	Error	Sep 14 20:08:22.033	110	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
9/14/2015 4:06:34.885 PM	192.168.5.3	local 3	Error	Sep 14 20:06:33.878	103	%LINK-3-UPDOWN: Interface FastEthernet1/2, changed state to down
9/14/2015 4:01:50.032 PM	192.168.5.3	local 3	Notice	Sep 14 20:01:49.025	102	%SYS-5-CONFIG: Configured from console by vty0 (192.168.2.2)
9/14/2015 4:00:22.215 PM	192.168.5.2	local 3	Notice	Sep 14 20:00:21.208	189	%SYS-5-CONFIG: Configured from console by vty0 (192.168.5.202)
9/11/2015 3:42:15.586 PM	192.168.5.2	local 3	Error	Sep 11 19:42:15.582	188	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down
9/11/2015 3:42:15.586 PM	192.168.5.2	local 3	Notice	Sep 11 19:42:14.576	187	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/11/2015 2:47:41.629 PM	192.168.5.2	local 3	Notice	Sep 11 18:47:40.621	186	%SYS-5-CONFIG: Configured from console by vty0 (192.168.5.202)
9/11/2015 2:47:38.005 PM	192.168.5.2	local 3	Notice	Sep 11 18:47:36.997	185	%SYS-5-CONFIG: Configured from console by vty0 (192.168.5.202)
9/11/2015 2:05:44.190 PM	192.168.5.2	local 3	Notice	Sep 11 18:05:44.187	184	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/11/2015 2:05:44.190 PM	192.168.5.2	local 3	Error	Sep 11 18:05:43.180	183	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
9/11/2015 2:05:00.435 PM	192.168.5.2	local 3	Error	Sep 11 18:05:00.432	182	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down
9/11/2015 2:05:00.435 PM	192.168.5.2	local 3	Notice	Sep 11 18:04:59.425	181	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/11/2015 1:48:49.071 PM	192.168.5.2	local 3	Notice	Sep 11 17:48:49.069	180	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...
9/11/2015 1:48:49.071 PM	192.168.5.2	local 3	Error	Sep 11 17:48:48.062	179	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
9/10/2015 3:11:05.412 PM	192.168.5.2	local 3	Error	Sep 10 19:11:05.410	178	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down

Figure 41: Dynamic ARP Inspection

The steps to configure DAI on a switch are:

1. Configure DHCP snooping (see section 4.3.4).
2. Configure **ip arp inspection vlan <vlan-range>**

If DHCP is not used, DAI can instead use an ARP ACL to inspect ARPs from static devices. Here is an example that configures an ARP ACL with the name DAI:

Active-Router#

Active-Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Active-Router(config)#arp access-list DAI

Active-Router(config-arp-nacl)#\$permit ip host 192.168.5.200 mac host 0024.9b0c.3755

Active-Router(config-arp-nacl)#exit

Active-Router(config)#ip arp inspection filter DAI vlan 5

Active-Router(config)#int fa1/1

Active-Router(config-if)#no ip arp inspection trust

Active-Router(config-if)#exit

Active-Router(config)#exit

Active-Router#

Active-Router#sho arp access-list

ARP access list DAI

permit ip host 192.168.5.200 mac host 0024.9b0c.3755

Active-Router#

This ACL specifically states that the device connected to port FA1/1 must have the matching IP address and MAC address, otherwise the switch discards the packet and triggers a syslog event.

4.3.6. MAC Move Notifications

In the event there are enabled open ports on a network switch, you can use MAC move notification to detect if a user, malicious or not, moves a device from one physical switch port to another.

As mentioned in section 2.4.6. this triggers both a syslog event and a security violation. The MAC move notification feature is configured from the CLI.

The first step is to configure the MAC address table notification to enable change notifications, set the interval to send trap to 123 seconds and keep the history size to 100 entries. The second interval may depend of the complexity of the network. The default is 1 second. In a network with a lot of devices, the default time could potentially flood the network managing server.

```
mac address-table notification change interval 123
mac address-table notification change history-size 100
mac address-table notification change
```

Figure 42: Configuring MAC address table notifications

The next step is to enable the MAC change and MAC move notifications globally on the switch to send SNMP traps the the SNMP manager:

```
snmp-server enable traps mac-notification change move
snmp-server host 192.158.5.202 private mac-notification
snmp-server host 192.168.5.202 private mac-notification
```

Figure 43: Enabling MAC change and MAC move notifications

The final step is to enable the change notification on each interface

```
interface FastEthernet1/2
switchport access vlan 5
switchport mode access
snmp trap mac-notification change added
spanning-tree bpdudfilter enable
```

Figure 44: Enabling MAC change notifications on each interface

In conjunction with the port security features, detection of a MAC move violation triggers a restriction in which the source address is dropped.

4.3.7. Port Security

Schneider Electric recommends that you disable any port not in use. CCP includes a security wizard to help configure port security. Here are the steps to configure port security:

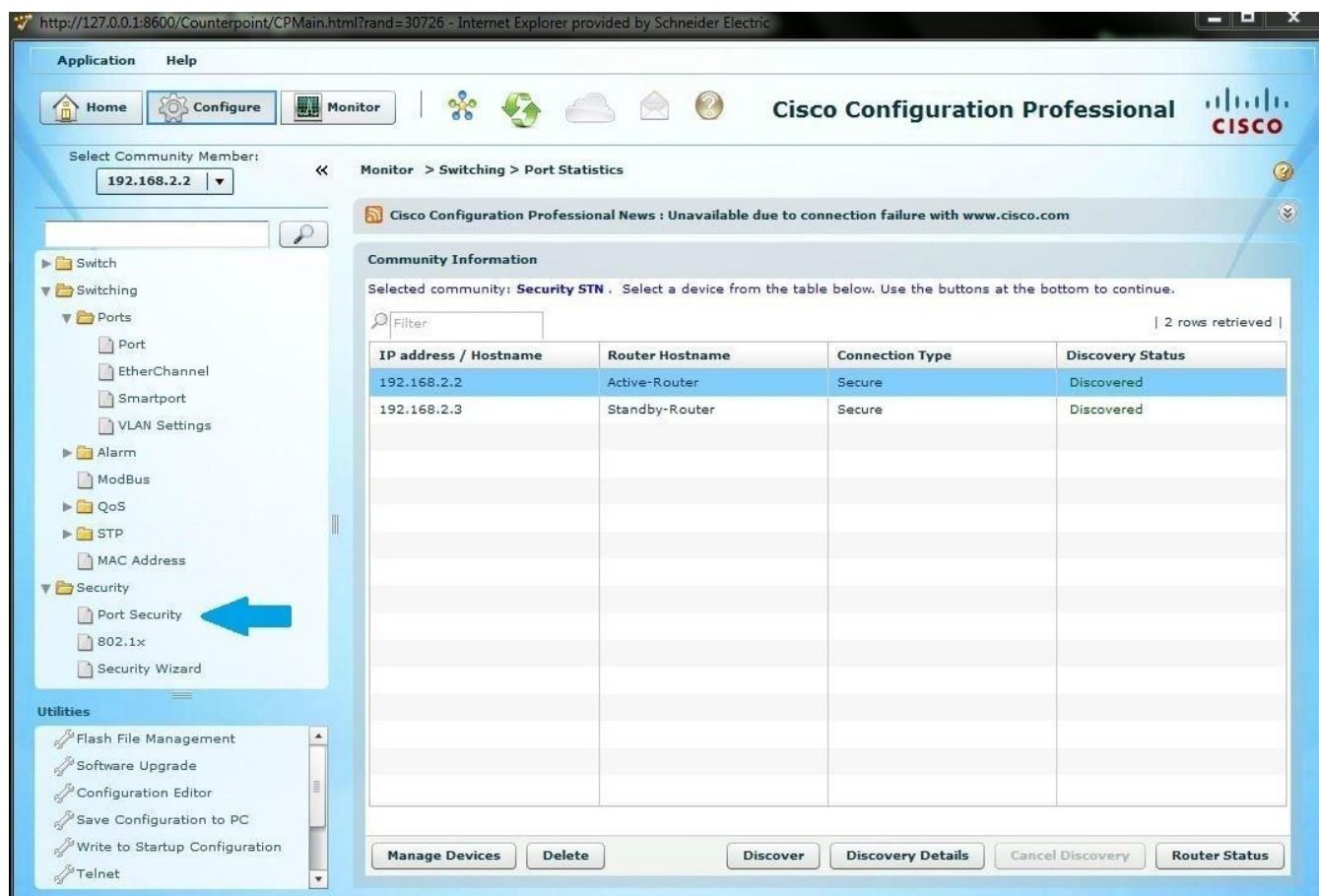


Figure 45: Port Security Step 1: Select Port Security from the Security Folder

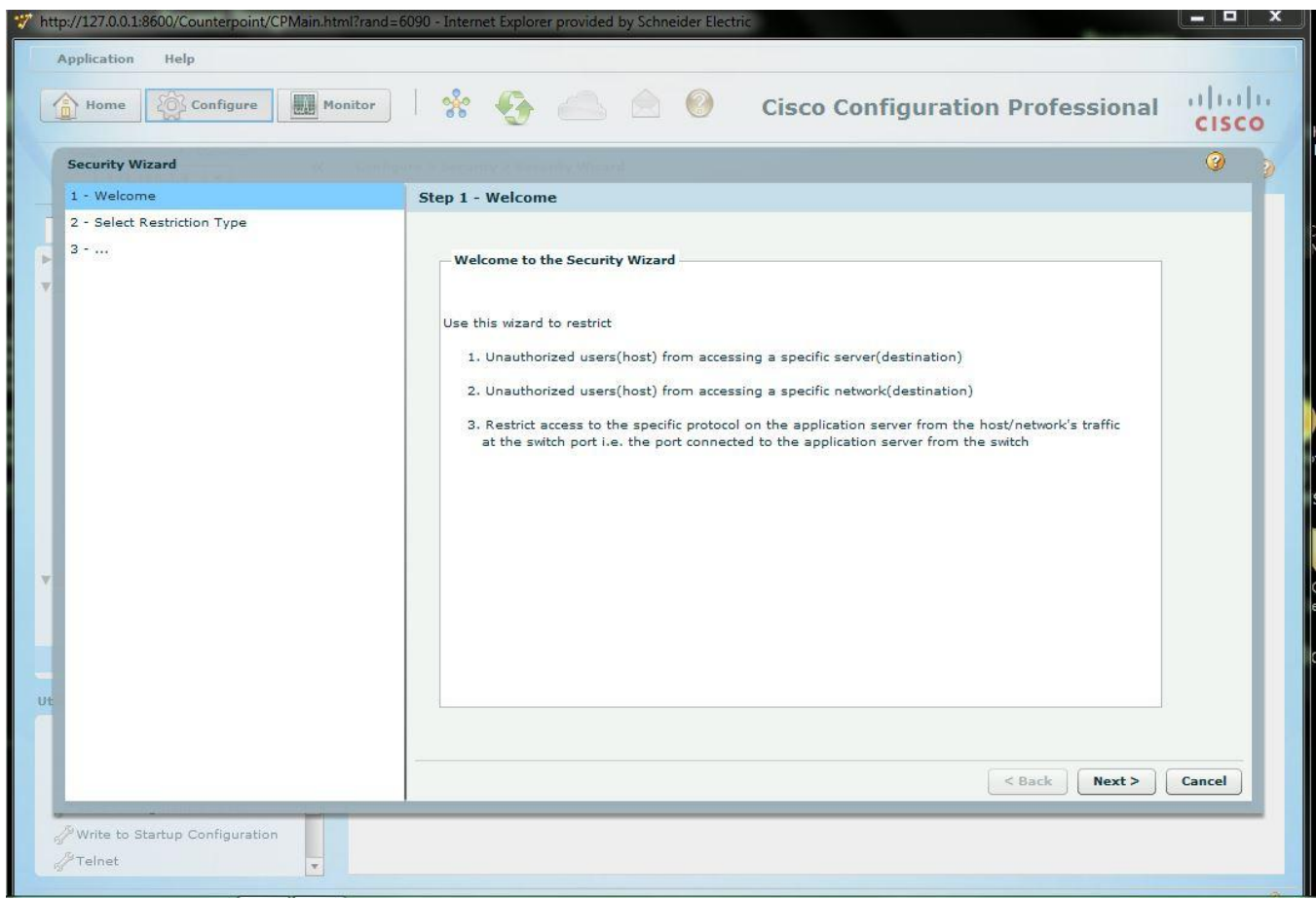


Figure 46: Port Security Step 2: Click Next

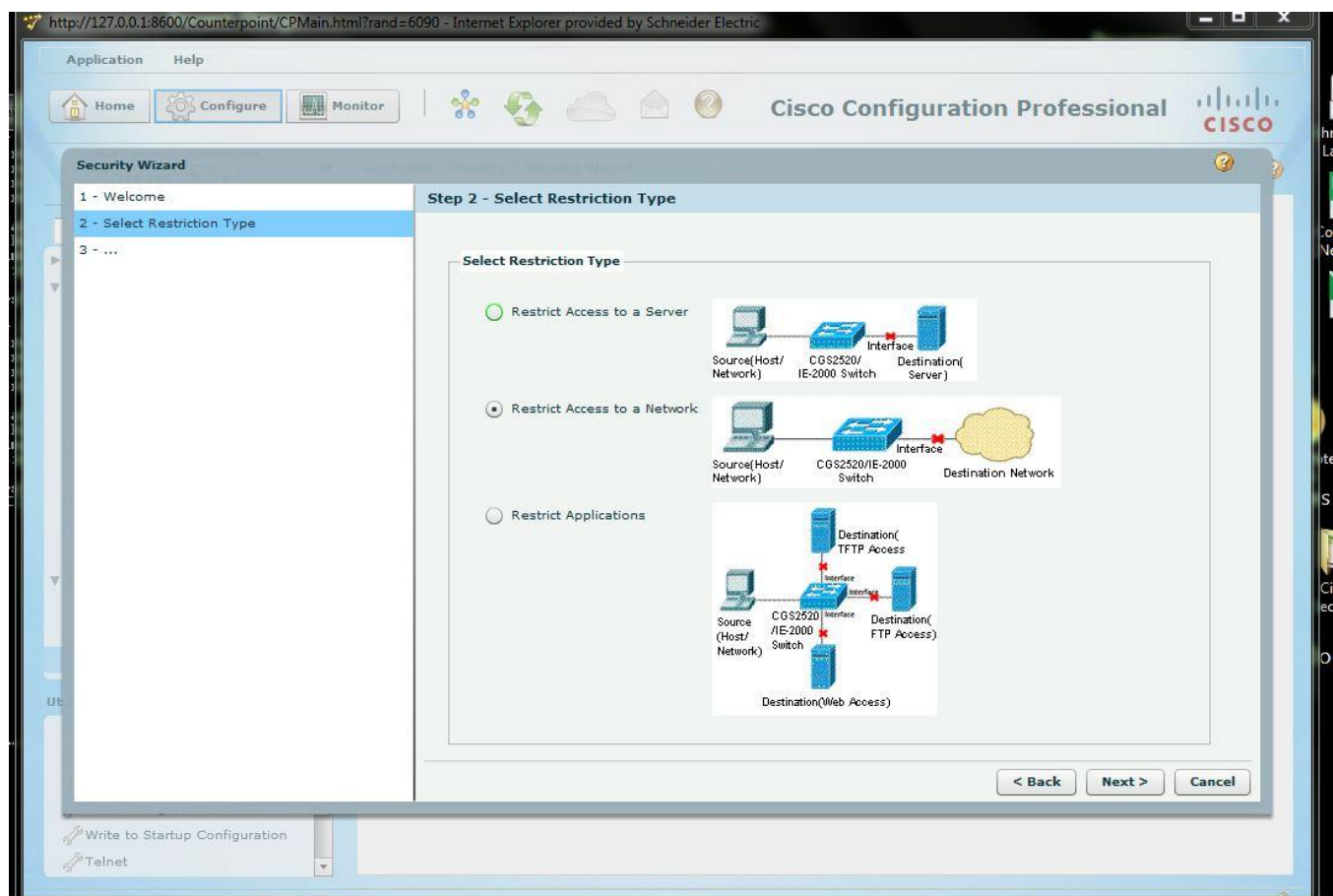


Figure 47: Port Security Step 3: Select Restrict Access to a Network then Click Next

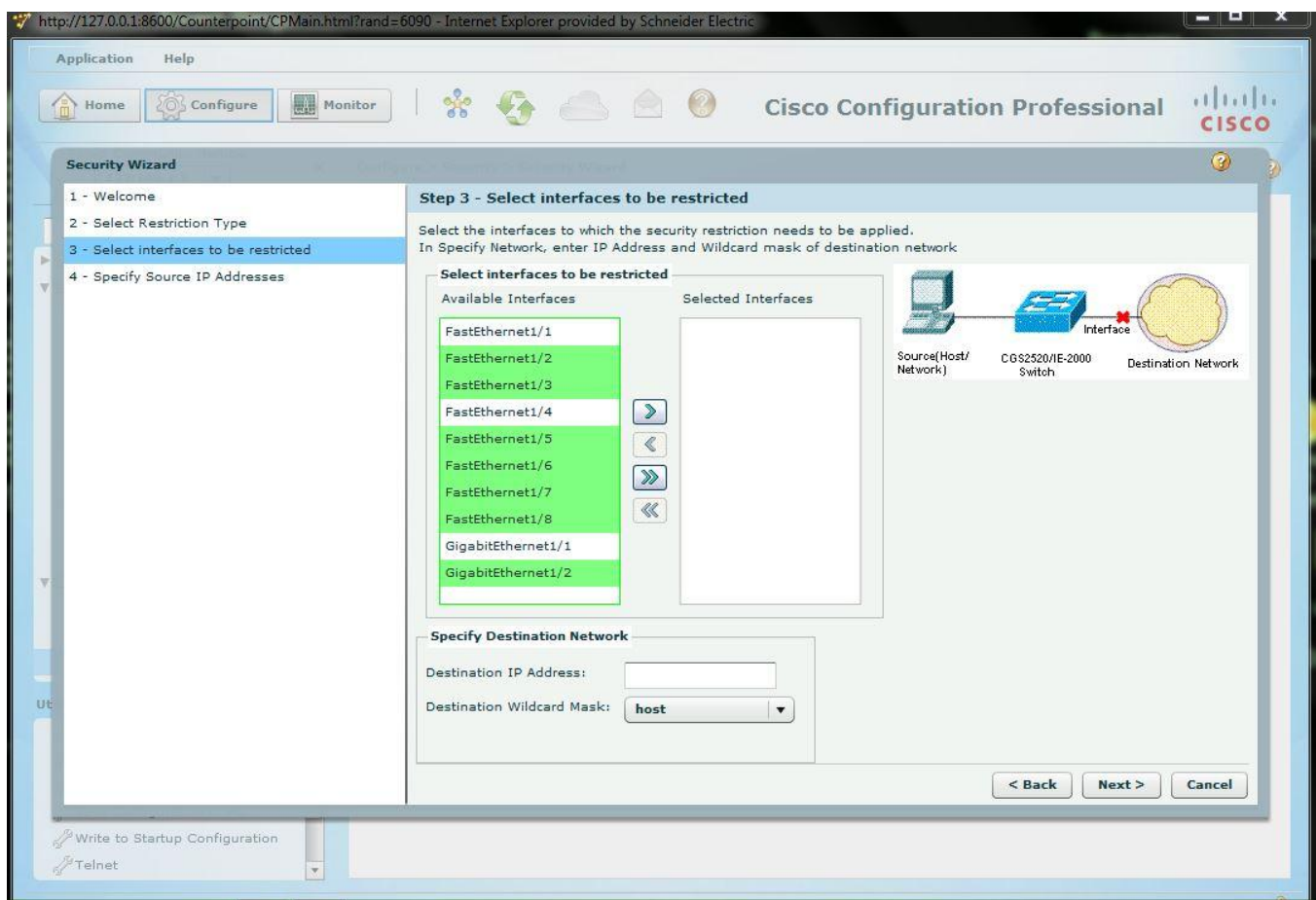


Figure 48: Port Security Step 4: Highlight the Interfaces to Secure, then click the > Button

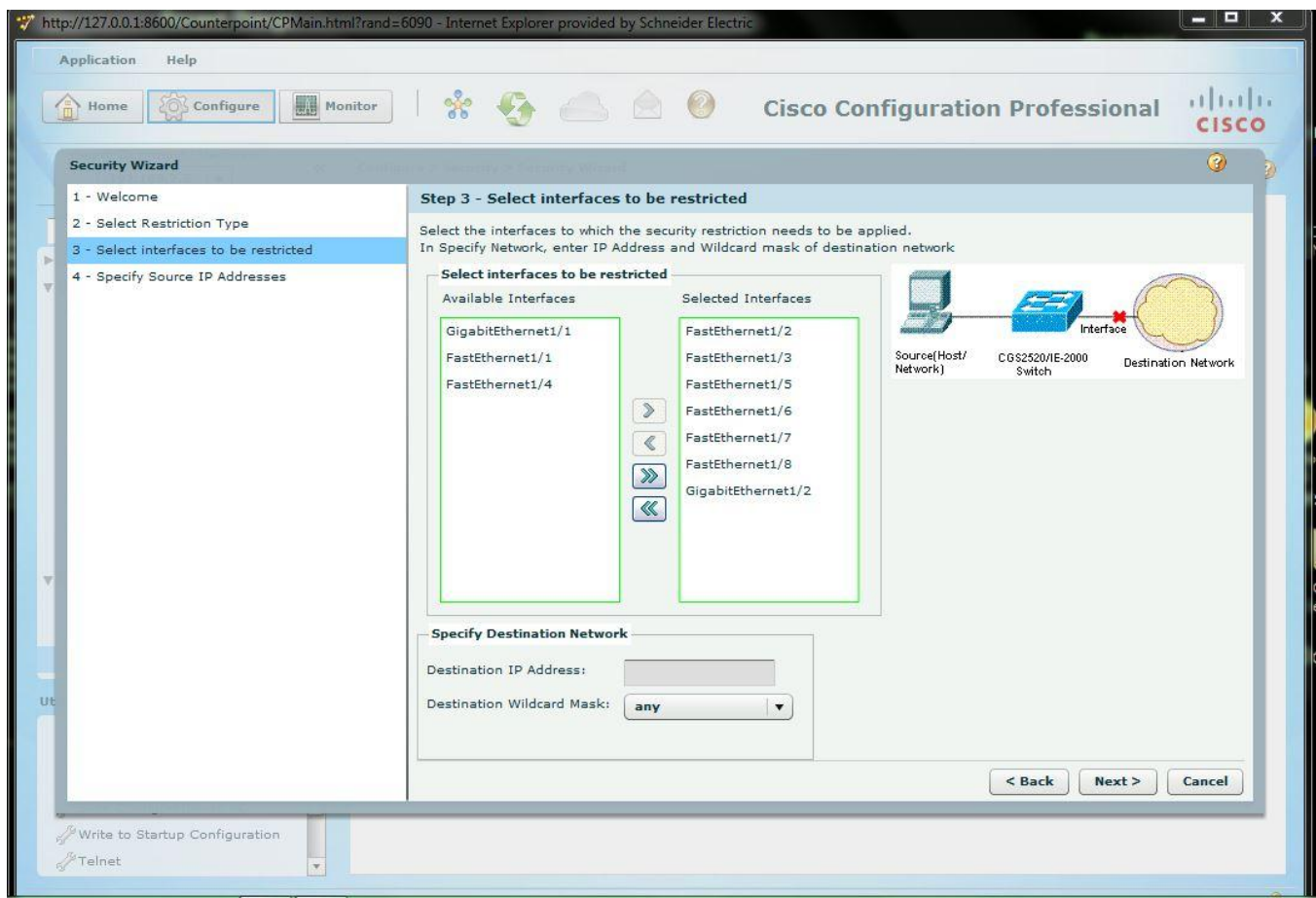


Figure 49: Port Security Step 5: Click Next

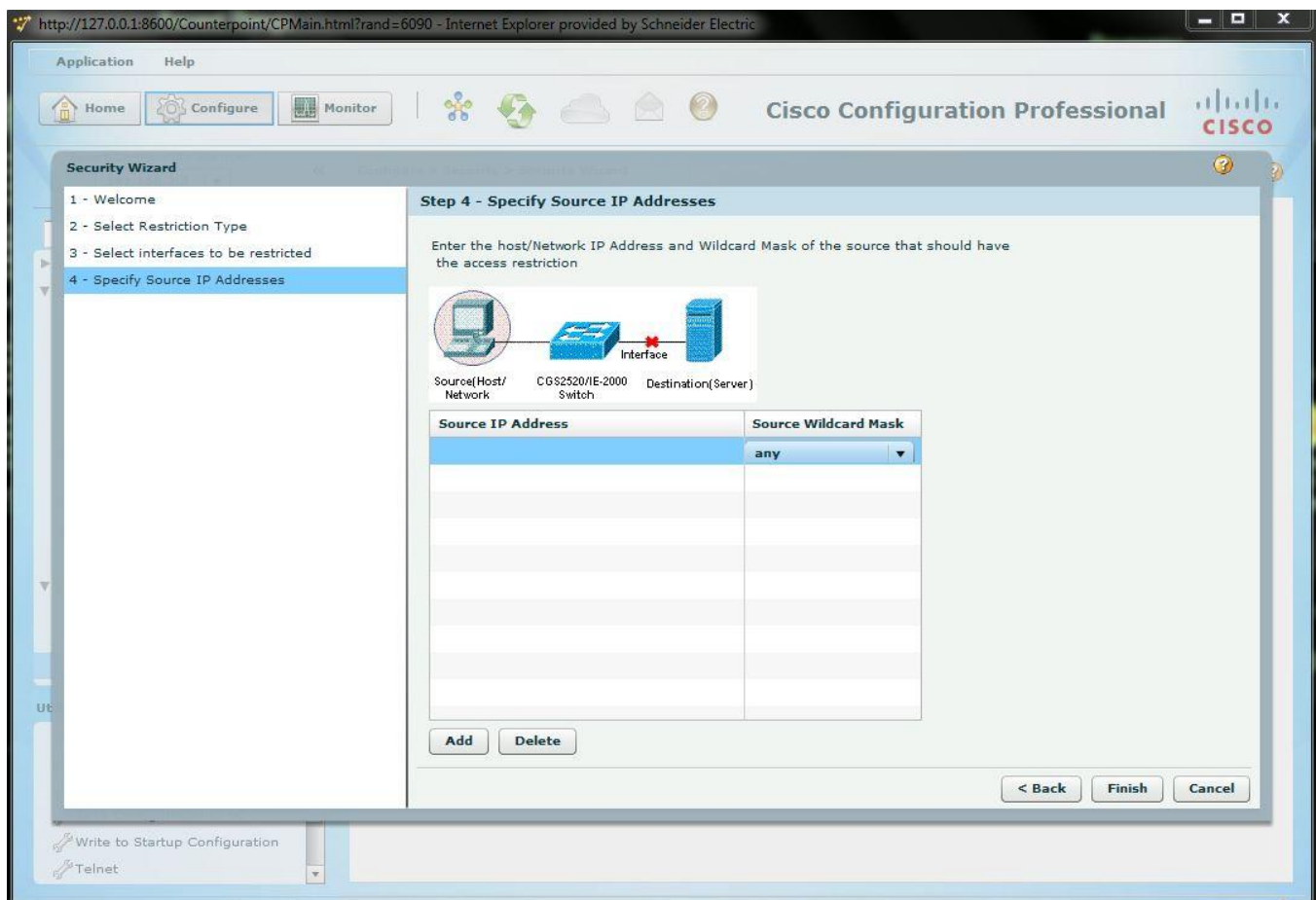


Figure 50: Port Security Step 6: Set Source Wildcard Mask to “any”, then click Finish

The wizard displays the ACL that will be delivered to the configuration, below:

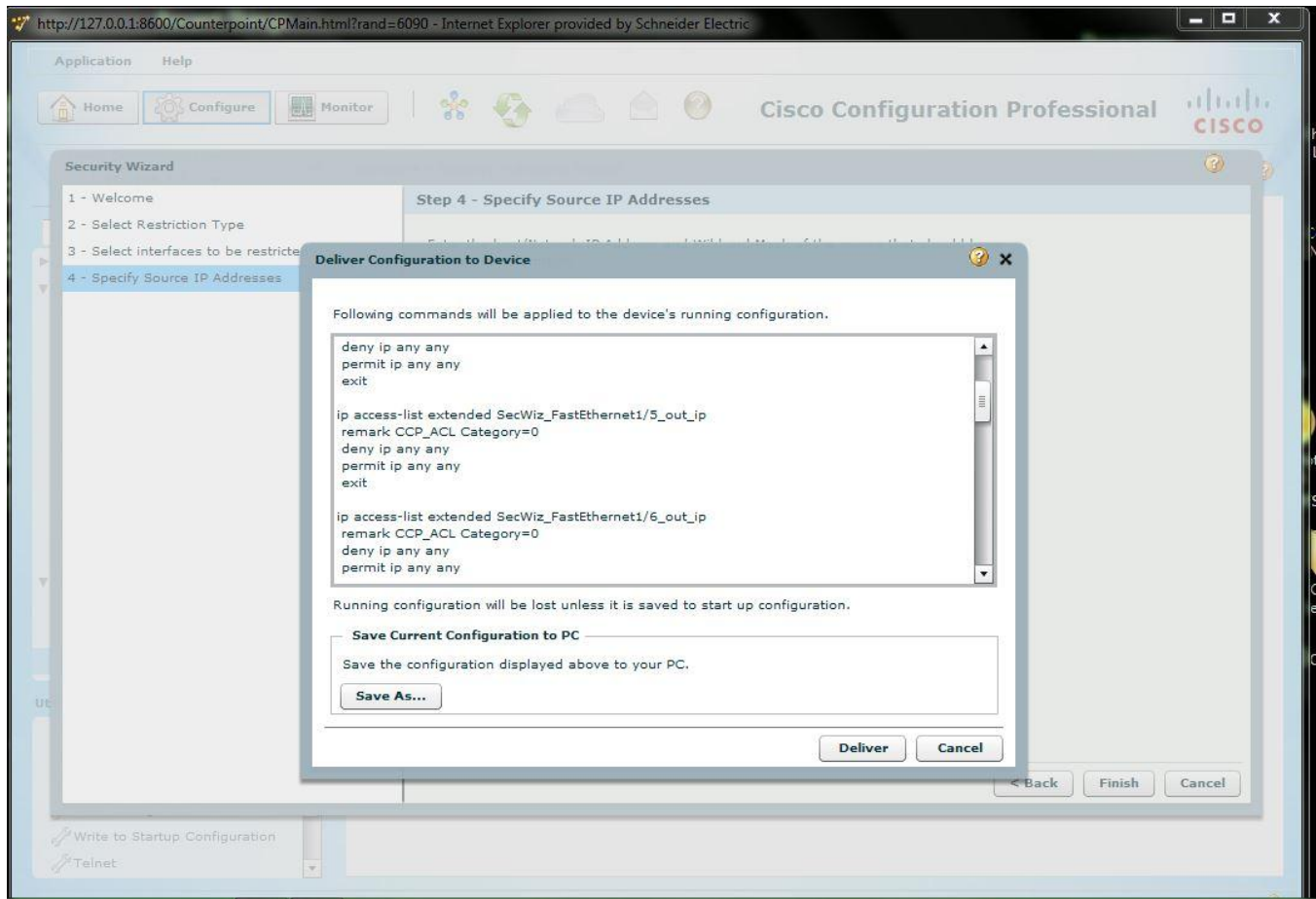


Figure 51: Port Security Step 7: Click Deliver

Here is a screenshot of the configuration that lists the ACL. Notice the ports are locked down by the **deny ip any any** statement:

```
ip access-list extended SecWiz_FastEthernet1/2_out_ip
remark CCP_ACL Category=0
deny ip any any
permit ip any any
ip access-list extended SecWiz_FastEthernet1/3_out_ip
remark CCP_ACL Category=0
deny ip any any
permit ip any any
ip access-list extended SecWiz_FastEthernet1/5_out_ip
remark CCP_ACL Category=0
deny ip any any
permit ip any any
ip access-list extended SecWiz_FastEthernet1/6_out_ip
remark CCP_ACL Category=0
deny ip any any
permit ip any any
ip access-list extended SecWiz_FastEthernet1/7_out_ip
remark CCP_ACL Category=0
deny ip any any
permit ip any any
ip access-list extended SecWiz_FastEthernet1/8_out_ip
remark CCP_ACL Category=0
deny ip any any
permit ip any any
ip access-list extended SecWiz_GigabitEthernet1/2_out_ip
remark CCP_ACL Category=0
deny ip any any
permit ip any any
```

Figure 52: Port Security: ACL Configuration

This is the ACL applied to the interfaces:

```
interface FastEthernet1/5
ip access-group SecWiz_FastEthernet1/5_out_ip in
shutdown
!
interface FastEthernet1/6
ip access-group SecWiz_FastEthernet1/6_out_ip in
shutdown
!
interface FastEthernet1/7
ip access-group SecWiz_FastEthernet1/7_out_ip in
shutdown
!
```

Figure 53: Port Security: Interface Shutdown

As an added measure the ports have the **shutdown** command applied.

For ports that remain active, port security helps prevent malicious attacks from disabling a switch by using a spoofed MAC address or by flooding the switch with erroneous MAC addresses, thereby rendering the switch inoperable. A violation such as those described here can then trigger a configured response such as discarding the packet or shutting down the port. CCP is used to help secure active ports. Configurable settings include: the maximum number of MAC address on the port, an inactivity timer, and the action to take if a violation is detected.

Here is the configuration for the access port connected to the network management workstation:

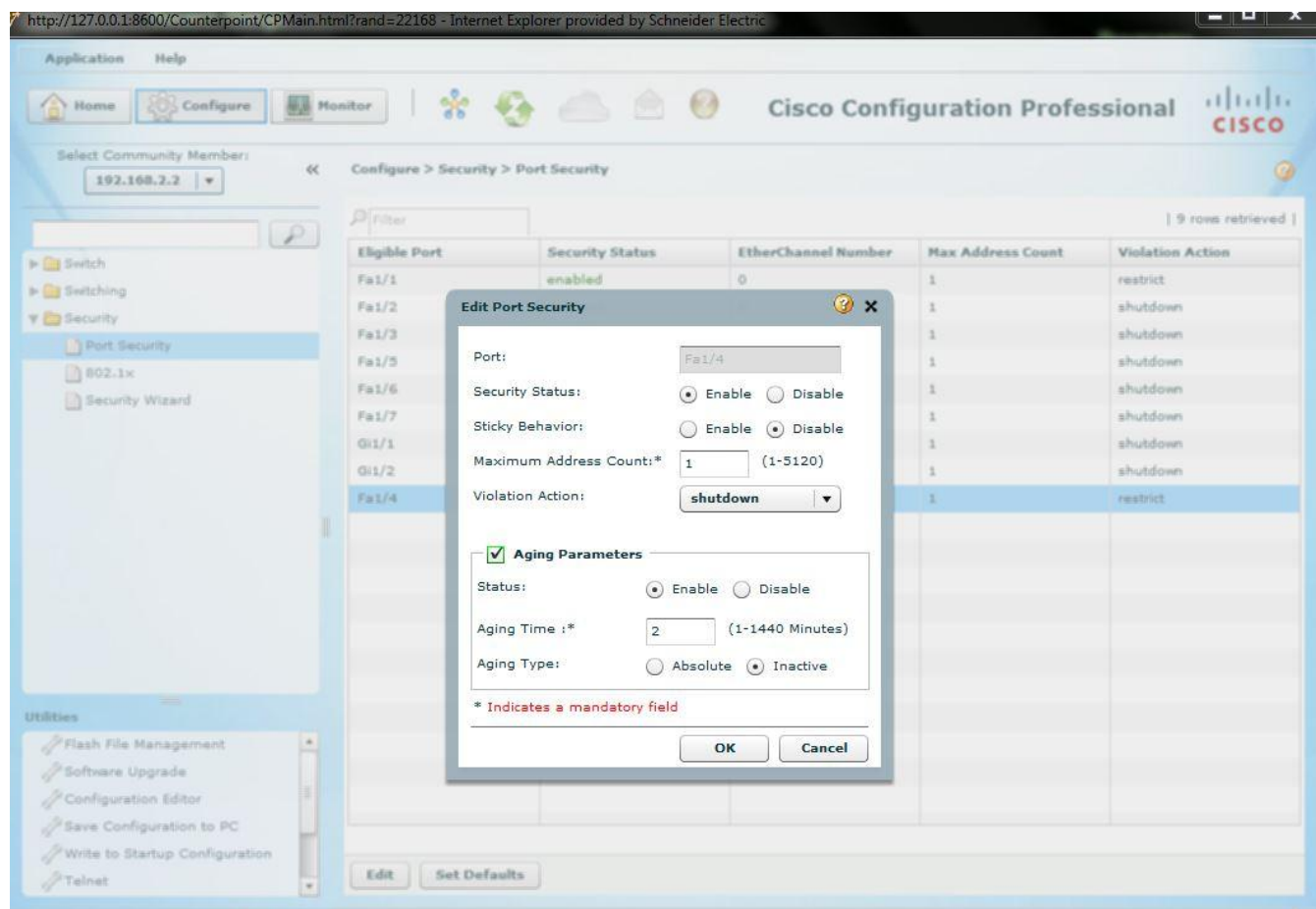


Figure 54: Network Management Workstation Access Port Configuration Settings

These settings help provide port security by allowing a maximum of one MAC address on the port. If there is a violation the port is shut down. This configuration also disables the port after two minutes of inactivity.

This is how the port configuration looks after these configuration settings are applied:

```
interface FastEthernet1/1
description Engineering WS
switchport access vlan 5
switchport mode access
switchport port-security
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
macro description cisco-ie-desktop ! cisco-desktop
spanning-tree portfast
spanning-tree bpduguard enable
```

Figure 55: Network Management Workstation Access Port Configuration Applied

4.3.8. Storm Control

The broadcast storm traffic control mechanism is configured on the switches in the control network. The percentage of packets received has been configured for the active ports. CNA displays the configured settings for switches in the network.

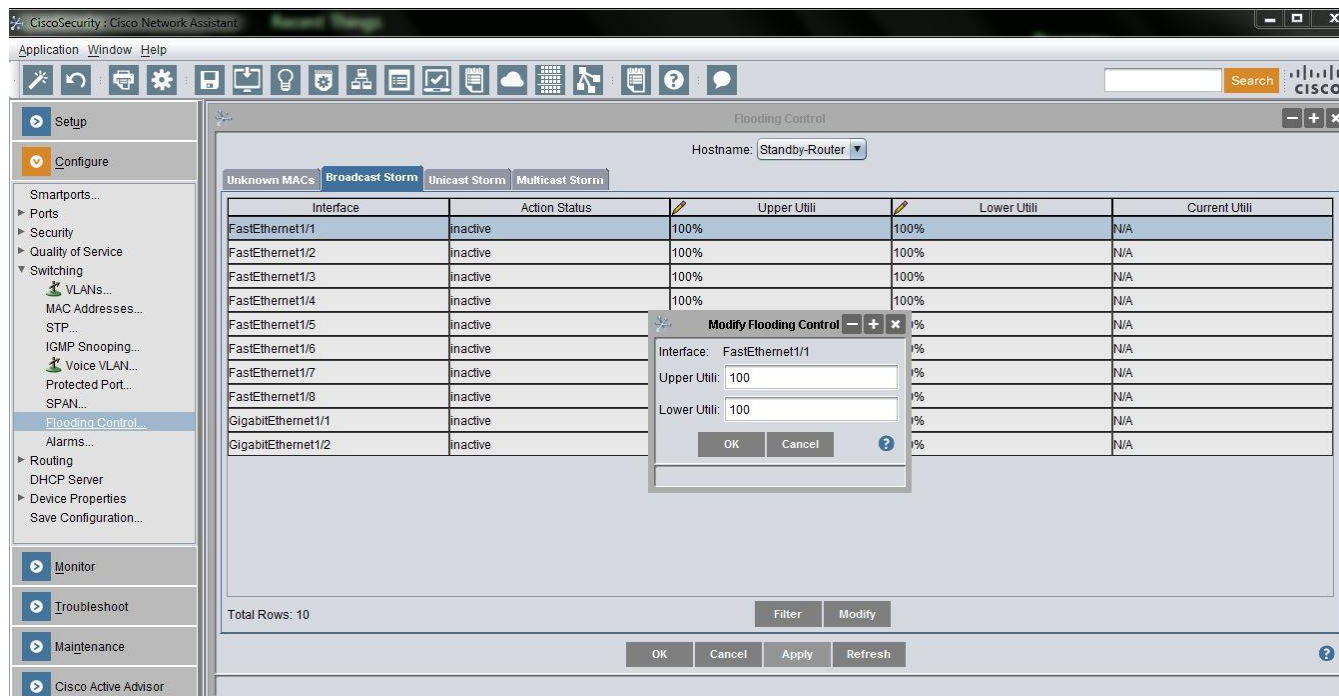


Figure 56: Configuring Storm Control

To configure broadcast storm control:

1. Select **Flooding Control** from the left side configure menu.
2. Click the **Broadcast Storm** tab.
3. Double-click on a port to open the Modify Flooding Control dialog.
4. Input values for the **Upper Utilization** and **Lower Utilization** limits.
5. Click **OK** to save settings for the selected port.

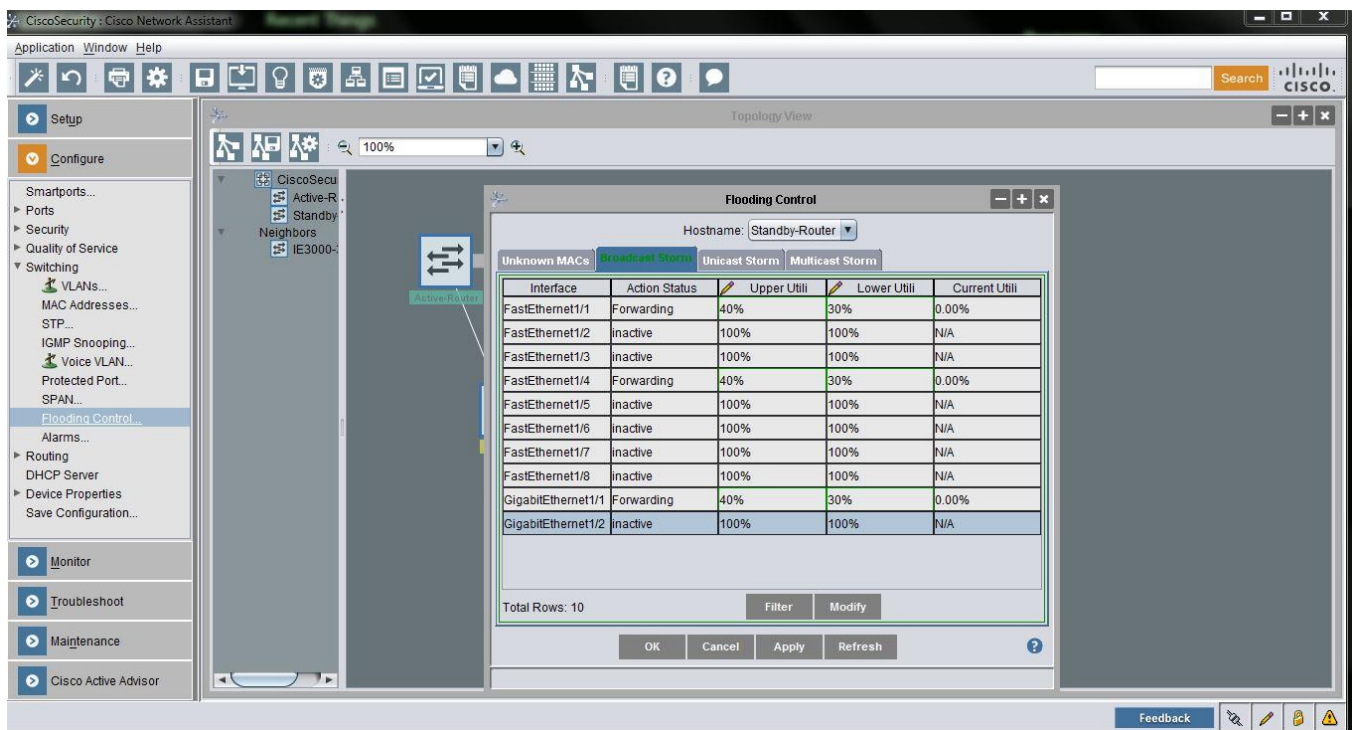


Figure 57: Completed Storm Control Settings

The upper and lower limits were set to 40% and 30% accordingly. This means that if greater than 40% of the bandwidth is used in a one second interval, the port will drop all packets and will not resume normal service until the level of bandwidth usage falls below 30%. The storm control feature is very effective when a broadcast storm occurs as a result of a network loop.

4.3.9. Root Guard / BPDU Guard / BPDU Filter

Root guard safeguards the network by keeping the root bridge in control. Enable root guard is enabled on the root bridge port and all the other switch ports in the STP ring. Here is a screenshot of CNA configuring root guard:

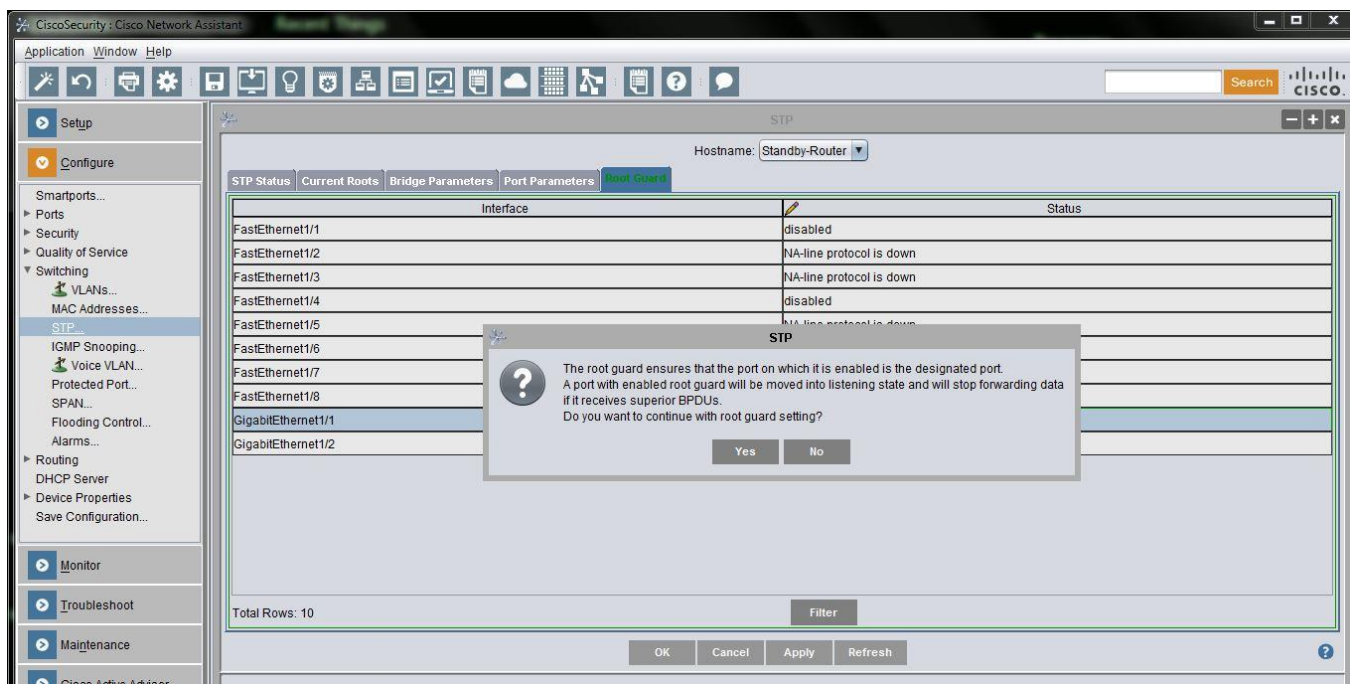


Figure 58: Configuring Root Guard

In the lab control network interface, GigabitEthernet 1/1 is the port connected to the other switch that is passing BPDUs every two seconds.

BPDU guard stops an access port from receiving inadvertent BPDU. An access port controls end devices such as PCs. BPDUs are informational messages between network switches. They transmit information (such as switch adjacency), act as keep-alive messages, and control the RSTP ring topology by defining the state of the device (forwarding or blocking) and the path to the root bridge (top of the RSTP tree).

An access port should not receive BPDUs because there is no network switch connected to this port. A malicious user may attempt to inject a false BPDU into the network to cause a disruption or attempt to redirect control of the network.

With BPDU guard, if a malicious user injects a BPDU meant to cause a disruption of the RSTP ring, the port is disabled. The last line of the screenshot below enables BPDU guard.

```
interface FastEthernet1/1
description Engineering WS
switchport access vlan 5
switchport mode access
switchport port-security
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
macro description cisco-ie-desktop ! cisco-desktop
spanning-tree portfast
spanning-tree bpduguard enable
```

Figure 59: Enabling Root Guard

Using CNA to configure a port with the smartport feature, create a macro which defines the port as an access port and enables BPDU guard. Here is an example of defining a port as an access port:

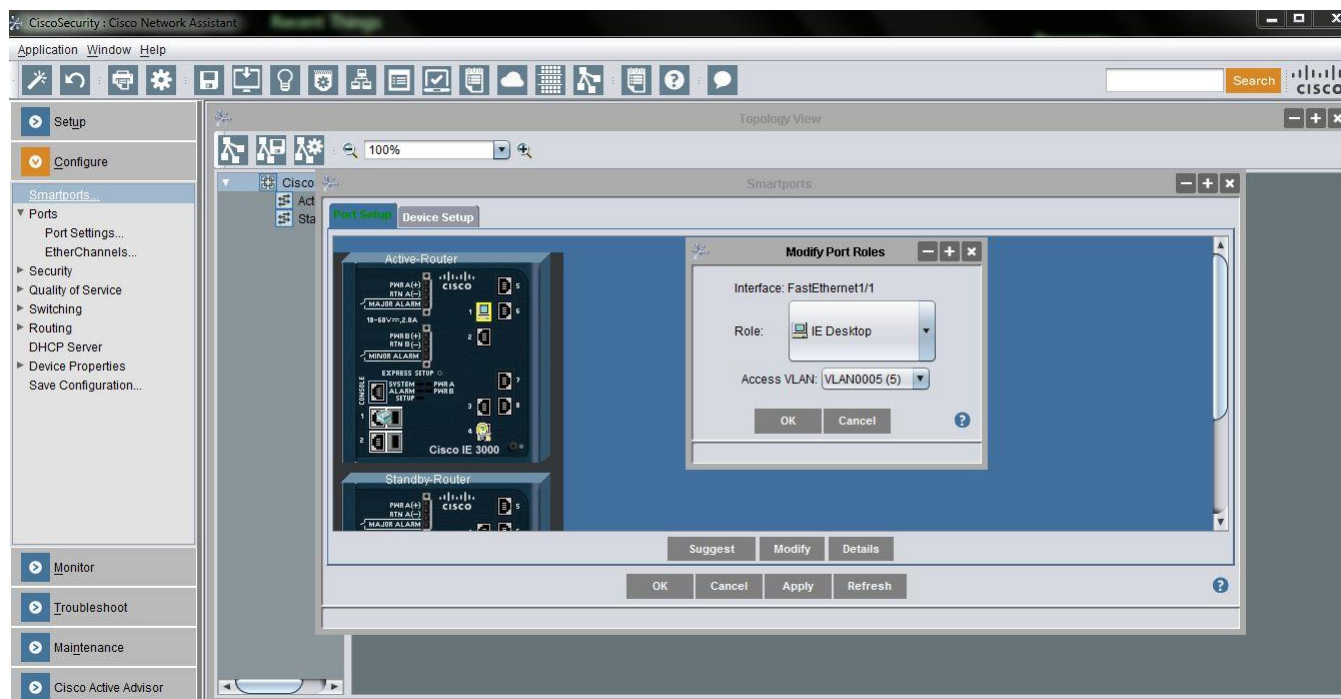


Figure 60: Defining an Access Port

BPDU filter causes the switch to drop BPDU packets received on the port. Similar to BPDU guard, it is applied on an interface and will drop BPDUs. Here is an example of BPDU guard at work in the process control network:

```
interface FastEthernet1/4
description To PAC
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security aging time 2
switchport port-security aging type inactivity
ip arp inspection trust
macro description cisco-desktop
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree bpduguard disable
ip verify source
```

Figure 61: BPDU Guard Example


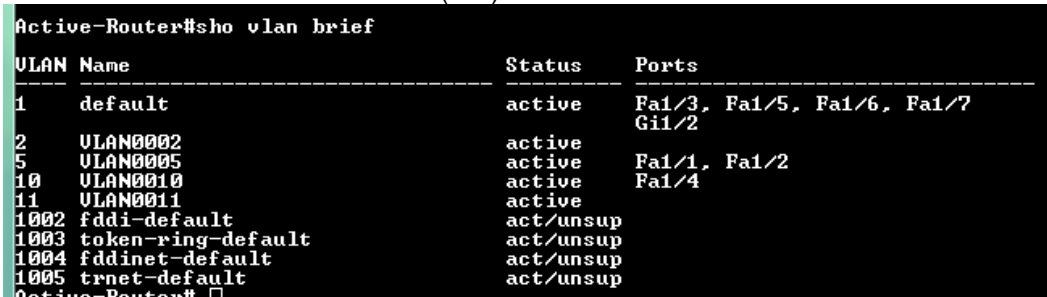
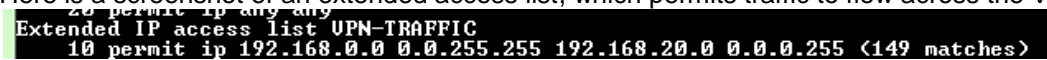
5. Validation

Two types of functional tests were performed to validate the example system:

- General operational tests
- Security feature tests, i.e. port scanning, vulnerability scanning and penetration

5.1. General Operational Tests

The following table describes the results of tests performed to verify the operation of the security features of the Cisco switches:

Test	Result	Discussion
Protocol Authentication	PASS	Functions according to specification. See Figure 31 in section 4.2.2.
VLANs	PASS	<p>Functions according to specification. Here is a screenshot of the VLANs on the switches:</p>  <p>These are switched virtual interfaces (SVI). Here is a screenshot of the SVIs on the switch:</p> 
Access Lists	PASS	<p>Functions according to specification.</p> <p>Here is a screenshot of an extended access list, which permits traffic to flow across the VPN:</p>  <p>All devices in 192.168.0.0/16 can reach the 192.168.20.0/24 subnet which is on another switch across the VPN. The Encryption test, which is the next test, proves it is operating as required.</p>

Test	Result	Discussion
Encryption	PASS	<p>Functions according to specification.</p> <p>Wireshark of ping to 192.168.20.1 from switch:</p> <pre>Active-Router#ping 192.168.20.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds: .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 1/4/9 ms Active-Router#</pre> <p>Here is a screenshot of the log from the switch showing encryption of the packets:</p> <pre>Active-Router# sho crypto ipsec sa interface: FastEthernet1/8 Crypto map tag: CMAP, local addr 10.10.10.1 protected vrf: <none> local ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0) current_peer 10.10.10.2 port 500 PERMIT, flags=<origin_is_acl> #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19 #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 19 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/8 current outbound spi: 0x571D549F(146153999) PFS (Y/N): Y, DH group: none inbound esp sas: spi: 0xCA60D83D(339534444) transform: esp-256-aes esp-sha256-hmac , --More-- in use settings =(Tunnel,) conn id: 11, flow_id: 11, sibling_flags 80000040, crypto map: CMAP sa timing: remaining key lifetime (k/sec): (4317869/3536) IV size: 16 bytes replay detection support: Y Status: ACTIVE</pre> <p>Connected to other switch on interface 1/8</p> <p>Routes permitted</p> <p>Packets Encrypted</p> <p>Address of tunnel endpoints</p> <p>Status</p>
Port Security	PASS	<p>Functions according to specification.</p> <p>Here is a screenshot showing port security enabled on interface FA1/1:</p> <pre>Active-Router#sho port-security Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action (Count) (Count) (Count) ----- Fa1/1 1 1 0 Restrict Total Addresses in System (excluding one mac per port) : 0 Max Addresses limit in System (excluding one mac per port) : 2048 Active-Router#</pre> <p>This port is set to allow only one device (one MAC per port). The addition of another device on that port causes a security violation.</p> <p>Here is a syslog trap sent for a violation:</p> <pre>Critical / local 3 (192.168.5.2) %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0080.6301.ad1f on port FastEthernet1/4.</pre>

Test	Result	Discussion
MAC Move Notification	PASS	<p>Functions according to specification. Here is a screenshot of the status of the option:</p> <div><pre>Active-Router#sho mac address-table notification change MAC Notification Feature is Enabled on the switch Interval between Notification Traps : 123 secs Number of MAC Addresses Added : 6 Number of MAC Addresses Removed : 0 Number of Notifications sent to NMS : 5 Maximum Number of entries configured in History Table : 100 Current History Table Length : 2 MAC Notification Traps are Enabled History Table contents History Index 1, Entry Timestamp 70062127, Despatch Timestamp 70062127 MAC Changed Message : Operation: Added Ulan: 5 MAC Addr: 0024.9b0c.3755 Dot1dBasePort: 4 Operation: Added Ulan: 5 MAC Addr: 0024.9b0c.3755 Dot1dBasePort: 4 History Index 2, Entry Timestamp 70074428, Despatch Timestamp 70074428 MAC Changed Message : Operation: Added Ulan: 5 MAC Addr: 0024.9b0c.3755 Dot1dBasePort: 3 Active-Router#sho mac address-table notification change interface MAC Notification Feature is Enabled on the switch MAC Notification Flags For All Ethernet Interfaces : Interface MAC Added Trap MAC Removed Trap ----- FastEthernet1/1 Enabled Disabled FastEthernet1/2 Enabled Disabled FastEthernet1/3 Disabled Disabled FastEthernet1/4 Disabled Disabled FastEthernet1/5 Disabled Disabled FastEthernet1/6 Disabled Disabled FastEthernet1/7 Disabled Disabled GigabitEthernet1/1 Disabled Disabled GigabitEthernet1/2 Disabled Disabled Active-Router#sho mac address-table notification mac-move MAC Move Notification: enabled Active-Router#</pre></div> <p>Traps sent to Network Management System</p> <p>Must be enabled on the interface</p> <p>Move enabled</p>
Loop Guard (storm control)	PASS	<p>Functions according to specification. A network loop was created by adding additional multiple port from a single switch without the use of spanning tree. This generated a network loop. Here is a screenshot of the syslog trap for the loop guard:</p> <div><pre>Error Oct 26 19:40:06.337 129 %LINK-3-UPDOWN: Interface FastEthernet1/2, changed state to down Notice Oct 26 19:40:05.330 128 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/2, changed state to down Critical Oct 26 19:39:32.581 127 %SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet1/2 on VLAN0005.</pre></div>
Port Blocking	PASS	<p>Functions according to specification. Two Schneider Electric ConneXium switches were then connected to that port. This caused the number of MAC address to exceed the maximum number of allowed MAC addresses. In response to this violation, the port is blocked.</p> <p>Here is a screenshot of the syslog trap for blocking a port:</p> <div><pre>Critical / local 3 (192.168.5.2) %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0080.6301.ad1f on port FastEthernet1/4.</pre></div>
BDPU Filter	PASS	<p>Functions according to specification. BPDU filter was enabled on interface fa1/2:</p> <div><pre>interface FastEthernet1/2 switchport access vlan 5 switchport mode access spanning-tree bpdufilter enable</pre></div> <p>A ConneXium switch that sends out BPDUs every 2 seconds was then connected to that port. With the BPDU filter, the BPDUs are discarded and there is no network service interruption. The network continues to function normally while this condition persists.</p>

Test	Result	Discussion																																																																				
BPDU Guard	PASS	<p>Functions according to specification. The port was configured with this feature:</p> <div><pre>interface FastEthernet1/1 description Engineering WS switchport access vlan 5 switchport mode access switchport port-security switchport port-security aging time 2 switchport port-security violation restrict switchport port-security aging type inactivity macro description cisco-ie-desktop ! cisco-desktop spanning-tree portfast spanning-tree bpduguard enable</pre></div> <p>BPDU Guard</p> <p>Several ConneXium switches were then connected to this port, which has RSTP enabled, is sending a BPDU every 2s, and is configured as an access port. This is a security violation. Here is a screenshot of the syslog trap for the BPDU guard:</p> <table><tr><td>Warning</td><td>Oct 26 19:39:26.575</td><td>123</td><td>%PM-4-ERR_DISABLE: bpduguard error detected on Fa1/1, putting Fa1/1 in err-disable state</td></tr><tr><td>Critical</td><td>Oct 26 19:39:26.575</td><td>122</td><td>%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/1 with BPDU Guard enabled. Disabling port.</td></tr><tr><td>Error</td><td>Oct 26 19:39:26.164</td><td>121</td><td>%LINK-3-UPDOWN: Interface FastEthernet1/2, changed state to up</td></tr><tr><td>Notice</td><td>Oct 26 19:38:02.688</td><td>120</td><td>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up</td></tr></table>	Warning	Oct 26 19:39:26.575	123	%PM-4-ERR_DISABLE: bpduguard error detected on Fa1/1, putting Fa1/1 in err-disable state	Critical	Oct 26 19:39:26.575	122	%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/1 with BPDU Guard enabled. Disabling port.	Error	Oct 26 19:39:26.164	121	%LINK-3-UPDOWN: Interface FastEthernet1/2, changed state to up	Notice	Oct 26 19:38:02.688	120	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up																																																				
Warning	Oct 26 19:39:26.575	123	%PM-4-ERR_DISABLE: bpduguard error detected on Fa1/1, putting Fa1/1 in err-disable state																																																																			
Critical	Oct 26 19:39:26.575	122	%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/1 with BPDU Guard enabled. Disabling port.																																																																			
Error	Oct 26 19:39:26.164	121	%LINK-3-UPDOWN: Interface FastEthernet1/2, changed state to up																																																																			
Notice	Oct 26 19:38:02.688	120	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up																																																																			
Root Guard	PASS	<p>Functions according to specification. A ConneXium switch with a lower bridge priority was added to the test bed. It generated a BPDU election to become the root bridge. Because root guard was enabled on the existing root device, the BPDUs were blocked and the switch generated a root guard trap. Here is the screenshot from the syslog:</p> <table><tr><td>Critical</td><td>Oct 26 18:36:30.804</td><td>6949</td><td>%SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet1/1 on VLAN0005.</td></tr></table>	Critical	Oct 26 18:36:30.804	6949	%SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet1/1 on VLAN0005.																																																																
Critical	Oct 26 18:36:30.804	6949	%SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet1/1 on VLAN0005.																																																																			
Logging to syslog	PASS	<p>Functions according to specification. Shown below is the running syslog server:</p> <table><tr><td>Notice</td><td>Sep 18 14:16:57.799</td><td>339</td><td>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...</td></tr><tr><td>Error</td><td>Sep 18 14:16:56.792</td><td>338</td><td>%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up</td></tr><tr><td>Error</td><td>Sep 18 14:16:12.643</td><td>337</td><td>%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down</td></tr><tr><td>Notice</td><td>Sep 18 14:16:11.636</td><td>336</td><td>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...</td></tr><tr><td>Notice</td><td>Sep 18 14:14:34.881</td><td>335</td><td>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...</td></tr><tr><td>Error</td><td>Sep 18 14:14:33.875</td><td>334</td><td>%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up</td></tr><tr><td>Notice</td><td>SEP 16 19:26:13</td><td>HM_HPL_F... 192.168.11.25-1</td><td>src/hmpriv_main.c(301) 323 %% H_Event S_hpl_LINK_UP (3-0-0-0)</td></tr><tr><td>Notice</td><td>SEP 16 19:26:13</td><td>TRAPMGR... 192.168.11.25-1</td><td>traputil.c(697) 322 %% Link Up: Unit: 1 Slot: 1 Port: 3</td></tr><tr><td>Notice</td><td>SEP 16 19:26:07</td><td>HM_HPL_F... 192.168.11.25-1</td><td>src/hmpriv_main.c(324) 321 %% H_Event S_hpl_LINK_DOWN (3-0-0-0)</td></tr><tr><td>Notice</td><td>SEP 16 19:26:07</td><td>TRAPMGR... 192.168.11.25-1</td><td>traputil.c(697) 320 %% Link Down: Unit: 1 Slot: 1 Port: 3</td></tr><tr><td>Error</td><td>SEP 16 19:26:06</td><td>DOT1S[111]... 192.168.11.25-1</td><td>dot1s_ih.c(1704) 319 %% d1lDot1sStateSet failed intflNum 3, instance ID 0 state 4</td></tr><tr><td>Notice</td><td>Sep 16 18:12:33.104</td><td>333</td><td>%SYS-5-CONFIG: I: Configured from console by vty5 (192.168.5.202)</td></tr><tr><td>Error</td><td>Sep 16 17:23:06.803</td><td>332</td><td>%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down</td></tr><tr><td>Notice</td><td>Sep 16 17:23:05.796</td><td>331</td><td>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...</td></tr><tr><td>Notice</td><td>Sep 16 17:23:04.445</td><td>330</td><td>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...</td></tr><tr><td>Error</td><td>Sep 16 17:23:03.439</td><td>329</td><td>%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up</td></tr><tr><td>Notice</td><td>Sep 16 15:44:07.355</td><td>328</td><td>%SYS-5-CONFIG: I: Configured from console by vty5 (192.168.5.202)</td></tr></table>	Notice	Sep 18 14:16:57.799	339	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...	Error	Sep 18 14:16:56.792	338	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up	Error	Sep 18 14:16:12.643	337	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down	Notice	Sep 18 14:16:11.636	336	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...	Notice	Sep 18 14:14:34.881	335	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...	Error	Sep 18 14:14:33.875	334	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up	Notice	SEP 16 19:26:13	HM_HPL_F... 192.168.11.25-1	src/hmpriv_main.c(301) 323 %% H_Event S_hpl_LINK_UP (3-0-0-0)	Notice	SEP 16 19:26:13	TRAPMGR... 192.168.11.25-1	traputil.c(697) 322 %% Link Up: Unit: 1 Slot: 1 Port: 3	Notice	SEP 16 19:26:07	HM_HPL_F... 192.168.11.25-1	src/hmpriv_main.c(324) 321 %% H_Event S_hpl_LINK_DOWN (3-0-0-0)	Notice	SEP 16 19:26:07	TRAPMGR... 192.168.11.25-1	traputil.c(697) 320 %% Link Down: Unit: 1 Slot: 1 Port: 3	Error	SEP 16 19:26:06	DOT1S[111]... 192.168.11.25-1	dot1s_ih.c(1704) 319 %% d1lDot1sStateSet failed intflNum 3, instance ID 0 state 4	Notice	Sep 16 18:12:33.104	333	%SYS-5-CONFIG: I: Configured from console by vty5 (192.168.5.202)	Error	Sep 16 17:23:06.803	332	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down	Notice	Sep 16 17:23:05.796	331	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...	Notice	Sep 16 17:23:04.445	330	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...	Error	Sep 16 17:23:03.439	329	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up	Notice	Sep 16 15:44:07.355	328	%SYS-5-CONFIG: I: Configured from console by vty5 (192.168.5.202)
Notice	Sep 18 14:16:57.799	339	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...																																																																			
Error	Sep 18 14:16:56.792	338	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up																																																																			
Error	Sep 18 14:16:12.643	337	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down																																																																			
Notice	Sep 18 14:16:11.636	336	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...																																																																			
Notice	Sep 18 14:14:34.881	335	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...																																																																			
Error	Sep 18 14:14:33.875	334	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up																																																																			
Notice	SEP 16 19:26:13	HM_HPL_F... 192.168.11.25-1	src/hmpriv_main.c(301) 323 %% H_Event S_hpl_LINK_UP (3-0-0-0)																																																																			
Notice	SEP 16 19:26:13	TRAPMGR... 192.168.11.25-1	traputil.c(697) 322 %% Link Up: Unit: 1 Slot: 1 Port: 3																																																																			
Notice	SEP 16 19:26:07	HM_HPL_F... 192.168.11.25-1	src/hmpriv_main.c(324) 321 %% H_Event S_hpl_LINK_DOWN (3-0-0-0)																																																																			
Notice	SEP 16 19:26:07	TRAPMGR... 192.168.11.25-1	traputil.c(697) 320 %% Link Down: Unit: 1 Slot: 1 Port: 3																																																																			
Error	SEP 16 19:26:06	DOT1S[111]... 192.168.11.25-1	dot1s_ih.c(1704) 319 %% d1lDot1sStateSet failed intflNum 3, instance ID 0 state 4																																																																			
Notice	Sep 16 18:12:33.104	333	%SYS-5-CONFIG: I: Configured from console by vty5 (192.168.5.202)																																																																			
Error	Sep 16 17:23:06.803	332	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to down																																																																			
Notice	Sep 16 17:23:05.796	331	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...																																																																			
Notice	Sep 16 17:23:04.445	330	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state ...																																																																			
Error	Sep 16 17:23:03.439	329	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up																																																																			
Notice	Sep 16 15:44:07.355	328	%SYS-5-CONFIG: I: Configured from console by vty5 (192.168.5.202)																																																																			
NTP	PASS	<p>Functions according to specification. Here is a syslog entry showing the NTP server is operational:</p> <table><tr><td>Notice</td><td>OCT 22 10:36:31</td><td>TRAPMGR... 192.168.10.25-1</td><td>traputil.c(697) 193 %% saSNTPTrap: saNetSNTPOperStatus: 1</td></tr></table>	Notice	OCT 22 10:36:31	TRAPMGR... 192.168.10.25-1	traputil.c(697) 193 %% saSNTPTrap: saNetSNTPOperStatus: 1																																																																
Notice	OCT 22 10:36:31	TRAPMGR... 192.168.10.25-1	traputil.c(697) 193 %% saSNTPTrap: saNetSNTPOperStatus: 1																																																																			

Test	Result	Discussion
Dynamic ARP Inspection / DHCP Snooping	PASS	<p>Functions according to specification. Shown below is a DAI event on a non trusted port.</p> <p>The screenshot shows a log entry with a red arrow pointing to the warning message. The message is: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/1, vlan 11. ([381c.1a8c.ccc4/192.168.11.2/0000.0000.0000/192.168.11.4/10:28:01 EDT Wed Sep 16 2015])</p>

Table 1: General operational tests

5.2. Security Feature Tests

Several open source tools were used to perform a comprehensive test of the security of the example system. These tools included Zenmap (used for port scanning), W3af (used for web vulnerability scanning) and Kali Linux (used for additional penetration testing).

5.2.1. Zenmap

Zenmap is a software application that provides a graphical interface to the NMAP network discovery and security auditing tool. Zenmap was run against the Cisco switches to scan for open TCP/IP ports. Open ports can provide a way for non-authorized users to gain access and control of the switch or permit a hacker to flood the switch with data to disrupt normal operation. The program was set to perform an intense scan. Here are the results of the scan:

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
Port	Protocol	State	Service	Version
22	tcp	open	ssh	Cisco SSH 1.25 (protocol 1.99)
123	udp	open	ntp	NTP v4
161	udp	open	snmp	SNMPv1 server (public)
500	udp	open	isakmp	

Figure 62: Zenmap Scan Results

In this test, 999 known ports were scanned and 4 ports were found open. SSH was enabled on the switch, thus TCP port 22 was open. NTP was also enabled and runs on UDP port 123. SNMP was also enabled on the switch and it runs on UDP port 161. UDP port 500 is used for IPSEC

communication using ISAKMP for VPN tunnels between switches. No other ports were enabled, such as port 80 for HTTP traffic or port 22 for Telnet which sends data in clear text.

5.2.2. W3af

W3af is a web application attack and audit framework which is used to identify and exploit web application vulnerabilities. It was used in the test environment to scan the web based management of the Cisco switches. It is part of the Kali Linux network vulnerability test suite. Here is a screenshot of the interface:

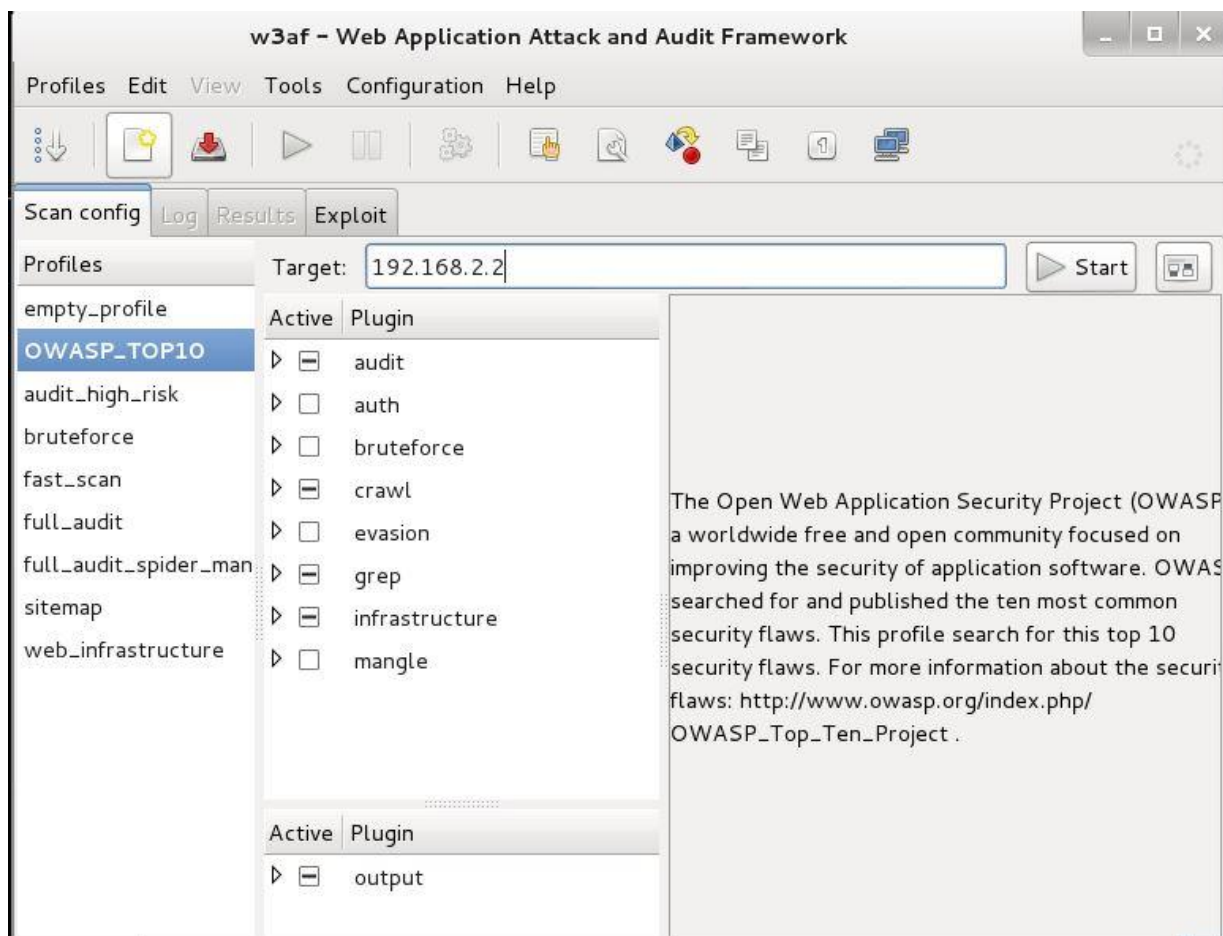


Figure 63: W3af Interface

To help further secure the Cisco switches, both HTTP and HTTPS were disabled on the device. The profile used for the test is identified in Figure 63. The expected result is that no vulnerabilities exist. Here is the result of the test:


```
error: [Errno 111] Connection refused ←
[Mon 02 Nov 2015 02:50:44 PM EST - debug] strategy.start() is raising exception "The remote web server is not
answering our HTTP requests, multiple errors have been found while trying to GET a response from the server.

In most cases this means that the configured target is incorrect, the port is closed, there is a firewall
blocking our packets or there is no HTTP daemon listening on that port.

Please verify your target configuration and try again."
[Mon 02 Nov 2015 02:50:44 PM EST - error]
**IMPORTANT** The following error was detected by w3af and couldn't be resolved:
The remote web server is not answering our HTTP requests, multiple errors have been found while trying to GET
a response from the server.

In most cases this means that the configured target is incorrect, the port is closed, there is a firewall
blocking our packets or there is no HTTP daemon listening on that port.

Please verify your target configuration and try again.

[Mon 02 Nov 2015 02:50:44 PM EST - information] Scan finished in 3 seconds.
[Mon 02 Nov 2015 02:50:44 PM EST - information] Stopping the core...
```

Figure 64: W3af Test Result

As indicated by the highlighted text, the connection request was denied and no HTTP session was established.

5.2.3. Cisco Torch

Cisco Torch is a mass scanning, fingerprinting, and exploitation tool included in the Kali Linux test suite. The main feature that differentiates Cisco Torch from similar tools is its extensive use of forking to launch multiple scanning processes on the background to scan more efficiently. It scans Cisco hosts running Telnet, SSH, Web, NTP and SNMP services and launches dictionary attacks against the services discovered. Here is result of the tests:

```
greg@kali:~$ cisco-torch -A 192.168.2.2 ←
Using config file torch.conf...
Loading include and plugin ...

#####
#   Cisco Torch Mass Scanner                               #
#   Becase we need it...                                   #
#   http://www.arhont.com/cisco-torch.pl                   #
#####

List of targets contains 1 host(s)
3170:  Checking 192.168.2.2 ...
HUH db not found, it should be in fingerprint.db
Skipping Telnet fingerprint
Cisco found by SSH banner SSH-1.99-Cisco-1.25

* Cisco by SNMP found *** ← Only found SNMP
*System Description: Cisco IOS Software, IES Software (IES-IPSERVICESK9-M), Vers
ion 15.0(2)EY3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Thu 14-Nov-13 13:52 by prod_rel_team

--->
- All scans done. Cisco Torch Mass Scanner -
---> Exiting.
greg@kali:~$
```

-A means run all comprehensive scans

Figure 65: Cisco Torch Test Result

5.3. Performance Criteria

The performance criteria are very simple: achieve a result of “PASS” for each test. In the event, all functional tests were passed. The network functioned as required when these security recommendations were implemented. No performance degradation was found and all devices performed according to specification.

6. Conclusion

The recommended use and configurations of Cisco switches, as described in this document, can help decrease the exposure to a successful attack on a PlantStruxure control room architecture.

As you apply these recommendations, be mindful that:

- No single feature by itself provides adequate security.
- The recommended features work in concert to more effectively mitigate the likelihood of a network disruption. Or, more simply stated, the whole of the recommended protections exceeds the sum of the individual parts.

7. Appendix

7.1. Glossary

The following table describes the acronyms and defines the specific terms used in this document.

Term	Description
ACL	<i>Access Control List</i> . There are many reasons to configure access lists; for example, you can use access lists to restrict updates to the routing table, or to provide traffic flow control, or to deny access to certain users or devices. One of the most fundamental reasons to configure access lists is to help secure the network.
ARP	<i>Address Resolution Protocol</i> is used to discover the mapping between a layer 3 (IP) and a layer 2 (MAC) address.
BGP	<i>Border Gateway Protocol</i> . A routing protocol that is used in complex networks. For example, the Internet uses BGP to route between service providers, who then provide internet access to their customers.
broadcast domain	A collection of devices that receive a broadcast sent on an Ethernet network. The broadcast domain ends at a router positioned in the network. If any device in a broadcast domain broadcasts information, that information is received by all devices in the domain. It is not received by devices connected through a router.
CCP	<i>Cisco Configuration Professional</i> . A Windows based tool to assist in the configuration of most Cisco switches and routers.
CLI	<i>Command Line Interface</i> . A CLI is used to configure Cisco devices.
CNA	<i>Cisco Network Assistant</i> is Cisco's GUI network configuration application for Cisco switches and routers.
frame	A series of bits containing data and control information, formatted for transmission from one node to another. It includes a header with a start frame delimiter, the source and destination addresses, control data, the message itself, and a trailer with error control data (called the frame check sequence). In the seven-layer OSI model of computer networking, frame strictly refers to a data unit at layer 2, the Data Link layer.
HSRP	<i>Hot Standby Router Protocol</i> is a Cisco proprietary protocol that uses two or more routers to act as a single virtual router. The protocol features an active router that controls the routing and one or more standby routers. If the active router ceases to perform the routing function, the standby with the highest priority takes over. The routers send "hello" packets to each other to verify if they are functioning properly.
IGMP Snooping	A traffic management mechanism in which a switch uses the <i>Internet Group Management Protocol</i> (IGMP) to listen to multicast traffic, maps which port needs the data, and then filters out the remaining ports.
interoperability	A property of a device that allows it to work with together with other devices within a network.
IP finger	A tool that matches an email address to the name of the person who owns the address.
layer 2	The hardware data link layer of the OSI model. The Data Link layer includes the Media Access Control (MAC) sub-layer.

Term	Description
layer 3	The network layer of the OSI model. The Network layer handles packet forwarding and network routing.
Native VLAN	The <i>virtual local area network</i> (VLAN) that is used to control traffic between the devices. Native VLAN traffic is not tagged and, as a general rule, is not used for data traffic.
OSPF	<i>Open Shortest Path First</i> . OSPF is a link state protocol that finds an optimal path in the network between two destinations. It advertises to the peer routers its health and capacity.
packet	A network packet is a formatted unit of data carried by a packet-switched network. A packet consists of two kinds of data: control information and user data. In the seven-layer OSI model of computer networking, packet strictly refers to a data unit at layer 3, the Network layer.
router	A device capable of filtering and forwarding packets based on network layer information. Whereas a bridge or switch may read only MAC layer addresses to filter, a router can read data such as IP addresses and route accordingly.
RSTP	<i>Rapid Spanning Tree Protocol</i> . An enhancement of the <i>Spanning Tree Protocol</i> (STP), RSTP is a specification defined as IEEE 802.1w. It provides a significantly faster (2 to 3 second) network convergence than its predecessor STP.
SSH	<i>Secure SHell</i> (SSH) is a protocol for securely accessing one computer from another. Despite the name, SSH allows you to run command line and graphical programs, transfer files, and even create secure virtual private networks over the Internet.
SNMP	<i>Simple Network Management Protocol</i> is a protocol of the application layer (layer 7) of the OSI model that provides the message format for communication between SNMP managers and agents.
SVI	<i>Switch Virtual Interface</i> . SVI provides layer 3 processing for packets from all switch ports associated with a VLAN.
trunk port	A port that is assigned to carry data traffic for multiple VLAN(s) by a specific switch.

Table 2: glossary

7.2. Bill of Material and Software

The following table summarizes all of the selected hardware:

Description	Reference	Firmware or software version	Function	Quantity
Cisco Switch	IE3000-8TC-E V03	15.0(2)EY	Ethernet L3 Switch	3
SE ConneXium Switch	TCSEM043F23F0		Ethernet L2 Switch	2
PC Workstations	HP Z210	Windows 7	SCADA, NTP, Syslog server	1
HP Laptop	ProBook 6470b	Windows 7	Engineering Workstation	1
Functional Unit 1	BMX-CPS3500		Power Supply	1
	BMX-P342020	2.6	CPU	1
	BMX-NOC0401	2.06	NOC	2
Remote Drop STB 1	STB NIP 2212	3.3	Ethernet Interface	2
	STB PDT 3100		Power Supply	2
	STB DDI 3610		Discrete IO module Input	2
	STB DDO 3410		Discrete IO module Output	2
Functional Unit 2	BMX-CPS3500		Power Supply	1
	BMX-P342020	2.6	CPU	1
	BMX-NOC0401	2.06	NOC	2
Remote Drop STB 2	STB NIP 2212	3.3	Ethernet Interface	7
	STB PDT 3100		Power Supply	7
	STB DDI 3610		Discrete IO module Input	7
	STB DDO 3410		Discrete IO module Output	7

Table 3: bill of material and software

7.3. Reference Documents

The following table is a list of documents you might want to refer to when more details are needed.

Source	Reference
Cisco	Guide to Hardening Cisco Devices
Cisco	Cisco IE-3000 System Configuration Guide
Cisco	http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html
Schneider Electric	STN – <i>How Can I Reduce Vulnerability to Cyber Attacks</i>
Schneider Electric	TVDA – <i>How can I Reduce Vulnerability to Cyber Attacks in the Control Room?</i>
Schneider Electric	TVDA – <i>How Can I Reduce Vulnerability to Cyber Attacks in the Functional Unit?</i>

Table 4: Reference documents

7.4. Security Functions outside the scope of this document

The following features were not tested as part of the preparation of this STN, but might be considered in designing your industrial automation network.

7.4.1. Reverse Path Forwarding

Reverse path forwarding (RPF) is a feature of a Cisco Layer 3 switch or router that limits potential malicious traffic on a network. This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. Unicast RPF works in one of three different modes: strict mode, loose mode, or virtual routing and forwarding (VRF) mode. Note that not all network devices support all three modes of operation. Unicast RPF in VRF mode is not covered in this document.

When administrators use unicast RPF in strict mode, the router accepts only packets received on the interface that the router would use to forward the return packet. Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

When administrators use unicast RPF in loose mode, the router accepts only packets whose source address appears in the routing table. Administrators can change this behavior using the **allow-default** option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to

the Null 0 interface will be dropped. An access list may also be specified that permits or denies certain source addresses in unicast RPF loose mode.⁶

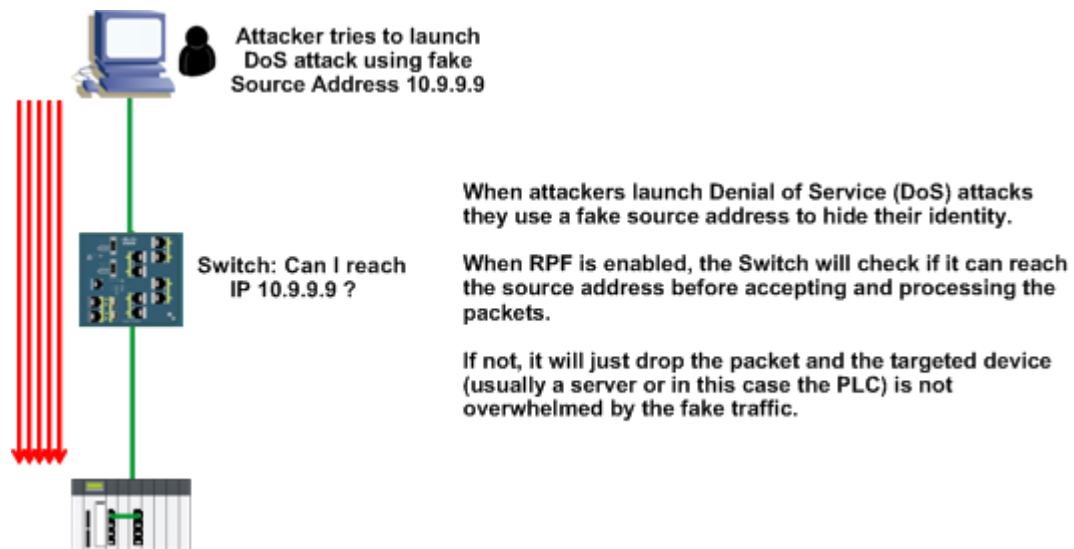


Figure 66: Reverse Path Forwarding

Reverse path forwarding is not part of the design and the implementation of the architecture that is used in the paper.

⁶ <http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html>

Altivar™, ConneXium™, Unity™, Vijeo™ are trademarks or registered trademarks of Schneider Electric. Other trademarks used herein are the property of their respective owners.

Schneider Electric Industries SAS
Head Office
35, rue Joseph Monier
92506 Rueil-Malmaison Cedex
FRANCE

Due to evolution of standards and equipment,
characteristics indicated in texts and images in this
document are binding only after confirmation by our
departments.

www.schneider-electric.com

Version 1.0 – 12 2015