Report Number: I33-010R-2004

# Cisco IOS Switch Security Configuration Guide

**Switch Security Guidance Activity**
**of the**
**Systems and Network Attack Center (SNAC)**

**Authors:**
**A. Borza**
**D. Duesterhaus**
**C. Grabczynski**
**J. Johnson**
**R. Kelly**
**T. Miller**


**Date:** **21 June 2004**
**Version:** **1.0**

**National Security Agency**
**9800 Savage Road, Suite 6704**
**Fort Meade, MD 20755-6704**
**snac.guides@nsa.gov**

# Table of Contents

# 1 Introduction

## 1.1 Overview

Switches direct and control much of the data flowing across computer networks. This guide provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented here, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

This guide was developed in response to numerous questions and requests for assistance received by the System and Network Attack Center (SNAC). The topics covered in the guide were selected on the basis of customer interest and on the SNAC's background in securing networks. A major goal for this guide is to improve the security of the switches used on Department of Defense operational networks.

This guide presents network security at Layer 2 (Data Link) of the Open Systems Interconnection Reference Model (OSI RM). A network hierarchy is introduced that explains the types of switches used in a computer network. Then vulnerabilities and corresponding countermeasures are described for the following topics: operating system; passwords; management port; network services; port security; system availability; Virtual Local Area Networks; Spanning Tree Protocol; access control lists; logging and debugging; and authentication, authorization and accounting. Advanced topics are identified for future work for this guide. A combined section of acronyms and glossary for terms used throughout this guide and a reference section are provided. Sample configuration files for two different models of Cisco switches are included that combine most of the countermeasures in this guide. Finally, a security checklist for Cisco switches summarizes the countermeasures.

## 1.2 Caveats

The guide focuses only on Cisco switches that use the Internetworking Operating System (IOS). Specifically, the authors of this guide used IOS version 12.1 for all of the examples. Note that IOS versions for switches are not necessarily identical to IOS versions for routers. Also, it deals only with Ethernet, Fast Ethernet and Gigabit Ethernet media technologies. The intended audience for this guide is those individuals who administer these switches in their organization's networks. The guide presumes that these administrators have at least a basic knowledge of these switches. The administrators should be familiar with configuring the switches with the command line interface, including using commands in the User Exec mode and in the Privileged Exec mode. The guide agrees with some settings on Cisco switches that are enabled or disabled by default; for completeness the guide presents these settings along with the other recommended settings. Note that some default settings will not appear normally in a listing of the switch configuration file. The authors also assume that the administrator provides physical security for each switch and allows only authorized personnel to access the switch.

Following the recommendations in this guide does not guarantee a secure environment or that the administrator will prevent all intrusions. However, the administrator can achieve reasonable security by establishing a good security policy, following the recommendations in this guide, staying current on the latest developments in the hacker and security communities, and maintaining and monitoring all systems with sound system administration practices. This includes awareness of application security issues that are not comprehensively addressed in this guide. Finally, use the following references as additional sources of guidance: Cisco's IOS switch command reference [2]; SAFE, Cisco's security blueprint for

enterprise networks [5]; Cisco's Product Security Advisories and Notices [4]; and NSA's Cisco Router Security Configuration Guide for more details on the principles for securing systems that are part of a network [11].

## 1.3 Acknowledgements

The authors would like to acknowledge the following personnel for their support to the development of this guide: Neal Ziring and James Houser for their technical reviews, and the office and division management within the System and Network Attack Center for their guidance and patience.

## 1.4 Feedback

This guide was created by a team of individuals in the System and Network Attack Center (SNAC), which is part of the NSA Information Assurance Directorate. The editor was Daniel Duesterhaus. Feedback about this guide may be directed to either of the following addresses.

Mail: SNAC (Attn: Daniel Duesterhaus)
National Security Agency
9800 Savage Road, Suite 6704
Fort Meade, MD 20755-6704

E-Mail: snac.guides@nsa.gov

## 1.5 Revision History

| Version | Date | Status |
|---|---|---|
| 0.9 | 16 Mar 2004 | First complete draft by SNAC team |
| 0.9a | 7 May 2004 | Draft updated from external review |
| 0.9b | 14 May 2004 | Minor updates to draft |
| 1.0 | 21 Jun 2004 | First public release |

## 1.6 Trademark Information



## 1.7 Warnings

This document is only a guide to recommended security countermeasures for Cisco IOS switches. It is not meant to replace well-designed policy or sound judgment. This guide does not address site-specific configuration issues. Care must be taken when implementing the countermeasures described in this guide. Ensure that all countermeasures chosen from this guide are thoroughly tested and reviewed prior to imposing them on an operational network.

# 2 Network Hierarchy

In a well-formed hierarchical network, there are three defined layers: access, distribution and core. In an enterprise network, each layer provides different functions. Because these layers are not always recognized by their traditional names, the names have been referred to as access or workgroup, distribution or policy, and core or backbone.

The access or workgroup layer connects users. Other functions of this layer are shared bandwidth, switched bandwidth, Media Access Control (MAC) address filtering, and micro segmentation. Local area network (LAN) switches exist most commonly in the access layer.

The distribution or policy layer performs the complex, processor-intensive calculations such as filtering, inter-Virtual LAN routing, multicast tree maintenance, broadcast and multicast domain definition, and address or area aggregation. This layer might also contain the local servers. Routers, LAN switches and switches with routing capability reside in the distribution layer.

The core or backbone layer is the backbone of the network. It is high-speed and concerned with quick traffic switching. It does not get involved in extensive packet manipulation. The central servers might also be attached to the high-speed backbone in the core. Switch routers, high-speed routers and occasionally LAN switches can be found in the core layer.

The following network diagram serves as a reference point for this guide. The two Cisco 3550 switches at the top of the diagram operate at the access layer. The two Cisco 6500 switches provide combined functionality for the distribution layer and the core layer. All of the recommended security countermeasures in this guide will refer to this diagram. This diagram represents just one recommended network architecture; there are several other architectures that are possible.

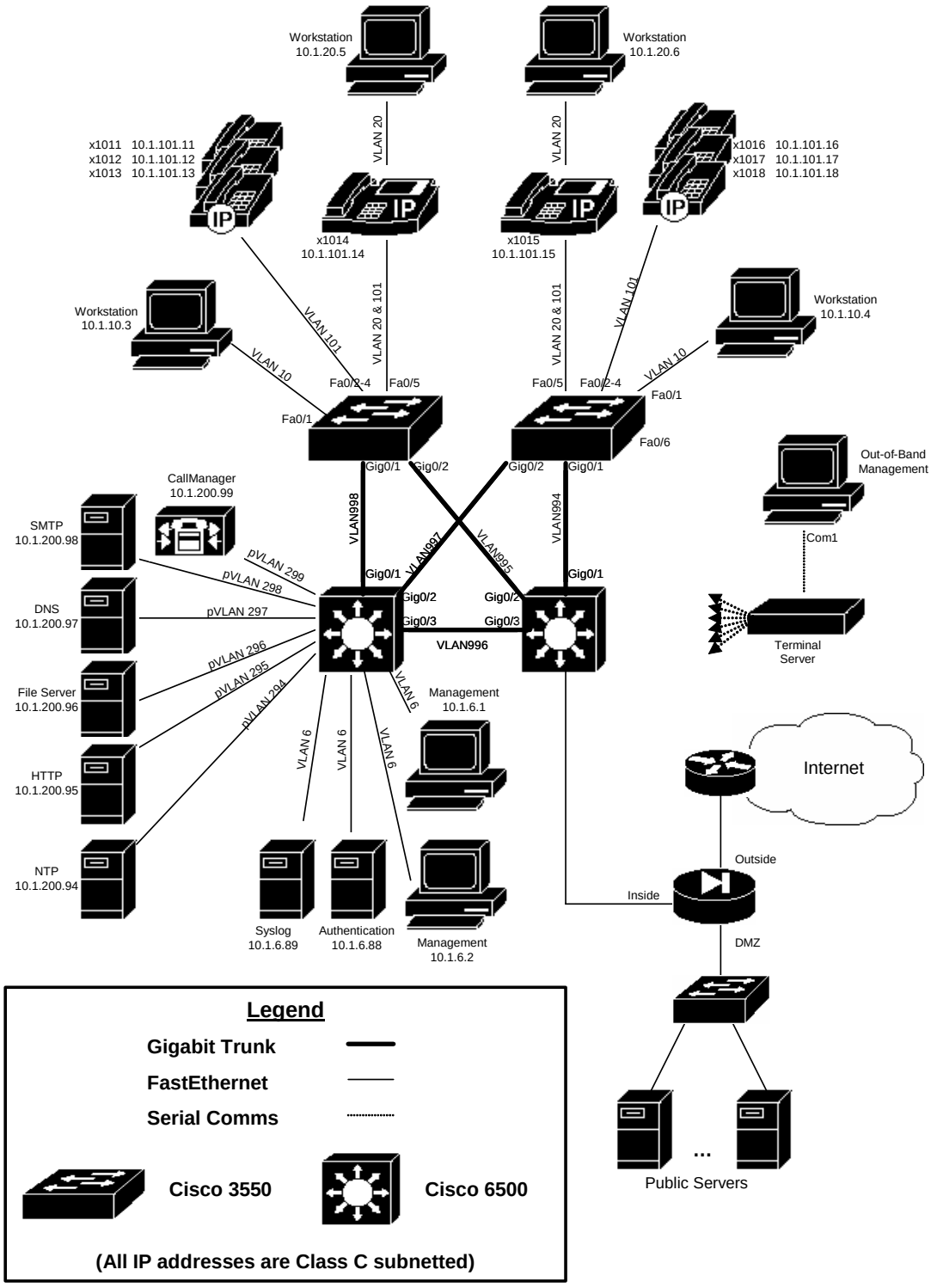


**Figure 1 - Example Network**

# 3 Operating System

## 3.1 Vulnerabilities

If an operating system on a switch is not kept current then the switch may be susceptible to information gathering and network attacks. Attackers find weaknesses in versions of an operating system over time. New security features are added to each new version of an operating system. Cisco's operating system, the Internetworking Operating System (IOS), is similar to other operating systems with respect to being susceptible to weaknesses.

## 3.2 Countermeasures

Install the latest stable version of the IOS on each Cisco switch. Cisco also refers to the IOS as the system image. An upgrade can be beneficial for security, but if done improperly it can leave a switch vulnerable. It is important to note that most IOS upgrades can only be accomplished by replacing the IOS running on the switch; there is no facility for amending or patching the installed IOS.

An IOS upgrade will impact the switch and possibly the network. For example, the switch performance may be affected due to downtime for the upgrade or to features that do not function properly after the upgrade. It is very important to read the release notes for a new IOS version carefully before installing it, to ensure that this version can fully support the switch functions needed on the network. Be prepared to back out of the upgrade if the switch performance or security has suffered. If possible, replace the switch with a spare switch to perform the upgrade offline without causing a long disruption in network connectivity. In networks with redundant switches, upgrade each redundant switch separately and confirm success before upgrading its counterpart.

### 3.2.1 Obtaining IOS Versions

Cisco makes new versions of IOS available through a variety of purchase and maintenance mechanisms. The logistics of purchasing IOS versions is beyond the scope of this document. If the administrator has a maintenance agreement with Cisco, then the administrator can download versions from the Software Center on Cisco's Internet web site. After downloading the version, check the length of the version. During the selection of the IOS version and the download sequence at Cisco's web site, the administrator will be given the length of the version in bytes. Print the summary web page, which will include the length and the MD5 checksum, for the desired IOS version. Also, compare the MD5 checksum for the downloaded IOS with the MD5 checksum on the download page. If the checksums do not match, then discard the file and download it again.

To determine which IOS version is needed for a switch, the administrator should consider the following factors: feature availability, version status, cost, amount of required memory and bug history. For more information about IOS versions, refer to the following web pages on Cisco's Internet web site.

http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html
http://www.cisco.com/warp/public/732/releases/packaging/

### 3.2.2 Before Installing New Version

Follow the checklist below before installing a new version of the IOS on each switch.

1. Verify amount of memory.
   Cisco switches have two fundamental kinds of memory: Random Access Memory (RAM) and Flash. Every Cisco IOS version has minimum memory requirements. Do not install a new version unless the switch to be upgraded satisfies the memory requirements for both RAM and Flash. (Often, a major new version will require more memory because Cisco typically sells switches with just enough memory to run the version pre-installed at purchase.) Use the command **`show version`** to check the amount of memory that the switch has and to determine the current version running on a switch as shown in the example below.

   ```
   Switch> show version
   Cisco Internetwork Operating System Software
   IOS (tm) c6sup2_rp Software (c6sup2_rp-PSV-M), Version 12.1(13)E6,
   EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

   System image file is "sup-bootflash:c6sup22-psv-mz.121-13.E6.bin"

   cisco Catalyst 6000 (R7000) processor with 112640K/18432K bytes of
   memory.  381K bytes of non-volatile configuration memory.

   32768K bytes of Flash internal SIMM (Sector size 512K).
   Configuration register is 0x2102
   ```

   The underlined portions of the example are the IOS version, the switch model, the RAM size, and the flash memory size, respectively. To compute the total RAM on the switch, simply add the two parts of the RAM size rating. The example above shows the switch having 128MB of RAM. It is important to know the switch model and memory sizes before attempting to obtain a new IOS version.

2. Check file transfer configuration on switch.
   Loading new IOS versions for a switch involves using either Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP) (available only in IOS version 12.0 or later). Make sure that the TFTP or FTP server is correctly set up for both upload and download, including setting the necessary permissions (e.g., usually world-read and world-write). Also, make sure that the switch has network access to the server. Copy the new version into the server's download directory. If available, use FTP for performing the upgrade because FTP provides authentication while TFTP does not. Although TFTP is supported by all IOS versions, it is not a secure service and normally should not be running on any system in a secure network. If FTP is not available, then enable TFTP only for the upgrade sequence and then disable it again. If possible, connect the TFTP server to the switch through a separate network connection, not through the operational network. This may also be possible using a dedicated Virtual Local Area Network.

3. Schedule switch downtime.
   Installing an upgrade to the switch imposes a downtime. If the upgrade goes well, then the downtime may be 30 minutes or less. However, if the upgrade does not go well and the administrator has to back out, then the downtime could be hours. Schedule the upgrade ahead of time, and inform the user community as needed.

4. Read the following process for installing new versions.
   Review the entire process before beginning the installation of the IOS. Be familiar with all the IOS commands involved.

### 3.2.3 Install Process

This section presents a suggested process for installing new versions of the Cisco IOS. This process is conservative. Still, by following the process the administrator can avoid mishaps and can restore the previous IOS version if necessary. The process involves steps broken down into the following three phases: backup, load, and test. The backup phase, steps 1-3, involves copying the running IOS version and configuration onto the FTP server or the TFTP server for safekeeping. The install phase, step 4, involves loading the new IOS version. The test phase, step 5, involves checking that the new version is running the old configuration successfully. Each step is described below, including example commands where appropriate.

1. Log into the switch console.
   It is best to perform installation of new versions from the system console rather than from a network login. The console will show important status messages in the later steps of the installation that would not be visible otherwise. Elevate to privileged user.

2. Back up the current IOS version.
   Copy the current IOS version using one of the appropriate examples shown below.

   Using FTP:

   ```
   Switch# archive upload-sw ftp://netwadmin:G00dpa55@10.1.6.1/IOS-
         images/c3550-i9k212q3-tar.121-11.EA1a.tar
   ```

   where **netwadmin** is the username, **G00dpa55** is the password, **10.1.6.1** is the FTP server, **IOS-images** is the directory on the FTP server, and **c3550-i9k212q3-tar.121-11.EA1a.tar** is the image file

   Using TFTP:

   ```
   Switch# copy flash tftp
   ```

   The switch will prompt for the Internet Protocol (IP) address of the TFTP server.

   If this step fails, do not proceed, abandon the upgrade and check the server configuration before trying again.

3. Back up the current running configuration.
   Copy the current running configuration using one of the appropriate examples shown below.

   Using FTP:

   ```
   Switch# copy system:running-config
         ftp://netwadmin:G00dpa55@10.1.6.1/configs/switch-confg
   ```

   where **netwadmin** is the username, **G00dpa55** is the password, **10.1.6.1** is the FTP server, **configs** is the directory on the FTP server, and **switch-confg** is the configuration file

   Using TFTP:

   ```
   Switch# copy running-config tftp
   ```

   The switch will prompt for the IP address of the TFTP server.

   If this step fails, do not proceed, abandon the upgrade and check the server configuration before trying again.

4. Load the new IOS version.
   Copy the new version using one of the appropriate examples shown below. On most Cisco switches, the flash will be erased automatically during this step; if asked whether to erase the flash, answer yes.

   Using FTP:

   ```
   Switch# archive download-sw /imageonly /overwrite
         ftp://netwadmin:G00dpa55@10.1.6.1/IOS-images/c3550-i9k212q3-
         tar.121-13.EA1a.tar
   ```

   where **netwadmin** is the username, **G00dpa55** is the password, **10.1.6.1** is the FTP server, **IOS-images** is the directory on the FTP server, and **c3550-i9k212q3-tar.121-13.EA1a.tar** is the image file

   Using TFTP:

   ```
   Switch# copy tftp flash
   ```

   The switch will prompt for the IP address of the TFTP server.

   (On some Cisco switches, it is possible to store several IOS versions in flash memory and select which one to run. Because only some Cisco switches have sufficient flash memory to hold multiple IOS versions, that scenario is not covered here.)

   If this copy succeeds, then the switch may automatically reboot; if it does not, then reboot it manually using the command **reload**. If performing the new install over a network connection, the connection will be broken at this point.

   ```
   Switch# reload
   Proceed with reload? [confirm]  y
   ```

5. Confirm the new IOS version and boot image.
   When using the console, watch the boot messages on the switch to confirm the new IOS version and boot image. When using a network connection, re-establish the connection at this point. Check the IOS version and boot image with the command **`show version`**. Then, confirm the configuration status with the command **`show running-config`**. Check the status of the interfaces with the command **`show ip interface brief`**.

Depending on network speed and switch model, this procedure may take about 5-20 minutes. Note that, for some older Cisco switch models, additional hardware-specific steps may be needed. Consult the release notes for the particular switch for details.

### 3.2.4 Recovery from Problem Install

If functional testing reveals a problem with the switch after an upgrade, the administrator may need to return to the previous IOS version. Simply follow the procedure described above, starting with step 3. In step 3, use a different name for the running configuration than the one used during the upgrade procedure. In step 4, load the backup copy of the old IOS version. Note that if the administrator has upgraded from one IOS major version to another (e.g., from 11.2 to 12.0), the stored configuration might not work correctly when the administrator returns to the previous version. In that case, restore the backup copy of the configuration saved during the upgrade procedure step 3.

### 3.2.5 Additional Security Concerns

First, using a TFTP server during the installation procedure described previously is a concern because TFTP provides no security. Thus, it is critical that the administrator protects the TFTP transaction and the server from potential attackers. There are several approaches to doing this, but the simplest is to ensure that the TFTP traffic does not traverse hostile networks. Also, do not leave the TFTP service enabled on the server; always disable it immediately after finishing the installation procedure. Second, whenever making any kind of backup copy of a switch configuration, the administrator may be exposing the encrypted passwords to disclosure. The simplest approach to mitigating this risk is to change the **`enable secret`** immediately after installation. Third, many default settings differ between various IOS versions. Some of these settings can affect the switch's security. Also, some newer versions offer services not present in older versions. Therefore, it is important to read and follow the release notes for a new IOS version carefully.

# 4 Passwords

## 4.1 Vulnerabilities

Cisco IOS switches have two levels of access by default: User (Level 1) and Privileged (Level 15). The User level is typically accessed via Telnet or SSH connections to a switch or via the console line on the switch. The Privileged level is typically accessed after the User level is established. Each level is usually configured with a password. The Privileged level can be configured with either an "enable" password or an "enable secret" password. The "enable secret" password is protected more securely, using a function based on MD5 hashes, than an "enable" password. Specific vulnerabilities associated with these passwords include the following.

- A Cisco switch shows the passwords in plaintext by default for the following settings in the configuration file: the "enable" password, the username password, the console line and the virtual terminal lines. If an attacker can collect the configuration file for the switch from the network using a network analyzer, then he can use these passwords to access this system.
- If the "enable secret" password on a Cisco switch is not set or is a weak password, then an attacker may be able to obtain Privileged level access to retrieve or to change information on the switch. Also, setting the same password for the "enable secret" passwords on multiple switches provides a single point of failure because one compromised switch will endanger other switches. Finally, using the same password for both the "enable secret" and other settings on a switch allows for potential compromise because the password for certain settings (e.g., telnet) may be in plaintext and can be collected on a network using a network analyzer. The attacker who can collect passwords going to a switch may be able to gain Privileged level access at a later time.

## 4.2 Countermeasures

The following countermeasures will mitigate the vulnerabilities associated with passwords on Cisco IOS switches. Countermeasures are described for passwords for the console line, the virtual terminal lines and username in the Management Port and the Network Services sections of this guide.

- Basic encryption can be provided to the passwords for the following settings in the configuration file: the "enable" password, the username password, the console line and the virtual terminal lines. Use the following command to provide this basic encryption on each Cisco IOS switch.

  ```
  Switch(config)# service password-encryption
  ```

- Configure an "enable secret" password on each Cisco switch. Do not configure any "enable" passwords on any Cisco switch, unless there is a need for establishing more levels of access beyond the default levels. Use the following guidelines for creating the password: be at least eight characters long; not based on words; and include at least one character from each of the sets of letters, numbers and special characters (e.g., ,./<>;':"[]\{}|~!@#$%^&*()_+`-= ). Also, Cisco recommends that the first character of the password not be a number. Change passwords at least once every 90 days. Use a unique password for the "enable secret" password on each switch. Also, use a different password for the "enable secret" password than for the passwords used for the other settings (e.g., telnet) on the same switch. The following example shows the command to use to configure an "enable secret" password (e.g., **r3all7-G00D-psw6**).

  ```
  Switch(config)# enable secret r3all7-G00D-psw6
  ```

# 5 Management Port

## 5.1 Vulnerabilities

A Cisco IOS switch has a management port, the console line (line con 0), that provides direct access to the switch for administration. If the management port on the switch has settings that are too permissive, then the switch is susceptible to attacks. Specific vulnerabilities associated with the management port include the following.

- A switch with a management port using a default user account allows an attacker to attempt to make connections using one or more of the well-known default user accounts (e.g., administrator, root, security).
- If a switch has a management port set with no password, with a default password or with a weak password, then an attacker may be able to guess the password or crack it (e.g., via dictionary attacks) and retrieve or change information on the switch. Also, setting the same password for the management port on multiple switches provides a single point of failure. The attacker who compromises one switch will be able to compromise other switches. Finally, using the same password for both the management port and other settings on a switch allows for potential compromise because the password for certain settings (e.g., telnet) may be in plaintext and can be collected on a network using a network analyzer. The attacker who can collect telnet passwords from network traffic going to a switch may be able to access the switch's management port at a later time.
- If the connections to a management port on a switch do not have a timeout period set or have a large timeout period (greater than 9 minutes), then the connections will be more available for an attacker to hijack them.
- A banner gives notice to anyone who connects to a switch that it is for authorized use only and any use of it will be monitored. Courts have dismissed cases against those who have attacked systems without banners. Thus, no banner on a switch may lead to legal or liability problems.

## 5.2 Countermeasures

The most secure method to administer a switch is out-of-band management. This method does not mix management traffic with operational traffic and does not consume operational bandwidth. Out-of-band management uses dedicated systems and communication pathways. Figure 1 shows a serial line terminal server and separate management host for out-of-band console port access to all switches. This solution is sufficient for many management functions. However, network-based, out-of-band access would be preferable for certain functions (e.g., IOS upgrades). This access involves using a Virtual Local Area Network (VLAN) and is described in the countermeasures for VLAN 1 in the Virtual Local Area Networks section of this guide.

The following countermeasures will mitigate the vulnerabilities to the console line available on each switch.

- Set up a unique account for each administrator for access to the console line. The following commands present an example that creates an account (e.g., **ljones**) with a privilege level (e.g., **0**) and that sets the default privilege level (e.g., **0**) for the console line. Privilege level **0** is the lowest level on Cisco switches and allows a very small set of commands. The administrator can go to a higher level (e.g., **15**) from level **0** using the **enable** command. Also, this account can be used for access to the virtual terminal lines.

```
Switch(config)# username ljones privilege 0
Switch(config)# line con 0
Switch(config-line)# privilege level 0
```

- Use the following guidelines for creating the password: be at least eight characters long; not based on words; and include at least one character from each of the sets of letters, numbers and special characters (e.g., ,./<>;':"[]\{}|~!@#$%^&*()_+`-= ). Also, Cisco recommends that the first character of the password not be a number. Change passwords at least once every 90 days. Use a unique password for the console line on each switch. Do not use the same password for the console line and for other services (e.g., telnet) on the same switch. The following commands present an example that sets an account (e.g., **ljones**) with a password (e.g., **g00d-P5WD**) that will be MD5-encrypted and that enables local account checking at login at the console line.

```
Switch(config)# username ljones secret g00d-P5WD
Switch(config)# line con 0
Switch(config-line)# login local
```

  For more elaborate authentication services, as well as other related capabilities, to configure on the console line refer to the Authentication, Authorization and Accouting section of this guide.

- Set the exec-timeout period to 9 minutes or less to disconnect idle connections to the console line on each switch. Do not set the timeout period to zero because on Cisco switches that will disable the timeout. The following example sets the timeout period for the console line to 9 minutes and 0 seconds.

```
Switch(config)# line con 0
Switch(config-line)# exec-timeout 9 0
```

- Create a legal banner for the login process into the console line for each switch. The following example shows how to do this with the **banner motd** command using the **'$'** as the delimiting character. The administrator should have the banner approved by the general counsel of the administrator's organization. Also, this banner will appear when connections are made to the virtual terminal lines.

```
Switch(config)# banner motd $

                    NOTICE TO USERS

This is an official computer system and is the property of the
ORGANIZATION.  It is for authorized users only.  Unauthorized users
are prohibited.  Users (authorized or unauthorized) have no explicit
or implicit expectation of privacy.  Any or all uses of this system
may be subject to one or more of the following actions:  interception,
monitoring, recording, auditing, inspection and disclosing to security
personnel and law enforcement personnel, as well as authorized
officials of other agencies, both domestic and foreign.  By using this
system, the user consents to these actions.  Unauthorized or improper
use of this system may result in administrative disciplinary action
and civil and criminal penalties.  By accessing this system you
indicate your awareness of and consent to these terms and conditions
of use.  Discontinue access immediately if you do not agree to the
conditions stated in this notice.

$
```

# 6 Network Services

## 6.1 Vulnerabilities

Cisco IOS switches can have a number of network services enabled. Many of these services are typically not necessary for a switch's normal operation; however if these services are enabled then the switch may be susceptible to information gathering or to network attacks. The characteristics or the poor configuration of the network services on a switch can lead to compromise. Most of these services use one of the following transport mechanisms at Layer 4 of the OSI RM: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Specific vulnerabilities associated with network services include the following.

- Connections to many services on a switch are not encrypted, so an attacker may be able to collect network traffic related to these services using a network analyzer. The traffic may contain usernames, passwords or other configuration information related to the switch.
- A switch with a network service using a default user account allows an attacker to attempt to make connections using one or more of the well-known default user accounts (e.g., administrator, root, security).
- If a switch has a network service set with no password, with a default password or with a weak password, then an attacker may be able to guess the password or crack it (e.g., via dictionary attacks) and retrieve or change information on the switch. Also, setting the same password for the network service on multiple switches provides a single point of failure. The attacker who compromises one switch will be able to compromise other switches.
- Broad access to the network service on a switch makes the switch vulnerable to attack. Broad access means that all systems or a large number of systems can connect to the switch.
- If the connections to a network service on a system do not have a timeout period set or have a large timeout period (e.g., greater than 9 minutes), then the connections will be more available for an attacker to hijack them.

## 6.2 Countermeasures

If possible, instead of using a network service (e.g., telnet) to perform in-band management of a switch, use out-of-band management (e.g., via the console port) for each switch. Out-of-band management reduces the exposure of configuration information and passwords better than in-band management. Refer to the Management Port section for more details on out-of-band management.

The following countermeasures will mitigate the vulnerabilities of the network services enabled on the switch. The countermeasures are categorized as the following: unnecessary network services and potentially necessary network services.

### 6.2.1 Unnecessary Network Services

If possible, disable each unnecessary network service on each switch. The following commands will disable services of concern. In some cases, the commands affect the switch globally, while in other cases the commands affect only a single interface. Many of the following recommended configuration settings are the same for different sets of interfaces (e.g., FastEthernet, GigabitEthernet) on the switch. To assist in applying these settings across a set of interfaces, use the **range** command for specifying the set of interfaces to configure.

Below is an example for the set of interfaces that includes GigabitEthernet 6/1 through 6/3.

```
Switch(config)# interface range gigabitethernet 6/1 – 3
```

#### 6.2.1.1 *TCP and UDP Small Servers - TCP/UDP Ports 7, 9, 13, 19*

Cisco provides support for "small servers" (e.g., echo, discard, daytime and chargen). Two of these servers, echo and chargen, can be used in denial-of-service attacks against one or more switches. These services can be disabled using the following commands.

```
Switch(config)# no service tcp-small-servers
Switch(config)# no service udp-small-servers
```

#### 6.2.1.2 *Bootp Server - UDP Port 67*

A Cisco switch can act as a bootp server to distribute system images to other Cisco systems. Unless this is an operational requirement, it is best to disable this service with the following command to minimize unauthorized access to the switch's system image.

```
Switch(config)# no ip bootp server
```

#### 6.2.1.3 *Finger - TCP Port 79*

Cisco switches support the finger service, which can provide information about users currently logged onto the switch. Either of the following commands will disable finger service. The first command will replace the second command in future versions of IOS.

```
Switch(config)# no ip finger
Switch(config)# no service finger
```

#### 6.2.1.4 *Configuration Autoload*

A Cisco switch can obtain its configuration from a network server via a few methods. These methods are not recommended because configuration information is passed in cleartext during the boot process and can be collected by unauthorized users. Use the following commands to disable these methods.

```
Switch(config)# no service config
Switch(config)# no boot host
Switch(config)# no boot network
Switch(config)# no boot system
```

#### 6.2.1.5 *Packet Assembler/Disassembler (PAD)*

PAD enables X.25 connections between network systems. Unless a network requires this capability the PAD service should be disabled with the following command.

```
Switch(config)# no service pad
```

#### 6.2.1.6 *Address Resolution Protocol (ARP)*

Normally, ARP messages are confined to a single broadcast domain, but a switch can proxy ARP messages from one domain to another. Unless a switch is required to be an intermediary for ARP requests, this feature should be disabled with the following commands on each interface where it is not required.

```
Switch(config-if)# no ip proxy-arp
```

#### 6.2.1.7 *Internet Control Message Protocol (ICMP) Messages*

A Cisco switch can generate automatically three types of ICMP messages: Host Unreachable, Redirect and Mask Reply. The Mask Reply message provides the subnet mask for a particular network to the requestor. An attacker can use these messages to aid in mapping a network. Disabling these messages with the following commands is recommended for each interface and for the Null 0 interface.

```
Switch(config-if)# no ip unreachables
Switch(config-if)# no ip redirects
Switch(config-if)# no ip mask-reply
```

The Null 0 interface deserves particular attention. This interface is a packet sink. It is sometimes utilized in denial-of-service attack prevention and all blocked packets are forwarded to this interface. It will generate Host Unreachable messages that could flood the network unless the facility is disabled. Attackers might also be able to use these messages to determine access-control list configuration by identifying blocked packets.

Directed broadcasts allow broadcast messages initiated from different broadcast domains than are locally attached to the switch. For example, attackers have used ICMP directed broadcasts for this purpose. It is recommended that this broadcast capability be turned off, using the following command on each interface.

```
Switch(config-if)# no ip directed-broadcast
```

### 6.2.2 Potentially Necessary Network Services

Certain network services may be necessary for the administration of a switch. If in-band management or a specific network service is necessary, then consider the following subsections for configuring network services more securely.

Set up a unique account for each administrator for access to any necessary network service. The following commands present an example that creates an account (e.g., **`ljones`**) with a privilege level (e.g., **`0`**). This account is local to the switch only. Privilege level **`0`** is the lowest level on Cisco switches and allows a very small set of commands. The administrator can go to a higher level (e.g., **`15`**) from level **`0`** using the **`enable`** command.

```
Switch(config)# username ljones privilege 0
Switch(config)# username ljones secret g00d-P5WD
```

For more elaborate authentication services, as well as other related capabilities, for the network services refer to the Authentication, Authorization and Accouting (AAA) section of this guide.

#### 6.2.2.1 *Domain Name System (DNS) - TCP Port 53 and UDP Port 53*

To specify a DNS server for name resolution, use the **`ip name-server`** command. This command can be used to set up to six DNS servers. The following example sets the IP address of **`10.1.200.97`** as the DNS server.

```
Switch(config)# ip name-server 10.1.200.97
```

To enable the DNS-based hostname-to-address translation, use the **`ip domain-lookup`** command. This command allows DNS broadcast queries from the switch to be resolved by a DNS server.

```
Switch(config)# ip domain-lookup
```

In some cases, the administrator may not want this DNS query capability. For example, if the administrator types a command incorrectly, then the switch may attempt to resolve the mistyped string to an IP address. This attribute can cause undesirable delay. Thus, use the following command to disable the capability if necessary.

```
Switch(config)# no ip domain-lookup
```

To specify a default domain name to complete unqualified hostnames, use the **`ip domain-name`** command. The following example sets the domain name to **`test.lab`** using this command.

```
Switch(config)# ip domain-name test.lab
```

#### 6.2.2.2 *Secure Shell (SSH) - TCP Port 22*

If remote access to a switch is necessary, then consider using SSH instead of telnet. SSH provides encrypted connections remotely. However, only IOS versions that include encryption support SSH. Also, to include SSH capability the switch may need to have its IOS updated.

Before using SSH on the switch, the administrator must configure the switch with the following commands: **`hostname`**, **`ip domain-name`**, and **`crypto key generate rsa`**. The following example sets the hostname to **`Switch`**.

```
Switch(config)# hostname Switch
```

Refer to the previous subsection on DNS for an example using the **`ip domain-name`** command.

The **`crypto key generate rsa`** command depends on the **`hostname`** and **`ip domain-name`** commands. This crypto command generates a Rivest, Shamir, Adleman (RSA) key pair, which includes one public RSA key and one private RSA key.

The following example shows this crypto command, including the two parameters, the name for the keys (e.g., **switch.test.lab**) and the size of the key modulus (e.g., **1024**), that are prompted for.

```
Switch(config)# crypto key generate rsa
The name for the keys will be: switch.test.lab

Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys.  Choosing a key modulus greater than 512 may
take a few minutes.
How many bits in the modulus[512]? 1024
Generating RSA keys.... [OK].
```

To restrict SSH access to the switch, configure an extended access-list (e.g., **101**) that allows only the administrators' systems to make these connections and apply this access-list to the virtual terminal lines. Allow only SSH connections to these lines by using the **transport input ssh** command. Set the privilege level to 0, and set the **exec-timeout** period to 9 minutes and 0 seconds to disconnect idle connections to these lines. Finally, use the **login local** command to enable local account checking at login that will prompt for a username and a password.

The following commands show the example configuration for SSH on the virtual terminal lines.

```
Switch(config)# no access-list 101
Switch(config)# access-list 101 remark Permit SSH access from
      administrators' systems
Switch(config)# access-list 101 permit tcp host 10.1.6.1 any eq 22 log
Switch(config)# access-list 101 permit tcp host 10.1.6.2 any eq 22 log
Switch(config)# access-list 101 deny ip any any log
Switch(config)# line vty 0 4
Switch(config-line)# access-class 101 in
Switch(config-line)# transport input ssh
Switch(config-line)# privilege level 0
Switch(config-line)# exec-timeout 9 0
Switch(config-line)# login local
```

The **login local** command cannot be used with AAA. Instead, use the **login authentication** command. Refer to the AAA section of this guide for more details.

#### 6.2.2.3 *Telnet Server - TCP Port 23*

If the administrator cannot upgrade the switch to an IOS version with SSH, then restrict telnet access to the switch. Configure an extended access-list (e.g., **102**) that allows only the administrators' systems to make these connections and apply this access-list to the virtual terminal lines. Allow only telnet connections to these lines by using the **transport input telnet** command. Set the privilege level to 0, and set the **exec-timeout** period to 9 minutes and 0 seconds to disconnect idle connections to these lines. Finally, use the **login local** command to enable local account checking at login that will prompt for a username and a password.

The following commands show the example configuration for telnet on the virtual terminal lines.

```
Switch(config)# no access-list 102
Switch(config)# access-list 102 remark Permit telnet access from
      administrators' systems
Switch(config)# access-list 102 permit tcp host 10.1.6.1 any eq 23 log
Switch(config)# access-list 102 permit tcp host 10.1.6.2 any eq 23 log
Switch(config)# access-list 102 deny ip any any log
Switch(config)# line vty 0 4
Switch(config-line)# access-class 102 in
Switch(config-line)# transport input telnet
Switch(config-line)# privilege level 0
Switch(config-line)# exec-timeout 9 0
Switch(config-line)# login local
```

The **login local** command cannot be used with AAA. Instead, use the **login authentication** command. Refer to the AAA section of this guide for more details.

#### 6.2.2.4 *Hyper Text Transfer Protocol (HTTP) - TCP Port 80*

An HTTP server is included in IOS to allow remote administration of the switch through a web interface. If web-based administration of the switch is not necessary, then disable the HTTP server using the following command.

```
Switch(config)# no ip http server
```

If web-based administration of the switch is necessary, then restrict HTTP access to the switch. Configure a standard access-list (e.g., **11**) that allows only the administrators' systems to make these connections and apply this access-list to the HTTP service on the switch. Finally, use the **ip http authentication local** command to enable local account checking at login that will prompt for a username and a password.

```
Switch(config)# no access-list 11
Switch(config)# access-list 11 remark Permit HTTP access from
      administrators' systems
Switch(config)# access-list 11 permit host 10.1.6.1 log
Switch(config)# access-list 11 permit host 10.1.6.2 log
Switch(config)# access-list 11 deny any log
Switch(config)# ip http server
Switch(config)# ip http access-class 11
Switch(config)# ip http authentication local
```

Note that the web browser used for administration will cache important information (e.g., passwords). Make sure that the cache is emptied periodically.

#### 6.2.2.5 *Simple Network Management Protocol (SNMP) - UDP Ports 161, 162*

SNMP is a service used to perform network management functions using a data structure called a Management Information Base (MIB). Unfortunately, SNMP version 1 is widely implemented but not very secure, using only clear-text community strings for access to information on the switch, including its configuration file.

If SNMP is not being used, then executing the following commands will disable the service.

```
Switch(config)# no snmp-server community
Switch(config)# no snmp-server enable traps
Switch(config)# no snmp-server system-shutdown
Switch(config)# no snmp-server
```

If SNMP is required for a switch, then configure the switch for SNMP version 3. This version is more secure than SNMP version 1 because version 3 can use cryptographic hashes for authentication to protect the community string. The above commands for disabling SNMP are recommended for use before deploying SNMP version 3 to remove any possible default community strings.

The following commands show an example User Security Model for SNMP version 3 for the switch. The model begins with creating a standard access-list (e.g., **12**) that allows only those systems that manage the switch. Next, define a group (e.g., **admins**) with read and write MIB views (e.g., **adminview**). Then each user (e.g., **root**) is added to the group with a password (e.g., **5ecret-5TR1N**) that can be hashed (e.g., using **md5**) before being sent across the network. Also, the standard access-list (e.g., **12**) is applied to the user. Finally, the MIB view (e.g., **adminview**) is defined by one or more statements to include or to exclude portions of the MIB. The MIB view in the following example gives access to the Internet branch of the MIB except the branches that display IP addresses and IP routing information.

```
Switch(config)# no access-list 12
Switch(config)# access-list 12 permit 10.1.6.1
Switch(config)# access-list 12 permit 10.1.6.2
Switch(config)# snmp-server group admins v3 auth read adminview write
      adminview
Switch(config)# snmp-server user root admins v3 auth md5 5ecret-5TR1N
      access 12
Switch(config)# snmp-server view adminview internet included
Switch(config)# snmp-server view adminview ipAddrEntry excluded
Switch(config)# snmp-server view adminview ipRouteEntry excluded
```

If SNMP is required for a switch and only SNMP version 1 is available, then the following commands show an example of how to configure the switch with a community string (e.g., **g00d-5tr1n9**) that has read-only permissions and a standard access-list (e.g., **12**) applied to it.

```
Switch(config)# no access-list 12
Switch(config)# access-list 12 permit 10.1.6.1
Switch(config)# access-list 12 permit 10.1.6.2
Switch(config)# snmp-server community g00d-5tr1n9 ro 12
```

In addition to the configuration of the SNMP service, SNMP Trap information can be sent to the systems that manage the switches. The following commands show an example of this configuration.

```
Switch(config)# snmp-server host 10.1.6.1 traps g00d-5tr1n9-2
Switch(config)# snmp-server host 10.1.6.2 traps g00d-5tr1n9-2
Switch(config)# snmp-server trap-source Loopback0
Switch(config)# snmp-server enable traps
```

#### 6.2.2.6 *Cisco Discovery Protocol (CDP)*

CDP provides a capability for sharing system information between Cisco routers, switches and other products. Some of this information includes VLAN Trunking Protocol (VTP) domain name, native VLAN and duplex. If this information is not required for operational needs, then it should be disabled globally and disabled on each interface (e.g., physical, Virtual LAN {VLAN}). To disable CDP globally on a switch, use the **no cdp run** command. To disable CDP on an interface on a switch, use the **no cdp enable** command. The following commands provide an example, including how to disable advertising CDP version 2 on a switch.

```
Switch(config)# no cdp run
Switch(config)# no cdp advertise-v2
Switch(config)# interface range fastethernet 0/1 - 24
Switch(config-if)# no cdp enable
```

If CDP is necessary, then it needs to be enabled globally and enabled only on interfaces where it is necessary. The following commands provide an example of disabling CDP on one interface while enabling CDP on another interface.

```
Switch(config)# cdp run
Switch(config)# interface VLAN10
Switch(config-if)# no cdp enable
Switch(config)# interface VLAN101
Switch(config-if)# cdp enable
```


A voice network may need CDP to perform properly, depending on the voice network design and the security policy. If IP phones will be deployed using Auto Discovery or Dynamic Host Configuration Protocol (DHCP), then CDP will need to be enabled globally and disabled on all ports not connected to an IP phone. However, these services provide potential avenues for information gathering and attacks. Auto Discovery and DHCP options are not recommended for secure Voice over IP (VoIP) implementations.

# 7 Port Security

## 7.1 Vulnerabilities

Layer 2 interfaces on a Cisco switch are referred to as ports. A switch that does not provide port security allows an attacker to attach a system to an unused, enabled port and to perform information gathering or attacks. A switch can be configured to act like a hub, which means that every system connected to the switch can potentially view all network traffic passing through the switch to all systems connected to the switch. Thus, an attacker could collect traffic that contains usernames, passwords or configuration information about the systems on the network.

## 7.2 Countermeasures

Port security limits the number of valid MAC addresses allowed on a port. All switch ports or interfaces should be secured before the switch is deployed. In this way the security features are set or removed as required instead of adding and strengthening features randomly or as the result of a security incident. Note that port security cannot be used for dynamic access ports or destination ports for Switched Port Analyzer. Still, use port security for active ports on the switch as much as possible.

The following examples show the commands to shut down a single interface or a range of interfaces.

Single interface:

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# shutdown
```

Range of interfaces:

```
Switch(config)# interface range fastethernet 0/2 - 8
Switch(config-if-range)# shutdown
```

Port security capabilities vary depending on the switch model and the IOS version. Each active port can be restricted by a maximum MAC address count with an action selected for any violations. These actions can be to drop the packet (**`violation protect`**), to drop the packet and send a message (**`violation restrict`** or **`action trap`**), or to shutdown the port altogether (**`violation shutdown`** or **`action shutdown`**). **`shutdown`** is the default and the most secure. **`protect`** and **`restrict`** both require tracking the MAC addresses that have been observed and consume more processor resources than **`shutdown`**.

MAC addresses are gathered dynamically, with some switches supporting static entries and sticky entries. Static entries are manually entered for each port (e.g., **`switchport port-security mac-address`** ***`mac-address`***) and saved in the running configuration. Sticky entries are similar to static entries except they are dynamically learned. Existing dynamic entries are converted to sticky entries when the **`switchport port-security mac-address sticky`** command is issued for a port. These former dynamic entries are saved in the running configuration as **`switchport port-security mac-address sticky`** ***`mac-address`***. If the running configuration is then saved to the startup configuration then these MAC addresses will not need to be relearned on restart. Also, the maximum number of MAC addresses (e.g., **`switchport port-security maximum`** ***`value`***) for the port can be set.

The administrator can enable aging for statically configured MAC addresses on a port using the **`switchport port-security aging static`** command. The aging time command (e.g., **`switchport port-security aging time`** ***`time`***) can be set in terms of minutes. Also, the aging type command can be set for inactivity (e.g., **`switchport port-security aging type inactivity`**), which means that the addresses on the configured port age out only if there is no data traffic from these addresses for the period defined by the aging time command. This feature allows continuous access to a limited number of addresses.

The following example shows the commands for restricting a port statically on a Catalyst 3550 switch.

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security mac-address 0000.0200.0088
Switch(config-if)# switchport port-security aging time 10
Switch(config-if)# switchport port-security aging type inactivity
```

To restrict a port dynamically on a Catalyst 3550 switch use the following commands. Note that the aging commands cannot be used with sticky MAC addresses.

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security mac-address sticky
```

Note that when a port security violation occurs, the port will immediately become error-disabled and its LED will turn off. The switch also sends an SNMP trap, logs a syslog message and increments the violation counter. When a port is in the error-disabled state, the administrator can bring it out of this state by entering the **`errdisable recovery cause psecure-violation`** global configuration command or by entering the **`shutdown`** and **`no shutdown`** interface configuration commands.


There are a number of issues to keep in mind when configuring port security on a port connected to an IP phone. Although port security cannot be used on trunk ports, MAC address counters do consider the VLAN tags of arriving packets. The same IP phone sending packets on two VLANs will have two separate entries in the MAC table for the same MAC address and will therefore be counted twice toward the maximum MAC count.

Since IP phones may use both untagged packets (e.g., Layer 2 CDP protocol) and Voice VLAN tagged packets, the IP phone's MAC address will be seen on both the native VLAN and the Voice VLAN. Therefore it will be counted twice. Set the maximum MAC count for a port connected to an IP phone to account for this plus the number of computers attached to the IP phone. Computers that legitimately transmit using multiple MAC address (e.g., Network Load Balancing protocol) must also be taken into account.

A new capability to secure switch ports more quickly and consistently is macros. Macros allow the grouping of available port commands in the order the commands would be manually applied. Any comment is included by using the '**`#`**' character at the start of a line. Macro definitions are closed using the '**`@`**' character.

The following example creates a strict security macro called **unused** to secure the ports, or interfaces, on a 3550 switch.

```
Switch(config)# macro name unused
macro description unused
shutdown
description *** UNUSED Port ***
no ip address
switchport
# Set secure defaults for access mode
switchport mode access
switchport access vlan 999
switchport nonegotiate
# Set secure defaults for trunking mode
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan none
# Only learn source MAC addresses
switchport block multicast
switchport block unicast
# Enable MAC control and set secure options
switchport port-security
switchport port-security maximum 1
switchport port-security aging time 10
switchport port-security aging type inactivity
# Apply any switch-wide access-lists
ip access-group ip-device-list in
mac access-group mac-device-list in
# Set secure defaults for misc. flags and protocols
mls qos cos override
dot1x port-control force-unauthenticated
storm-control broadcast level 0.00
storm-control multicast level 0.00
storm-control unicast level 0.00
no cdp enable
# Default Spanning-tree to secure host settings
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
spanning-tree guard root
@
```

After creating this strict security macro, **unused**, apply the macro to all switch ports as a secure baseline with the following commands.

```
Switch(config)# interface range fasteth0/1 – 24 , giga0/1 – 2
Switch(config-if-range)# macro apply unused
```

The following macros build on the secure base that the **unused** macro has established to open security features enough to support the intended type of system.

```
Switch(config)# macro name host
# Apply macro 'unused' first!
macro description host
# Set the port for a PC host
```

```
dot1x port-control auto
no storm-control broadcast level
no storm-control multicast level
no storm-control unicast level
no shutdown
# The following are recommended port specific commands
#description Host <10.1.10.3>
#switchport access vlan <10>
#switchport trunk native vlan <10>
@

Switch(config)# macro name ipphone
# Apply macro 'unused' first!
macro description ipphone
#
# Set the port for an ipphone without attached PC host
switchport port-security maximum 2
no mls qos cos override
mls qos trust device cisco-phone
mls qos trust dscp
no storm-control broadcast level
no storm-control multicast level
no storm-control unicast level
cdp enable
no shutdown
#
# The following are recommended port specific commands
#description IP PHONE <x1013>
#switchport voice vlan <101>
@

Switch(config)# macro name ipphone-host
# Apply macro 'unused' first!
macro description ipphone & host
#
# Set the port for an ipphone with attached PC host
switchport port-security maximum 3
no mls qos cos override
mls qos trust device cisco-phone
mls qos trust dscp
dot1x port-control auto
no storm-control broadcast level
no storm-control multicast level
no storm-control unicast level
cdp enable
no shutdown
#
# The following are recommended port specific commands
#description IP PHONE <x1014> & HOST <10.1.20.5>
#switchport access vlan <20>
#switchport trunk native vlan <20>
#switchport voice vlan <101>
@
```

Applying these macros will make only those changes to the secure baseline required for the port to fully support the intended type of system. The following example shows how to utilize the previous macros to

configure access ports of the switch from the example diagram for each type of system: host, IP phone, and IP phone with an attached host.

Host:

```
Switch(config)# interface fa0/1
Switch(config-if)# macro apply host
Switch(config-if)# description Host 10.1.10.3
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# exit
```

IP phone:

```
Switch(config)# interface range fa0/2 - 4
Switch(config-if-range)# macro apply ipphone
Switch(config-if-range)# switchport voice vlan 101
Switch(config-if-range)# exit
Switch(config)# interface fa0/2
Switch(config-if)# description IP PHONE x1011
Switch(config)# interface fa0/3
Switch(config-if)# description IP PHONE x1012
Switch(config)# interface fa0/4
Switch(config-if)# description IP PHONE x1013
Switch(config-if)# exit
```

IP phone with an attached host:

```
Switch(config)# interface fa0/5
Switch(config-if)# macro apply ipphone-host
Switch(config-if)# description IP PHONE x1014 & Host 10.1.20.5
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport trunk native vlan 20
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# exit
```

The administrator may want to use the **`macro trace`** command instead of the **`macro apply`** command because the **`macro trace`** command provides for some debugging of macros. Also, the **`show parser macro description`** command will show the last macro applied to each port.

Finally, static MAC addresses and port security applied to every switch port can become burdensome for network administrators. Port Access Control Lists (PACLs) can provide similar security as static MAC addresses and Port Security, and PACLs also provide more flexibility and control. Allowed MAC and IP addresses could be pooled and viewed from a switch-wide perspective. Refer to the Access Control Lists section of this guide for more detail.

# 8 System Availability

## 8.1 Vulnerabilities

Many attacks exist and more are being created that cause denial of service, either partially or completely, to systems or networks. Switches are just as susceptible to these attacks. These attacks focus on making resources (e.g., system processor, bandwidth) unavailable. Specific vulnerabilities associated with system availability include the following.

- Some fast flooding attacks can cause the switch processor to be unavailable for management access.
- 802.3X Flow Control allows receiving ports to pause transmission of packets from the sender during times of congestion. If this feature is enabled, a pause frame can be received, stopping the transmission of data packets. Flow Control pause frames could be used in a denial of service attack.
- Some active attacks and certain errors can cause packet floods to the ports on a switch.
- Directly connected switches running the Unidirectional Link Detection (UDLD) protocol can determine if a unidirectional link exists between them. If one is detected, then the link is shutdown until manually restored. UDLD messages could be used in a denial of service attack.
- The SYN Flood attack sends repeated connection requests without sending acceptance of the acknowledgments to the connection request. This attack can overwhelm the switch's incomplete connection buffer and disable the switch.
- Converged networks carry both data and voice [e.g., Voice over IP (VoIP)] traffic. If not configured properly, these networks can allow voice traffic to become a flood attack against data traffic.

## 8.2 Countermeasures

The following countermeasures will mitigate the vulnerabilities to system availability on each switch.

- To prevent fast flooding attacks and to guarantee that even the lowest priority processes get some processor time use the **`scheduler interval`** command. The following example sets the maximum time before running the lowest priority process to 500 milliseconds access.

  ```
  Switch(config)# scheduler interval 500
  ```

  Another way to guarantee processor time for processes is to use the **`scheduler allocate`** command. This command sets the interrupt time and the process time. The interrupt time is the maximum number of microseconds to spend on fast switching within any network interrupt context. The process time is the minimum number of microseconds to spend at the process level when the network interrupts are disabled. The following example makes 10 percent of the processor available for process tasks, with an interrupt time of 4000 microseconds and a process time of 400 microseconds.

  ```
  Switch(config)# scheduler allocate 4000 400
  ```

- Use the following command on each interface to turn Flow Control off.

  ```
  Switch(config-if)# flowcontrol receive off
  ```

- UDLD should be disabled globally and on every interface where it is not required. To disable UDLD globally use the following command.

```
Switch(config)# no udld enable
```

To disable UDLD on each interface use one of the following commands, depending on the switch model and IOS version.

```
Switch(config-if)# no udld port
Switch(config-if)# udld disabled
```

- To help prevent the SYN Flood attack the administrator can set the amount of time the switch will wait while attempting to establish a TCP connection. The following command sets the wait time to 10 seconds.

```
Switch(config)# ip tcp synwait-time 10
```

- In order for voice traffic to have priority through a network it must be easy to determine which packets are voice, even if the voice signaling and data are encrypted. However, anyone with a network analyzer can also easily pick out the voice traffic. This additional risk must be considered in order to decide if Quality of Service (QoS) parameters will be configured for voice traffic. QoS can be critical to acceptable VoIP implementations. Classifying packets is the first step in establishing their priority throughout the network and should be done at the first available point. Certain switches can classify packets for QoS purposes. The following are some examples of how this could be done in a QoS capable switch.

The following command will turn on QoS features.

```
Switch(config)# mls qos
```

The following command will force best effort priority for an untrusted system.

```
Switch(config-if)# mls qos cos 0
Switch(config-if)# mls qos cos override
```

The following command will accept the priority assigned by a trusted system (e.g., voice gateway).

```
Switch(config-if)# mls qos trust dscp
```

The following commands will accept the priority assigned by an IP Phone but will force best effort priority for any attached computer.

```
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos trust device cisco-phone
Switch(config-if)# switchport priority extend cos 0
```

Isolate voice traffic in separate subnets using VLANs, and control the interactions between voice and data subnets. See the Access Control Lists section of this guide for more information on controlling access on voice and data subnets. Monitor switch and network utilization as changes to the VoIP network distribution, voice codec or additional VoIP telephony systems may be required to correct for flooded subnets or switches.

# 9 Virtual Local Area Networks

## 9.1 Overview

A Virtual Local Area Network (VLAN) is a broadcast domain. All members of a VLAN receive every broadcast packet sent by members of the same VLAN, but they do not receive packets sent by members of a different VLAN. All members of a VLAN are grouped logically into the same broadcast domain independent of their physical location. Adding, moving or changing members is achieved via software within a switch. Routing is required for communication among members of different VLANs.

VLANs provide logical segmentation of a switch into separate domains. Separation of networks into VLANs along functional lines is generally good administrative practice. Stateless filtering, which this guide describes later in the Access Control Lists section, is simpler to implement when systems on the VLAN have similar functions. For instance, creating different VLANs for voice and data simplifies filtering.

There are a variety of methods for implementing VLAN membership [12]. Layer 2 methods include port-based VLANs and MAC layer grouping. Layer 3 methods include network protocol grouping and IP multicast grouping. Cisco switches implement both Layer 2 methods, but Cisco refers to MAC layer grouping as dynamic VLANs. Port-based membership is the most common method of defining VLANs, with all switch vendors supporting it. Only port-based VLANs and dynamic VLANs are discussed in this guide.

For port-based VLANs, the administrator assigns each port of a switch to a VLAN. For example, ports 1-5 could be assigned to VLAN 100, ports 6-8 to VLAN 200 and ports 9-12 to VLAN 300. The switch determines the VLAN membership of each packet by noting the port on which it arrives. On the other hand, dynamic VLAN implementations assign specific MACs to each VLAN. This allows a system to be moved to another port without changing the port's VLAN assignment.

Another important distinction of VLAN implementations is the method used to indicate membership when a packet travels between switches. Switches tag each packet to indicate VLAN membership in accordance with Cisco's Inter-Switch Link (ISL) or the Institute of Electrical and Electronics Engineers (IEEE) 802.1q VLAN trunk standard. Only the IEEE 802.1q trunking is discussed in this guide.

Separation of networks that do not interact makes good sense as well as being good security practice. Physically separate networks for Voice and Data are the most secure, but they can be impractical for all but the most demanding security environments. Providing no separation of Voice and Data networks can also be impractical due to the operationally different demands each type of traffic imposes on the network. For most implementations then, Voice and Data networks must share some common network resources while remaining as physically separate as practicality allows.

Logical separation through the use of VLANs stands out as the best solution in order to balance capability and security within shared network resources. However, logical separation is cooperative and provides little attack mitigation by itself. A layered security approach using defense-in-depth techniques that can make good use of logical separation of the Voice and Data networks is required. Refer to the Access Control Lists section of this guide for ways to provide additional layers of defense. Two useful references from Cisco for best security practices with VLANs are [5] and [9].

The next subsections describe the vulnerabilities and corresponding countermeasures for the following areas: VLAN 1, Private VLAN, VTP, Trunk Auto-Negotiation, VLAN Hopping and Dynamic VLAN Assignment.

## 9.2 VLAN 1

### 9.2.1 Vulnerability

Cisco switches use VLAN 1 as the default VLAN to assign to their ports, including their management ports. Additionally, Layer 2 protocols, such as CDP and VTP, need to be sent on a specific VLAN on trunk links, so VLAN 1 was selected. In some cases, VLAN 1 may span the entire network if not appropriately pruned. It also provides attackers easier access and extended reach for their attacks.

### 9.2.2 Countermeasures

Do not use VLAN 1 for either out-of-band management or in-band management. To provide network-based, out-of-band management, dedicate a physical switch port and VLAN on each switch for management use. Create a Switch Virtual Interface (SVI) Layer Three interface for that VLAN, and connect the VLAN to a dedicated switch and communications path back to the management hosts. Do not allow the operational VLANs access to the management VLAN. Also, do not trunk the management VLAN off the switch.

To provide out-of-band management that separates management traffic from user traffic, use the following commands as an example.

Create the out-of-band management VLAN.

```
Switch(config)# vlan 6
Switch(config-vlan)# name ADMINISTRATION-VLAN
```

Create a management IP address and restrict access to it. Also, enable the interface.

```
Switch(config)# no access-list 10
Switch(config)# access-list 10 permit 10.1.6.1
Switch(config)# access-list 10 permit 10.1.6.2
Switch(config)# interface vlan 6
Switch(config-if)# description ADMIN-VLAN
Switch(config-if)# ip address 10.1.6.121 255.255.255.0
Switch(config-if)# ip access-group 10 in
Switch(config-if)# no shutdown
```

Assign the management VLAN to the dedicated interface.

```
Switch(config)# interface fastethernet 4/1
Switch(config-if)# description Out-Of-Band Admin
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 6
Switch(config-if)# no shutdown
```

Ensure all trunk ports will not carry the management VLAN (e.g., **6**).

```
Switch(config)# interface range gigabitethernet 6/15 - 16
Switch(config-if)# switchport trunk allowed vlan remove 6
```

Assigned the following name for VLAN 1.

```
Switch# vlan 1
Switch(vlan)# name *** DEFAULT VLAN - Do NOT Use! ***
```

Assign all inactive interfaces to an unused VLAN other than VLAN 1 and shut down these interfaces. Note that unused VLANs are not routable.

```
Switch# vlan 999
Switch(vlan)# name *** BIT BUCKET for unused ports ***
Switch(vlan)# shutdown
Switch(vlan)# exit
Switch(config)# interface range fastethernet 5/45 - 48
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 999
Switch(config-if)# shutdown
```

Assign all interfaces to VLANs other than VLAN 1.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 999
```

## 9.3 Private VLAN (PVLAN)

### 9.3.1 Vulnerability

In certain instances where similar systems do not need to interact directly, PVLANs provide additional protection. A primary PVLAN defines the broadcast domain with which the secondary PVLANs are associated. The secondary PVLANs may either be isolated PVLANs or community PVLANs. Hosts on isolated PVLANs communicate only with promiscuous ports, and hosts on community PVLANs communicate only among themselves and with associated promiscuous ports. This configuration provides fine-grained Layer 2 isolation control for each system.

Proper use of PVLANs protects systems from one another that share a common VLAN segment by providing Layer 2 separation. This configuration is commonly found in configurations with multiple servers, such as a De-Militarized Zone (DMZ) subnet off a firewall or a campus-accessible server area off of a high-speed switch. If one server is compromised, then that server may be the source of an attack on other servers. PVLANs mitigate this risk by disallowing communication among servers that should not contact one another.

PVLANs have a limitation that must be addressed for a system to be secure. A router may forward traffic back on the same subnet from which it originated. A PVLAN only isolates traffic at Layer 2. A router, which is a Layer 3 system and is attached to a promiscuous port, could route traffic to all ports in the PVLAN. Two hosts on an isolated PVLAN will fail to communicate at Layer 2 but may succeed at Layer 3, which circumvents the PVLAN's Layer 2 protection. This situation can be addressed where needed by Router Access Control Lists.

### 9.3.2 Countermeasures

A configuration with multiple servers on a single VLAN should use PVLANs for Layer 2 separation among the servers. Routers should be on promiscuous ports and servers on an isolated PVLAN. Only servers that need to communicate directly with other servers should be on a community PVLAN. Implement VACLs on the primary PVLAN to filter traffic originated by and routed to the same segment.

In certain instances where similar systems do not need to interact directly, PVLANs provide additional attack mitigation. In Voice networks this may be the case with certain proxies serving the same user set but using different protocols or collocated CallManagers serving different user sets. In this latter example, collocation allows the use of the same stateless filter for the CallManagers, while the private VLAN keeps a compromised CallManager from reaching the others directly at Layer 2.
The following example creates a PVLAN with an NTP server on a promiscuous port and two isolated servers.

```
Switch# vlan 200
Switch(vlan)# name SERVERS-PRIVATE
Switch(vlan)# private-vlan primary
Switch(vlan)# private-vlan association 201

Switch# vlan 201
Switch(vlan)# name SERVERS-ISOLATED
Switch(vlan)# private-vlan isolated

Switch(config)# interface GigabitEthernet6/1
Switch(config-if)# description SERVER 1
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# no shutdown

Switch(config)# interface GigabitEthernet6/2
Switch(config-if)# description SERVER 2
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# no shutdown

Switch(config)# interface GigabitEthernet6/6
Switch(config-if)# description SERVER NTP Server
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 200 201
Switch(config-if)# no shutdown
```

## 9.4 Virtual Trunking Protocol (VTP)

### 9.4.1 Vulnerability

VTP is a Cisco-proprietary Layer 2 messaging protocol used to distribute VLAN configuration information over trunks. VTP allows the addition, deletion and renaming of VLANs on a network-wide basis, which allows switches to have a consistent VLAN configuration within a VTP management domain. All switches in the same management domain share their VLAN information, and a switch may participate in only one VTP management domain.

A switch may be in one of three VTP modes: server, transparent and client. A switch in server mode originates VTP VLAN configurations for other switches to use. In server mode administrators can create, modify and delete VLANs for the entire VTP management domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their databases. A switch in transparent mode receives and forwards VTP packets, but it does not originate VTP packets, nor does it use the ones it receives to reconfigure its VLAN database. A switch in client mode receives, uses, and passes on VTP packets, but it does not originate them. A switch in any mode may engage in VTP pruning, in which it refrains from retransmitting VTP packets on selected ports.

By default, switches share VLAN information without any authentication. Thus, inaccurate VLAN settings can propagate throughout a VTP domain. Compounding this problem, switches come with VTP in server mode by default, and a server with a higher configuration revision number in its VTP database supersedes one with a lower number. It is entirely possible for a single switch, which has undergone a sufficient number of VTP reconfigurations, to completely overwrite or eliminate all VLAN assignments of an operational network by just connecting it to the network. Such an attack would not necessarily have to be malicious; simply moving a lab switch to an operational network could have this effect.

By default VTP management domains are set to an insecure mode without a password. It is possible to mitigate the danger of accidental overwrites with password protection. A client checks the password before implementing a VLAN configuration it receives via VTP. The password, however, does not encrypt or otherwise obscure the information within VTP. VTP configured with password only ensures message authenticity. An attacker with a network analyzer can easily gain knowledge of the local network's VLAN structure. Still, the password is hashed with other information, and it is difficult to determine the password from other collected network traffic.

### 9.4.2 Countermeasures

It is clear that VTP simplifies administration, particularly where large numbers of VLANs are deployed. Nevertheless, VTP is sufficiently dangerous that its use is discouraged. If possible, turn off VTP by using the following commands.

```
Switch(config)# no vtp mode
Switch(config)# no vtp password
Switch(config)# no vtp pruning
```

If VTP is necessary, then consider the following settings. Set up VTP management domains appropriately. All switches in the same management domain share their VLAN information. A switch can only participate in one VTP management domain. Use the following command as an example to set the VTP management domain.

```
Switch(config)# vtp domain test.lab
```

Assign a strong password to the VTP management domain. All switches within the domain must be assigned the same password. This prevents unauthorized switches from adding themselves to the VTP management domain and passing incorrect VLAN information. Use password protection on VTP domains as shown in the command in the following example.

```
Switch(config)# vtp password g00d-P5WD
```

Enable VTP pruning and use it on appropriate ports. By default, VLANs numbered 2 through 1000 are pruning-eligible.

```
Switch(config)# vtp pruning
```

Set VTP to transparent mode with the following command.

```
Switch(config)# vtp transparent
```

## 9.5 Trunk Auto-Negotiation

### 9.5.1 Vulnerability

A trunk is a point-to-point link between two ports, typically on different network systems, that aggregates packets from multiple VLANs. Cisco implements two types of trunks: IEEE 802.1q, which is an open standard; and ISL, which is a Cisco proprietary standard.

A port may use the Dynamic Trunking Protocol (DTP) to automatically negotiate which trunking protocol it will use, and how the trunking protocol will operate. By default, a Cisco Ethernet port's default DTP mode is "dynamic desirable", which allows the port to actively attempt to convert the link into a trunk. Even worse, the member VLANs of the new trunk are all the available VLANs on the switch. If a neighboring port's DTP mode becomes "trunk", "dynamic auto", or "dynamic desirable", and if the two switches support a common trunking protocol, then the line will become a trunk automatically, giving each switch full access to all VLANs on the neighboring switch. An attacker who can exploit DTP may be able to obtain useful information from these VLANs.

### 9.5.2 Countermeasures

Do not use DTP if possible. Assign trunk interfaces to a native VLAN other than VLAN 1.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 998
```

Put non-trunking interfaces in permanent non-trunking mode without negotiation.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport nonegotiate
```

Put trunking interfaces in permanent trunking mode, without negotiation.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
```

Specifically list all VLANs that are part of the trunk.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport trunk allowed vlan 6, 10, 20, 101
```

Use a unique native VLAN for each trunk on a switch.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport trunk native vlan 998

Switch(config)# interface fastethernet 0/2
Switch(config-if)# switchport trunk native vlan 997
```

## 9.6 VLAN Hopping

### 9.6.1 Vulnerability

In certain situations it is possible to craft a packet in such a way that a port in trunking mode will interpret a native VLAN packet as though it were from another VLAN, allowing the packet to become a member of a different VLAN. This technique is known as VLAN hopping. Using VLAN hopping, a malicious intruder who has access to one local network might inject packets into another local network in order to attack machines on the target network. [1, 13]

### 9.6.2 Countermeasures

Disable CDP, VTP and DTP on each switch if possible. Assign a shutdown VLAN as the 'native' VLAN of each of the trunks, and do not use this VLAN for any other purpose.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport trunk native vlan 998
Switch(config-if)# no cdp enable
```

Restrict the VLANs on a trunk to only those that are necessary for that trunk, as described in the Trunk Auto-Negotiation subsection previously.

# 10 Spanning Tree Protocol

## 10.1 Vulnerabilities

Spanning Tree Protocol (STP), also known as 802.1d, is a Layer 2 protocol designed to prevent loops within switched networks. Loops can occur when redundant network paths have been configured to ensure resiliency. Typically, STP goes through a number of states (e.g., block, listen, learn, and forward) before a port is able to pass user traffic. This process can take between 30 and 50 seconds. In cases where a single host is connected to a port, and there is no chance of a loop being created, the STP Portfast feature can be utilized to immediately transition the port into a forwarding state. However, it will still participate in STP calculations and move into a blocked state in the event of a network loop.

A vulnerability associated with STP is that a system within the network can actively modify the STP topology. There is no authentication that would prevent such an action. The bridge ID, a combination of a two-byte priority and a six-byte MAC address, determines the root bridge within a network. The lower the bridge ID, the more likely the switch will be elected as the root bridge. A switch with the lowest bridge ID can become the root bridge, thereby influencing traffic flows and reducing the efficiency of the network.

## 10.2 Countermeasures

### 10.2.1 STP Portfast Bridge Protocol Data Unit (BPDU) Guard

The STP Portfast BPDU Guard allows network administrators to enforce the STP topology on ports enabled with Portfast. Systems attached to ports with the Portfast BPDU Guard enabled will not be allowed to modify the STP topology. Upon reception of a BPDU message, the port is disabled and stops passing all network traffic.

This feature can be enabled both globally and individually for ports configured with Portfast. By default, STP BPDU guard is disabled. The following command is used to globally enable this feature on a Cisco 3550 series switch.

```
Switch(config)# spanning-tree portfast bpduguard default
```

Use the following command to verify the configuration.

```
Switch> show spanning-tree summary totals
…
…
PortFast BPDU Guard is enabled by default.
…
…
```

To enable this feature at the interface level on a Cisco 3550 series switch, use the following command.

```
Switch(config-if)# spanning-tree bpduguard enable
```

When STP BPDU guard disables a switch port, it can be configured to recover automatically, or it can be manually re-enabled by a network administrator. The following commands can be used to configure a port to automatically recover when placed in a disabled state. The timeout interval can range from 30 to 86400 seconds, with the default interval being 300 seconds. In the example below, a port placed in an error-disabled state will recover after 400 seconds.

```
Switch(config)# errdisable recovery cause bpduguard
Switch(config)# errdisable recovery interval 400
```

### 10.2.2 STP Root Guard

The STP Root Guard feature is another mechanism used to protect the STP topology. Unlike the BPDU Guard, STP Root Guard allows participation in STP as long as the attached system does not attempt to become the root. If the Root Guard is activated, then the port recovers automatically after it quits receiving the superior BPDUs that would make it the root. Root Guard can be applied to one or more ports on edge switches and on internal switches on a network. In general, apply this feature to those ports on each switch that should not become the root.

The following command is used within the interface configuration mode to enable STP Root Guard on the Cisco 3550 series switch.

```
Switch(config-if)# spanning-tree guard root
```

# 11 Access Control Lists

## 11.1 Vulnerabilities

A switch with either no access control list (ACL) or a permissive ACL applied to its interfaces allows broad access for TCP/IP connections (e.g., FTP, telnet, DNS, HTTP, SNMP, ICMP) through the switch to any system (e.g., critical server) on the protected network. Broad access means that all systems or large numbers of systems can connect through the switch. Both of these situations result in more avenues for information gathering and attacks. Some of this access may be allowed by default and may be configured in ways that are not obvious to the administrator.

## 11.2 Countermeasures

In preparation for implementing ACLs, categorize systems attached to the switches into groups that use the same network services. Grouping systems this way helps reduce the size and complexity of associated ACLs. In voice networks, using separate VLANs for CallManagers, SCCP IP Phones, SIP IP Phones, Proxies, MGCP gateways and H.323 gateways is a good example of this. Consider also the network services used by similar systems from different manufacturers (e.g., H.323 gateways) as further refinement of ACLs may make sense under the network security policy. Another useful reference from Cisco for understanding ACLs is [8].

ACLs can permit or deny each packet based on the first access control statement that the packet matches. There are different types of access control lists: Port Access Control List (PACL), Router Access Control List (RACL) and VLAN Access Control List (VACL).

### 11.2.1 Port Access Control List (PACL)

PACLs are used to restrict the packets allowed into a given port. There are two types of PACLs, IP PACLs based on IP access lists and MAC PACLs based on MAC access lists. IP PACLs only filter packets with an IP ethertype. Creating a standard or extended IP access list and applying the access list to a switchport interface is all that is required to implement IP PACLs.

On switches that support Unicast MAC Filtering, MAC PACLs will filter all packets regardless of their ethertype. On switches that don't support Unicast MAC Filtering, MAC PACLs will only filter packets with ethertypes other than IP. Consult the release notes for the IOS in use to determine Unicast MAC Filtering support or perform MAC filtering tests before using MAC PACLs. Creating an extended MAC access list and applying the access list to a switchport interface is all that's required to implement MAC PACLs.

Given an IOS that supports Unicast MAC Filtering, the following commands are an example of using PACLs to restrict port access to one specific MAC address and IP access to one specific IP address from that MAC address.

```
Switch(config)# mac access-list extended host-mac
Switch(config-ext-macl)# permit host 0000.0101.0011 any
Switch(config-ext-macl)# exit
Switch(config)# ip access-list extended host-ip
Switch(config-ext-nacl)# permit ip host 10.1.101.11 any
Switch(config-ext-nacl)# exit
Switch(config)# interface fa0/2
Switch(config-if)# mac access-group host-mac in
Switch(config-if)# ip access-group host-ip in
```

If the IOS does not support Unicast MAC Filtering, then the preceding example will restrict port access to one specific MAC address for non-IP packets and restrict IP access to one specific IP address for IP packets.

Another way to use PACLs is in place of static MAC addresses and port security. Allowed MAC and IP addresses could be pooled and viewed from a switch wide perspective. Consider the following commands as an example of this pooled addressing security.

```
Switch(config)# mac access-list extended mac-device-list
Switch(config-ext-macl)# permit host 0000.0101.0011 any
Switch(config-ext-macl)# permit host 0000.0101.0012 any
Switch(config-ext-macl)# permit host 0000.0101.0013 any
Switch(config-ext-macl)# permit host 0000.0101.0014 any
Switch(config-ext-macl)# permit host 0000.0010.0003 any
Switch(config-ext-macl)# permit host 0000.0020.0005 any

Switch(config)# ip access-list extended ip-device-list
Switch(config-ext-nacl)# permit ip host 10.1.101.11 any
Switch(config-ext-nacl)# permit ip host 10.1.101.12 any
Switch(config-ext-nacl)# permit ip host 10.1.101.13 any
Switch(config-ext-nacl)# permit ip host 10.1.101.14 any
Switch(config-ext-nacl)# permit ip host 10.1.10.3 any
Switch(config-ext-nacl)# permit ip host 10.1.20.5 any

Switch(config)# interface range fa0/1 - 24
Switch(config-if-range)# ip access-group ip-device-list in
Switch(config-if-range)# mac access-group mac-device-list in
```

This example applies lists of allowed MAC address and IP addresses to all access ports of the switch. The network administrator needs to maintain only the two lists instead of associating specific addresses with specific ports and of maintaining the addresses on each port individually. If established security policy allows, this switch wide implementation trades some additional risk to gain easier and more consistent configuration and administration.

### 11.2.2 Router Access Control List (RACL)

A RACL can restrict packets into or out of a given Layer 3 interface. A RACL is configured and applied identically to a router ACL, except a RACL is applied to a VLAN interface.

```
Switch(config)# access-list 1 remark Simple Example
Switch(config)# access-list 1 permit any
Switch(config)# interface vlan 6
Switch(config-if)# ip access-group 1 in
```

### 11.2.3 VLAN Access Control List (VACL)

VACLs use VLAN Maps that are configured like route-maps on routers. VLAN Maps can be applied to filter all traffic into, through and out of a specific VLAN. The same VLAN Map filters bridged, inbound and outbound packets for the VLAN. The following example will block all TCP packets from VLAN 6 while allowing all other packets through.

```
Switch(config)# no access-list 101
Switch(config)# access-list 101 remark Simple TCP Example
Switch(config)# access-list 101 permit tcp any any
Switch(config)# vlan access-map vlan6-map 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map vlan6-map 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter vlan6-map vlan-list 6
```

### 11.2.4 ACLs and Fragments

If extended ACL configurations filtering on Layer 4 (i.e., TCP or UDP ports) are used, then the filtering of fragment packets require special consideration. Fragment packets that do not contain Layer 4 information will never match **`deny`** statements that include Layer 4 rules. They will go through the switch. These same fragments, which otherwise match a **`permit`** statement that includes Layer 4 rules, will be permitted. This situation can pose a security risk in certain environments since the first fragment containing the Layer 4 information may match a **`deny`** statement and be dropped while the remaining fragments will not match the **`deny`** statement and pass through. Use the **`fragments`** keyword in each appropriate ACL statement.

### 11.2.5 ACL Implementation Issues

In general, the most restrictive and specific set of ACLs possible should be used on a switch. However, conflicts, limitations and cautions exist when different types of ACLs are used in combination. Before implementing any ACLs, consult the release notes for the specific IOS version and switch model. Also, perform testing on ACLs to fully understand all implementation interactions before deploying them as a security control. The following tables provide guidance on the possible combinations of the different types of ACLs on Cisco 3550 switches using IOS version 12.1(19)EA1. This IOS version supports Unicast MAC filtering.

**Table 1 – Options for Single Access Control List**

| ACL Type | Access Port | Trunk Port | VLAN Interface (SVI) | VLAN |
|---|---|---|---|---|
| **PACL (MAC)** | Input only | Input only | No | No |
| **PACL (IP)** | Input only, IP only | Input only, IP only, Native VLAN only | No | No |
| **VACL / VLAN Map** | No | No | No | Yes |
| **RACL** | No | No | Input, Output, or Both | No |

**Table 2 – Options for Multiple Access Control Lists**

| ACL Type | PACL (MAC) | PACL (IP) | VACL | RACL |
|---|---|---|---|---|
| **PACL (MAC)** | N/A | Yes | Caution (PACL Priority) | Output RACLs only |
| **PACL (IP)** | Yes | N/A | Caution (PACL Priority) | Output RACLs only |
| **VACL** | Caution (PACL Priority) | Caution (PACL Priority) | N/A | Caution (Merged) |
| **RACL** | Output RACLs only | Output RACLs only | Caution (Merged) | N/A |

PACL Priority – On a port where PACLs are applied and VLAN(s) are assigned (regardless if it is by access VLAN, voice VLAN or trunked VLANs) and any of the assigned VLANs has a VACL applied, then the PACL filters will be used and the VACL filters will be ignored for that port.

Merged – When VACLs are applied to a VLAN that also has a SVI (e.g., interface VLAN) with RACLs applied, the switch attempts to merge the access lists in memory. This may have unexpected results. Perform ACL tests before implementing any combination of ACLs.

# 12 Logging and Debugging

## 12.1 Vulnerabilities

Poor configuration and monitoring of the logging and debugging capabilities on a switch may lead to inadequate information when an attack occurs against the switch or the networks connected to it. Problems can also arise if logging is enabled but not managed properly. Log files maintained on the switch are at risk of being overwritten since there is limited space on the switch itself to store logging information. Also, logs that reside on the switch may be subject to erasure or compromise by an attacker.

System log information also needs to be detailed enough to be of use to an administrator. If logging is configured at an inappropriate logging level, then the administrator may not have critical information needed to identify an incident on a system or on the network. Logging that is not tuned properly can also overwhelm an administrator by providing information that is superfluous. Finally, log and debug messages that do not have timestamps or have an unreliable time source can cause confusion if an administrator is trying to piece together possible attack events.

## 12.2 Countermeasures

This section covers for switches both the configuration settings for logging and debugging and the ways to diagnose the status of the logging and debugging.

### 12.2.1 Logging Configuration

Enable logging on each switch with the following command.

```
Switch(config)# logging on
```

Direct logs from each switch to at least one log host, which should be a dedicated system on the protected network. Typically, the log host has a syslog service enabled to receive logs. On the log host disable all unnecessary TCP or UDP services. Also, remove all unnecessary user accounts. If possible, configure a ruleset on the log host itself to do the following: allow only the network systems (e.g., switches) to send logs to the log host, and allow only administrators' systems access to the log host. Finally, centralized log hosts are a good mechanism for correlating attacks across the computer network. The following command shows how to direct logs to a log host. Note that IOS can support multiple log hosts; the administrator just uses the **logging *<IP address>*** command for each log host on the network.

```
Switch(config)# logging 10.1.6.89
```

For each access-list on each switch, set the **log** keyword for each access-list statement that denies network traffic through the switch or that allows or denies access to the switch itself. The following command shows an example access-list statement with the **log** keyword.

```
Switch(config)# access-list 101 deny ip any any log
```

The administrator needs to configure the trap level for syslog on each switch to determine which logs will be sent to the log host. The following shows the command to set the trap level, along with description of the various trap levels.

```
Switch(config)# logging trap level
```

where ***level*** is the number or keyword that corresponds to one of the following eight syslog severity levels

| Number | Keyword | Message Examples |
|---|---|---|
| 0 | Emergencies | System is unusable |
| 1 | Alerts | Immediate action needed |
| 2 | Critical | Critical conditions |
| 3 | Errors | Error conditions |
| 4 | Warnings | Warning conditions |
| 5 | Notifications | Exit global configuration mode |
| 6 | Informational | Access-list statement match |
| 7 | Debugging | Debugging messages |

Set the trap level for syslog on each switch to at least **informational**. This is necessary because log messages for each access-list statement that has the **log** keyword are generated only at the **informational** level. When a level is configured for logging, all messages at that level and lower will be logged. For example, if **critical** is the level, then all **critical**, **alerts** and **emergencies** level messages will be logged.

There are other ways to send logs that are important to consider. For example, the console for the switch can receive logs, but how the console is used should help determine which logs the console should receive. If the console output is being captured, then more logging may be appropriate. At a minimum, set the trap level for the console to **critical** using the following command.

```
Switch(config)# logging console critical
```

Terminal lines can also receive logging information. At a minimum, set the trap level for the terminal lines to **critical** using the following command.

```
Switch(config)# logging monitor critical
```

The administrator can issue the following command to begin the display of logging information or debugging information for the current terminal and session.

```
Switch# terminal monitor
```

Each log message, sent from the switch to the log host, can have its source address set to the same value. This is useful because the administrator can distinguish at the log host which switch sent the log. Also, the administrator can create an access-list that allows only one source address per switch to send logs. The following command sets the source address by using one of the interfaces of the switch. Thus, this interface must be configured with an IP address for this setting to be successful. The **Loopback 0** interface would be a good choice for the source address.

```
Switch(config)# logging source-interface type number
```

where ***type*** is the interface type and ***number*** is the interface number

The syslog facility can also be set on the switch. Use the following command to do this.

```
Switch(config)# logging facility facility-type
```

where ***facility-type*** is one of the following keywords

| | | |
|---|---|---|
| **local0** | **local3** | **local6** |
| **local1** | **local4** | **local7 (default)** |
| **local2** | **local5** | **syslog** |

Each system status message logged in the system logging process has a sequence reference number applied. The following command makes the sequence number for each message visible by displaying the number with the message.

```
Switch(config)# service sequence-numbers
```

### 12.2.2 Time Information

Configure each switch and each log host to point to at least two different reliable timeservers to ensure accuracy and availability of time information and to protect against denial-of-service attacks against a single timeserver. Each timeserver typically has a Network Time Protocol (NTP) server enabled. NTP synchronizes systems to an authoritative time source. Accurate time is important for logging and debugging messages. Synchronizing the time greatly aids network-wide investigations involving multiple logging sources. For example, the following command designates the addresses of a timeserver and the interface for the source address to be used in the NTP messages sent from the switch to the timeserver.

```
Switch(config)# ntp server 10.1.200.94 source Loopback0 prefer
```

Cisco switches offer support for NTP authentication to prevent accidental or malicious changes of the system clock. For example, the following commands enable NTP authentication, create an authentication key (e.g., **aGr8key!**) associated with a key number (e.g., **42**), identify that key number as required for authentication, and configure an NTP server with associated key.

```
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 42 md5 aGr8key!
Switch(config)# ntp trusted-key 42
Switch(config)# ntp server 10.1.200.94 key 42 prefer
```

Note that when a switch is configured to use NTP for time synchronization, the switch also becomes an NTP server. Unless the switch is meant to act as an NTP server on the network, NTP should be disabled on all interfaces that do not pass NTP traffic.

```
Switch(config-if)# ntp disable
```

In addition to referencing timeservers, the switch should include the date and the time when a log message or a debug message is sent. To reflect the date and the time in these messages, timestamps need to be set on the switch. Configure timestamps for logging and debugging with the following commands.

```
Switch(config)# service timestamp log datetime msec localtime
      show-timezone
Switch(config)# service timestamp debug datetime msec localtime
      show-timezone
```

where

```
datetime          – Provides the date and the time
msec              – Include milliseconds with the time
localtime         – Shows time in terms of the local time
show-timezone     – Indicates the time zone
```

If the switches being managed are in multiple timezones, then use Greenwich Mean Time (GMT) for the timezone for all the switches. Otherwise, use the local timezone on the switch. The following commands show an example of setting the timezone for Eastern Standard Time (e.g., **EST**) and setting the switch to automatically change for daylight savings time (e.g., **EDT**).

```
Switch(config)# clock timezone EST –5
Switch(config)# clock summer-time EDT recurring
```

# 13 Authentication, Authorization, and Accounting

## 13.1 Vulnerabilities

Typically, remote administrator access to a Cisco switch requires a password but no username. There is no accountability for which administrator has connected to the switch. Also, no mechanism is set by default for what an administrator is allowed to do. Finally, performing authentication only locally at a switch does not provide a central method for authenticating administrators and can lead to inconsistencies in authentication.

## 13.2 Countermeasures

Cisco provides three security mechanisms called Authentication, Authorization and Accounting (AAA) that can address these vulnerabilities. Configure AAA on a switch in conjunction with a security server. Use of AAA with a security server provides the security mechanisms described below.

| | |
|---|---|
| Authentication | – This mechanism identifies remote and local users before granting access to the switch. |
| Authorization | – This mechanism controls access to remote services based on defined attributes associated with the authenticated user. |
| Accounting | – This mechanism provides a secure logging capability for recording services accessed by a user as well as a user's bandwidth consumption |

AAA allows for security servers to use three types of protocols: RADIUS, TACACS+ and Kerberos. Using a security server instead of relying on user data located on the switch (e.g., line passwords or enable passwords) provides the added benefit of having a centralized server that many network systems can make use of for AAA. The use of a security server also enhances authorization capabilities and allows for accounting, which is not available without using a security server. The following steps will provide options based on the type of security server chosen.

Define at least one local user first. This setting is important, especially if the administrator is configuring the switch remotely. If the administrator does not have a local user set and the remote connection breaks, then the administrator will not be able to connect remotely again. The following command shows an example of how to create a local user, including the username (e.g., **`ljones`**) with a privilege level (e.g., **`0`**) and a password (e.g., **`g00d-P5WD`**) that will be MD5-encrypted.

```
Switch(config)# username ljones privilege 0 secret g00d-P5WD
```

To enable AAA, use the following command.

```
Switch(config)# aaa new-model
```

Specifying a security server or set of security servers can be done using the following commands for TACACS+ and RADIUS:

```
{tacacs-server | radius-server} host ip-address
{tacacs-server | radius-server} key key
```

One important difference to note about using Kerberos, versus RADIUS or TACACS+, is that additional configuration is required to allow the switch to communicate with the key distribution center (KDC). Refer to [3] for more information on configuring a Cisco system for Kerberos.

### 13.2.1 Authentication

It is necessary to create a login authentication method list(s) (specifying which types of security server protocols will be used and in what order). The following shows the syntax for the command to enable authentication at login at the switch, using either the default list or a custom list and using authentication methods.

```
aaa authentication login {default | list-name } method1 [method2...]
```

where the methods include the following

**`group radius`** – uses all RADIUS servers listed
**`group tacacs+`** – uses all TACACS+ servers listed
**`group`** ***`group-name`*** – uses servers defined by ***`group-name`*** (RADIUS or TACACS+)
**`krb5`** – uses Kerberos

An example for configuring a switch to provide TACACS+ authentication using a group name of **`aaa-admin-servers`** is the following.

```
Switch(config)# aaa group server tacacs+ aaa-admin-servers
Switch(config)# aaa authentication login default group aaa-admin-
      servers
```

The switch can provide a local login method if for some reason the AAA server is unavailable. It will not allow a user that has been denied access by the AAA server to login using the local authentication mechanism. In order to implement local login, a username and password must be configured. Multiple accounts can be created on the switch each with different levels of access. The additional advantage of using the local login as a fallback authentication method is that the administrator is prompted for both a username and password. The following example shows the use of **`local`** as a fallback.

```
Switch(config)# aaa authentication login aaa-fallback group aaa-admin-
      servers local
```

The last step is to apply the authentication method list(s) to the desired lines. The following shows the syntax for the command to enable authentication services to a specific line or a group of lines, applying either the default list or a custom list.

```
login authentication {default | list-name}
```

The following example would apply the named list, **`aaa-fallback`**, to the console line.

```
Switch(config)# line con 0
Switch(config-line)# login authentication aaa-fallback
```

### 13.2.2 Authorization

Similar to authentication, configuring authorization requires the security administrator to define method lists. The following shows the syntax for the command to enable authorization of user access to systems on a network, using either the default list or a custom list and using

```
aaa authorization {auth-proxy | network | exec | commands level |
      reverse-access | configuration | ipmobile} {default | list-name}
      method1 [method2...]
```

Recommended authorization types include enabling authorization for the following.

| | |
|---|---|
| **auth-proxy** | – security policies are applied on a per-user basis |
| **network** | **–** service requests |
| **exec** | **–** initiation of an EXEC session |
| **commands *level*** | – EXEC command execution at specified levels |
| **reverse-access** | **–** reverse telnet session |
| **configuration** | **–** download configurations from security server |
| **ipmobile** | **–** IP Mobile services |

An example of configuring a switch to provide TACACS+ authorization, using the **aaa-admin-servers** group for EXEC and privileged EXEC commands, is the following.

```
Switch(config)# aaa authorization exec default group aaa-admin-servers
Switch(config)# aaa authorization commands 15 aaa-config group aaa-
      admin-servers if-authenticated
```

Applying named authorization lists is the final authorization configuration step. The following shows the syntax for the command to enable authorization services to a specific line or a group of lines.

```
authorization {arap | commands level | exec | reverse-access} {default
      | list-name}
```

To enable authorization services to the console line for commands at privilege level 15 (e.g., **commands 15**) with an authorization list (e.g., **aaa-config**), the administrator would use the following example.

```
Switch(config)# line con 0
Switch(config-line)# authorization commands 15 aaa-config
```

### 13.2.3 Accounting

The final piece of AAA to configure is accounting. Cisco switches support accounting records only for TACACS+ and RADIUS security servers. The following shows the syntax for the command to enable accounting of requested services for security purposes when using RADIUS or TACACS+.

```
aaa accounting {system | network | exec | connection | commands level}
      {default | list-name } {start-stop | stop-only | none} [method1
      [method2...]]
```

The five types of accounting that can be specified include the following.

**system** – information for all system events (no support for named lists, must be default)
**network** – information on all network service requests
**exec** – information on user EXEC terminal sessions
**connection** – information on all outbound connections
**commands *level*** – information about all EXEC commands, at a certain privilege level, that are issued

To control the amount of accounting records for events specified by a method list, use the following.

**start-stop** – notices begin at start of event and continue until the end of the event
**stop-only** – send only a stop notice related to the event
**none** – no accounting

It is recommended that accounting be enabled for all five types, in particular accounting for level 15 commands. The following example enables all five types and uses the default accounting method, **start-stop**.

```
Switch(config)# aaa accounting exec default start-stop group aaa-admin-
      servers
Switch(config)# aaa accounting commands 15 default start-stop group
      aaa-admin-servers
Switch(config)# aaa accounting network default start-stop group aaa-
      admin-servers
Switch(config)# aaa accounting connection default start-stop group aaa-
      admin-servers
Switch(config)# aaa accounting system default start-stop group aaa-
      admin-servers
```

The following shows the syntax for the command to enable accounting services to a specific line or a group of lines.

```
accounting {arap | commands level | exec | connection} {default | list-
      name}
```

To enable accounting services to the console line for commands at privilege level 15 (e.g., **commands 15**) and for system-level events (e.g., **exec**), the administrator would use the following example.

```
Switch(config)# line con 0
Switch(config-line)# accounting commands 15 default
Switch(config-line)# accounting exec default
```

To specify when accounting records are sent to security servers, enable interim accounting records.

```
Switch(config)# aaa accounting update {newinfo | periodic minutes}
```

The **newinfo** option only sends update records when there is new accounting information, while the **periodic** option will send updates based on a configurable interval, in minutes. Using the **periodic** setting will generate many more accounting records since interim reports on events that are currently happening are included. Thus, it is recommended to use the **newinfo** option.

By default, Cisco switches do not generate accounting records for failed login authentication attempts when accounting is enabled. To enable these accounting records, use the following command.

```
Switch(config)# aaa accounting send stop-record authentication failure
```

### 13.2.4 802.1X Port-Based Authentication

The IEEE 802.1X standard is a port-based access control and authentication protocol. Although the implementation of this standard is still evolving, it is currently available on many of Cisco's switches. It forces a client that is connected to a switch port to authenticate to a server, such as Cisco's Access Control Server, before gaining access to a network. The client must be running 802.1X compliant software, which is available on certain operating systems (e.g., Windows XP).

The following example enables 802.1X on a Cisco IOS switch on the interface Ethernet 1/0.

```
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# interface Ethernet 1/0
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode single-host
```

When 802.1X is configured on a port attached to a Cisco IP phone and a Voice VLAN is also configured, the IP phone does not need to authenticate using 802.1X to receive network access. The first IP phone identified through CDP will be given access to the network through the Voice VLAN. No other MAC addresses will be accepted on the Voice VLAN until a system authenticates using 802.1X. Since port security should be enabled, **`dot1x multiple-hosts`** mode may be required. With multiple-hosts mode enable, once any system is authenticated by 802.1X all MAC addresses will be accepted over the Voice VLAN but only the authenticated system will be accepted on the native VLAN. Port security or PACL capabilities must be used to restrict the allowable MAC addresses. See the Port Security section of this guide for details about accounting for IP phone MAC addresses. See the Access Control Lists section of this guide for details on PACLs.

# 14 Advanced Topics

Future versions of this guide will provide security configuration guidance for the following switch capabilities. These capabilities are available generally only on the high-end Cisco switches.

**Multi-Layer Switching (MLS):** MLS provides hardware-based Layer 3 switching. IP MLS offloads the processor-intensive packet routing from network routers by switching unicast IP data packet flows between IP subnets using ASIC switching hardware. Standard routing protocols, such as OSPF, EIGRP, RIP and IS-IS are used for route determination.

**Firewall Services Module (FWSM):** The FWSM is a stateful inspection firewall capability based on Cisco PIX technology. The FWSM creates a connection table entry for each session flow. The FWSM controls all inbound and outbound traffic by applying the security policy to these connection table entries. [6]

**Virtual Private Network Services Module (VPNSM):** The VPNSM feature enables both site-to-site and remote-access IPSEC VPN capability. The VPNSM adds hardware-based encryption, authentication and integrity to network services such as integrated voice, video and data. [10]

**Intrusion Detection System Service Module (IDSM):** The IDSM passively monitors network segments and traffic for malicious attacks. The IDSM is a signature-based network intrusion detection capability that inspects copies of packets thru either a VACL capture or SPAN configuration.

**Multi-Protocol Label Switching (MPLS):** MPLS is an emerging high-speed switching protocol typically deployed in the network core of a large enterprise such as an ISP. MPLS uses label switch technology to simplify routing and enhance overall network performance. MPLS offers traffic engineering, virtual private network, and QoS capabilities. [7]

**Redundancy:** Redundancy is a network design principle that protects against single points of failure.

# 15 Sample Configuration Files

## 15.1 Cisco Catalyst 6500 Switch

```
!==========================================================================
! 6500 - Distribution/Core Policy Layer
!==========================================================================

version 12.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname Cat121
!
boot system flash sup-bootflash:c6k222-jk9sv-mz.122-14.SY.bin
logging snmp-authfail
logging buffered 64000 notifications
aaa new-model
aaa group server tacacs+ aaa-admin-servers
 server 10.1.6.88
!
aaa authentication banner ^CAccessing AAA-Servers^C
aaa authentication fail-message ^CAAA Authentication FAILED.^C
aaa authentication login default group aaa-admin-servers
aaa authentication login aaa-fallback group aaa-admin-servers enable
aaa authorization exec default group aaa-admin-servers
aaa authorization commands 15 default group aaa-admin-servers
aaa authorization commands 15 aaa-config group aaa-admin-servers if-
authenticated
aaa authorization network default if-authenticated
aaa authorization configuration default group aaa-admin-servers
aaa accounting suppress null-username
aaa accounting send stop-record authentication failure
aaa accounting delay-start
aaa accounting nested
aaa accounting update periodic 1440
aaa accounting exec default start-stop group aaa-admin-servers
aaa accounting commands 15 default start-stop group aaa-admin-servers
aaa accounting network default start-stop group aaa-admin-servers
aaa accounting connection default start-stop group aaa-admin-servers
aaa accounting system default start-stop group aaa-admin-servers
enable secret <password>
!
clock timezone EST -5
clock summer-time EDT recurring
clock calendar-valid
vtp domain test.lab
vtp mode transparent
ip subnet-zero
no ip source-route
```

```
no ip gratuitous-arps
ip icmp rate-limit unreachable 1000
ip flow-cache feature-accelerate
!
!
ip tcp synwait-time 10
ip domain-name test.lab
ip name-server 10.1.200.97
ip dhcp relay information option
!
no ip bootp server
ip ssh time-out 10
ip ssh authentication-retries 2
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
mls qos
!
!
spanning-tree loopguard default
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree portfast bpdufilter default
spanning-tree extend system-id
no spanning-tree vlan 1-5,7-9,11-19,21-100,102-1001
spanning-tree vlan 6,10,20,101 priority 24576
spanning-tree vlan 6,10,20,101 forward-time 7
spanning-tree vlan 6,10,20,101 max-age 10
!
redundancy
 mode rpr-plus
 main-cpu
  auto-sync running-config
  auto-sync standard
!
mac access-list extended mac-any-any
  permit any any
!
!
vlan access-map ipphone-vacl-map 10
 match ip address ipphone-permits
 action forward
vlan access-map ipphone-vacl-map 20
 match ip address ipphone-no-log
 action drop
vlan access-map ipphone-vacl-map 30
 match ip address ip-any-any
 action drop log
vlan access-map ipphone-vacl-map 40
 match mac address mac-any-any
 action drop
vlan access-map ipphone-vacl-map 50
 match ipx address ipx-any-any
 action drop
!
```

```
vlan access-map server-vacl-map 10
 match ip address intraserver-permits
 action forward
vlan access-map server-vacl-map 20
 match ip address intraserver-any-any
 action drop log
vlan access-map server-vacl-map 30
 match ip address server-permits-in
 action forward
vlan access-map server-vacl-map 40
 match ip address server-permits-out
 action forward
vlan access-map server-vacl-map 50
 match ip address ip-any-any
 action drop log
vlan access-map server-vacl-map 60
 match mac address mac-any-any
 action drop
vlan access-map server-vacl-map 70
 match ipx address ipx-any-any
 action drop
!
vlan access-map management-vacl-map 10
 match ip address management-permits
 action forward
vlan access-map management-vacl-map 20
 match ip address ip-any-any
 action drop log
vlan access-map management-vacl-map 30
 match mac address mac-any-any
 action drop
vlan access-map management-vacl-map 40
 match ipx address ipx-any-any
 action drop
!
vlan filter management-vacl-map vlan-list 6
vlan filter ipphone-vacl-map vlan-list 101
vlan filter server-vacl-map vlan-list 200
!
vlan 6
 name MANAGEMENT-SUBNET
!
vlan 10
 name NET10-SUBNET
!
vlan 20
 name NET20-SUBNET
!
vlan 101
 name IP-PHONE-SUBNET
!
vlan 200
 name SERVERS-PRIVATE-PRIMARY
  private-vlan primary
  private-vlan association 201
!
```

```
vlan 201
 name SERVERS-PRIVATE-SECONDARY
  private-vlan isolated
!
vlan 996
 name CORE-LAYER-SUBNET
!
vlan 997
 name ***BIT-BUCKET-for-2nd-Trunk***
!
vlan 998
 name ***BIT-BUCKET-for-1st-Trunk***
!
vlan 999
 name ***BIT-BUCKET-for-unused-ports**
!
!
interface Loopback0
 ip address 10.0.0.121 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet1/1
 description TRUNK to Cat122
 no ip address
 mls qos trust dscp
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 996
 switchport trunk allowed vlan 6,10,20,101,200,201,996
 switchport mode trunk
 switchport nonegotiate
 no cdp enable
 spanning-tree bpdufilter disable
 spanning-tree bpduguard disable
 spanning-tree guard none
!
interface GigabitEthernet1/2
 description *** UNUSED Port ***
 no ip address
 shutdown
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport port-security
 storm-control broadcast level 0.00
```

```
 storm-control multicast level 0.00
 storm-control unicast level 0.00
 dot1x port-control force-unauthorized
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/1
 description SERVER CallManager
 no ip address
 mls qos trust dscp
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode private-vlan host
 switchport nonegotiate
 switchport private-vlan host-association 200 201
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/2
 description SERVER Internal E-Mail (SMTP)
 no ip address
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode private-vlan host
 switchport nonegotiate
 switchport private-vlan host-association 200 201
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/3
 description SERVER Internal Domain Name (DNS)
 no ip address
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode private-vlan host
 switchport nonegotiate
 switchport private-vlan host-association 200 201
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
```

```
!
interface GigabitEthernet6/4
 description SERVER Internal File (FTP)
 no ip address
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode private-vlan host
 switchport nonegotiate
 switchport private-vlan host-association 200 201
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/5
 description SERVER Internal Web (HTTP)
 no ip address
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode private-vlan host
 switchport nonegotiate
 switchport private-vlan host-association 200 201
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/6
 description SERVER Network Time Source-Primary (NTP)
 no ip address
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode private-vlan promiscuous
 switchport nonegotiate
 switchport private-vlan mapping 200 201
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/7
 description *** UNUSED Port ***
 no ip address
 shutdown
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
```

```
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport port-security
 storm-control broadcast level 0.00
 storm-control multicast level 0.00
 storm-control unicast level 0.00
 dot1x port-control force-unauthorized
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/8
 description *** UNUSED Port ***
 no ip address
 shutdown
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport port-security
 storm-control broadcast level 0.00
 storm-control multicast level 0.00
 storm-control unicast level 0.00
 dot1x port-control force-unauthorized
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/9
 description SERVER Management Logs (SysLog)
 no ip address
 switchport
 switchport access vlan 6
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport port-security
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/10
 description SERVER Management Authentication (RADIUS)
 no ip address
 switchport
 switchport access vlan 6
```

```
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 5
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/11
 description HOST Management (SNMPv3)
 no ip address
 switchport
 switchport access vlan 6
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport port-security
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/12
 description HOST Management (SSL, SSH, etc.)
 no ip address
 switchport
 switchport access vlan 6
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport port-security
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/13
 description *** UNUSED Port ***
 no ip address
 shutdown
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport port-security
 storm-control broadcast level 0.00
```

```
 storm-control multicast level 0.00
 storm-control unicast level 0.00
 dot1x port-control force-unauthorized
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/14
 description *** UNUSED Port ***
 no ip address
 shutdown
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport port-security
 storm-control broadcast level 0.00
 storm-control multicast level 0.00
 storm-control unicast level 0.00
 dot1x port-control force-unauthorized
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface GigabitEthernet6/15
 description TRUNK to Cat142
 no ip address
 mls qos trust dscp
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 997
 switchport trunk allowed vlan 6,10,20,101
 switchport mode trunk
 switchport nonegotiate
 no cdp enable
 spanning-tree bpdufilter disable
 spanning-tree bpduguard disable
 spanning-tree guard none
!
interface GigabitEthernet6/16
 description TRUNK to Cat141
 no ip address
 mls qos trust dscp
 switchport
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 998
 switchport trunk allowed vlan 6,10,20,101
 switchport mode trunk
```

```
 switchport nonegotiate
 no cdp enable
 spanning-tree bpdufilter disable
 spanning-tree bpduguard disable
 spanning-tree guard none
!
interface Vlan1
 description *** DEFAULT VLAN - Do NOT Use! ***
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 shutdown
 ntp disable
!
interface Vlan6
 description Layer 3 Interface to Management Subnet
 ip address 10.1.6.121 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
!
interface Vlan10
 description Layer 3 Interface to Net10 Subnet
 ip address 10.1.10.121 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 ntp disable
!
interface Vlan20
 description Layer 3 Interface to Net20 Subnet
 ip address 10.1.20.121 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 ntp disable
!
interface Vlan101
 description Layer 3 Interface to IP Phone Subnet
 ip address 10.1.101.121 255.255.255.0
 ip helper-address 10.1.200.99
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 ntp disable
!
```

```
interface Vlan200
 description Layer 3 Interface to Internal Servers
 ip address 10.1.200.121 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 private-vlan mapping 201
!
interface Vlan996
 description Layer 3 Interface to Core Subnet
 ip address 10.1.250.121 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 ntp disable
!
interface Vlan997
 description *** BIT BUCKET for 2nd Trunk ***
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 shutdown
 ntp disable
!
interface Vlan998
 description *** BIT BUCKET for 1st Trunk ***
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 shutdown
 ntp disable
!
interface Vlan999
 description *** BIT BUCKET for unused ports ***
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 shutdown
 ntp disable

ip classless
ip route 0.0.0.0 0.0.0.0 10.1.250.122
ip route 0.0.0.0 0.0.0.0 Vlan996
```

```
no ip http server
ip http access-class 1
ip http authentication aaa
no ip http secure-server

ip access-list extended intraserver-any-any
 remark Everything with Source AND Destination in VLAN200
 permit ip 10.1.200.0 0.0.0.255 10.1.200.0 0.0.0.255
 remark .
ip access-list extended intraserver-permits
 remark Allow NTP to the VLAN200 Servers
 permit udp host 10.1.200.94 eq ntp 10.1.200.0 0.0.0.255 eq ntp
 remark Allow NTP from the VLAN200 Servers
 permit udp 10.1.200.0 0.0.0.255 eq ntp host 10.1.200.94 eq ntp
 remark .
ip access-list extended ip-any-any
 remark Everything IP
 permit ip any any
 remark .
ip access-list extended ipphone-no-log
 remark Known IPPhone packets to drop without logging
 permit tcp 10.1.101.0 0.0.0.255 10.1.101.0 0.0.0.255 eq 2000
 remark .
ip access-list extended ipphone-permits
 remark -Allow DHCP BOOTP from IPPhones
 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
 remark -Allow DHCP BOOTP to IPPhone subnets (through ip helper-address)
 permit udp host 10.1.101.121 eq bootps host 255.255.255.255 eq bootpc
 permit udp host 10.1.101.122 eq bootps host 255.255.255.255 eq bootpc
 remark -Allow DNS lookup requests from IPPhones to CCM
 permit udp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99 eq domain
 remark -Allow DNS lookup replies from CCM to IPPhones
 permit udp host 10.1.200.99 eq domain 10.1.101.0 0.0.0.255 gt 32767
 remark -Allow TFTP request from IPPhones to CCM
 permit udp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99 eq tftp
 remark -Open (too many) ports for TFTP transfer from CCM to IPPhones
 permit udp host 10.1.200.99 10.1.101.0 0.0.0.255 gt 32767
 remark -Open (too many) ports for TFTP Acks from IPPhones to CCM
 permit udp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99
 remark -Allow Skinny from IPPhones to CCM
 permit tcp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99 range 2000 2002
dscp af31
 permit tcp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99 range 2000 2002
rst dscp default
 remark -Allow Skinny from CCM to IPPhones
 permit tcp host 10.1.200.99 range 2000 2002 10.1.101.0 0.0.0.255 gt 32767
dscp af31
 permit tcp host 10.1.200.99 range 2000 2002 10.1.101.0 0.0.0.255 gt 32767
rst dscp default
 remark -Allow RTP Voice between IPPhones
 permit udp 10.1.101.0 0.0.0.255 range 16384 32767 10.1.101.0 0.0.0.255 range
16384 32767 dscp ef
 remark -Allow HTTP management of IPPhones from CCM
 permit tcp host 10.1.200.99 10.1.101.0 0.0.0.255 eq www
 remark -Allow HTTP management replies from IPPhones to CCM
 permit tcp 10.1.101.0 0.0.0.255 eq www host 10.1.200.99 established
 remark -Allow ICMPs to IPPhones from CCM
```

```
 permit icmp host 10.1.200.99 10.1.101.0 0.0.0.255
 remark -Allow ICMPs from IPPhones to CCM
 permit icmp 10.1.101.0 0.0.0.255 host 10.1.200.99
 remark .
ip access-list extended management-permits
 remark Allowable MANAGEMENT Subnet Permits
 permit ip 10.1.6.0 0.0.0.255 10.1.6.0 0.0.0.255
 remark .
ip access-list extended server-permits-in
 remark HTTP Server Permits
 permit tcp 10.1.20.0 0.0.0.255 host 10.1.200.95 eq www
 permit tcp 10.1.20.0 0.0.0.255 host 10.1.200.95 eq 443
 remark FTP Server Permits
 permit tcp 10.1.10.0 0.0.0.255 host 10.1.200.96 eq ftp-data
 permit tcp 10.1.10.0 0.0.0.255 host 10.1.200.96 eq ftp
 remark DNS Server Permits
 permit udp 10.1.10.0 0.0.0.255 host 10.1.200.97 eq domain
 permit udp 10.1.20.0 0.0.0.255 host 10.1.200.97 eq domain
 permit tcp 10.1.10.0 0.0.0.255 host 10.1.200.97 eq domain
 permit tcp 10.1.20.0 0.0.0.255 host 10.1.200.97 eq domain
 remark SMTP Server Permits
 permit tcp 10.1.10.0 0.0.0.255 host 10.1.200.98 eq smtp
 permit tcp 10.1.20.0 0.0.0.255 host 10.1.200.98 eq smtp
 remark -Allow DHCP BOOTP from IPPhone subnets (through ip helper-address)
 permit udp host 10.1.101.121 eq bootpc host 10.1.200.99 eq bootps
 permit udp host 10.1.101.122 eq bootpc host 10.1.200.99 eq bootps
 remark -Allow DNS lookup requests to CCM
 permit udp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99 eq domain
 remark -Allow TFTP request from IPPhones to CCM
 permit udp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99 eq tftp
 remark -Open (too many) ports for TFTP Acks from IPPhones to CCM
 permit udp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99
 remark -Allow Skinny from IPPhones to CCM
 permit tcp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99 range 2000 2002
dscp af31
 permit tcp 10.1.101.0 0.0.0.255 gt 32767 host 10.1.200.99 range 2000 2002
rst dscp default
 remark -Allow HTTP management replies from IPPhones to CCM
 permit tcp 10.1.101.0 0.0.0.255 eq www host 10.1.200.99 established
 remark -Allow ICMPs from IPPhones to CCM
 permit icmp 10.1.101.0 0.0.0.255 host 10.1.200.99
 remark .
ip access-list extended server-permits-out
 remark HTTP Server Permits
 permit tcp host 10.1.200.95 eq www 10.1.20.0 0.0.0.255
 permit tcp host 10.1.200.95 eq 443 10.1.20.0 0.0.0.255
 remark FTP Server Permits
 permit tcp host 10.1.200.96 eq ftp-data 10.1.10.0 0.0.0.255
 permit tcp host 10.1.200.96 eq ftp 10.1.10.0 0.0.0.255
 remark DNS Server Permits
 permit udp host 10.1.200.97 eq domain 10.1.10.0 0.0.0.255
 permit udp host 10.1.200.97 eq domain 10.1.20.0 0.0.0.255
 permit tcp host 10.1.200.97 eq domain 10.1.10.0 0.0.0.255
 permit tcp host 10.1.200.97 eq domain 10.1.20.0 0.0.0.255
 remark SMTP Server Permits
 permit tcp host 10.1.200.98 eq smtp 10.1.10.0 0.0.0.255
 permit tcp host 10.1.200.98 eq smtp 10.1.20.0 0.0.0.255
```

```
 remark -Allow DHCP BOOTP to IPPhone subnets (through ip helper-address)
 permit udp host 10.1.200.99 eq bootps host 10.1.101.121 eq bootps
 permit udp host 10.1.200.99 eq bootps host 10.1.101.122 eq bootps
 remark -Allow DNS lookup replies to IPPhone subnets
 permit udp host 10.1.200.99 eq domain 10.1.101.0 0.0.0.255 gt 32767
 remark -Open (too many) ports for TFTP transfer from CCM to IPPhones
 permit udp host 10.1.200.99 10.1.101.0 0.0.0.255 gt 32767
 remark -Allow Skinny from CCM to IPPhones
 permit tcp host 10.1.200.99 range 2000 2002 10.1.101.0 0.0.0.255 gt 32767
dscp af31
 permit tcp host 10.1.200.99 range 2000 2002 10.1.101.0 0.0.0.255 gt 32767
rst dscp default
 remark -Allow HTTP management of IPPhones from CCM
 permit tcp host 10.1.200.99 10.1.101.0 0.0.0.255 eq www
 remark -Allow ICMPs from CCM to IPPhones
 permit icmp host 10.1.200.99 10.1.101.0 0.0.0.255
 remark .

logging history notifications
logging trap informational
logging facility local0
logging 10.1.6.89

no access-list 1
access-list 1 remark Permit access from ADMINISTRATION addresses
access-list 1 permit 10.1.6.1 log
access-list 1 permit 10.1.6.2 log
access-list 1 deny   any log

no access-list 2
access-list 2 remark Permit access from Master NTP Server addresses
access-list 2 permit 10.1.200.94
access-list 2 deny   any log

no access-list 3
access-list 3 remark Permit access from Client NTP Server addresses
access-list 3 permit 10.1.6.141
access-list 3 deny   any log

no access-list 4
access-list 4 remark Deny access from any address
access-list 4 deny   any log

no cdp run

tacacs-server host 10.1.6.88 key lablablab
tacacs-server directed-request

banner exec #
Connected to $(hostname).$(domain) on $(line-desc) $(line).
Use of this system constitutes your consent to monitoring.
#

banner login #
Session established with AUTHENTICATION Servers.
Provide the following tokens for User Access Verification
#
```

```
banner motd #

                                NOTICE TO USERS

================================================================================
   This is an official computer system and is the property of the
   ORGANIZATION.  It is for authorized users only.  Unauthorized users are
   prohibited.  Users (authorized or unauthorized) have no explicit or
   implicit expectation of privacy.  Any or all uses of this system may be
   subject to one or more of the following actions:  interception,
   monitoring, recording, auditing, inspection and disclosing to security
   personnel and law enforcement personnel, as well as authorized officials
   of other agencies, both domestic and foreign.  By using this system, the
   user consents to these actions.  Unauthorized or improper use of this
   system may result in administrative disciplinary action and civil and
   criminal penalties.  By accessing this system you indicate your awareness
   of and consent to these terms and conditions of use.  Discontinue access
   immediately if you do not agree to the conditions stated in this notice.
================================================================================

Contacting AUTHENTICATION Servers...#

banner prompt-timeout #
Session timed-out with AUTHENTICATION Servers. Goodbye!#

line con 0
 exec-timeout 9 0
 privilege level 0
 password <password>
 authorization commands 15 aaa-config
 logging synchronous
 login authentication aaa-fallback
 length 50
 notify
 transport preferred none
 transport output ssh
line vty 0 4
 access-class 1 in
 exec-timeout 9 0
 privilege level 0
 password <password>
 transport input ssh
 transport output none
line vty 5 15
 access-class 4 in
 exec-timeout 0 10
 privilege level 0
 password <password>
 no exec
 transport input none
 transport output none
```

```
scheduler allocate 4000 400
ntp authentication-key 123 md5 <key>
ntp authentication-key 124 md5 <key>
ntp authenticate
ntp trusted-key 123
ntp access-group peer 2
ntp access-group serve-only 3
ntp master 2
ntp server 10.1.200.94 key 123 prefer
end
```

## 15.2 Cisco Catalyst 3550 Switch

```
!============================================================================
! 3550 - Access Layer
!============================================================================


version 12.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname Cat141
!
logging buffered 64000 notifications
aaa new-model
aaa group server tacacs+ aaa-admin-servers
 server 10.1.6.88
!
aaa group server radius aaa-host-servers
 server 10.1.6.88 auth-port 1812 acct-port 1813
!
aaa authentication banner ^CAccessing AAA-Servers^C
aaa authentication fail-message ^CAAA Authentication FAILED.^C
aaa authentication login default group aaa-admin-servers
aaa authentication login aaa-fallback group aaa-admin-servers enable
aaa authentication dot1x default group aaa-host-servers
aaa authorization exec default group aaa-admin-servers
aaa authorization commands 15 default group aaa-admin-servers
aaa authorization commands 15 aaa-config group aaa-admin-servers if-
authenticated
aaa authorization network default if-authenticated
aaa authorization configuration default group aaa-admin-servers
aaa accounting suppress null-username
aaa accounting send stop-record authentication failure
aaa accounting delay-start
aaa accounting nested
aaa accounting update periodic 1440
aaa accounting exec default start-stop group aaa-admin-servers
aaa accounting commands 15 default start-stop group aaa-admin-servers
aaa accounting network default start-stop group aaa-admin-servers
aaa accounting connection default start-stop group aaa-admin-servers
aaa accounting system default start-stop group aaa-admin-servers
enable secret <password>
!
clock timezone EST -5
clock summer-time EDT recurring
ip subnet-zero
no ip source-route
no ip gratuitous-arps
ip icmp rate-limit unreachable 1000
```

```
ip dhcp relay information option
!
ip tcp synwait-time 10
no ip domain-lookup
ip domain-name test.lab
ip flow-cache feature-accelerate
ip ssh time-out 10
ip ssh authentication-retries 3
vtp domain test.lab
vtp mode transparent
mls qos
!
!
spanning-tree mode pvst
spanning-tree loopguard default
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree portfast bpdufilter default
spanning-tree extend system-id
no spanning-tree vlan 1
no spanning-tree vlan 995
no spanning-tree vlan 998
no spanning-tree vlan 999
!
mac access-list extended mac-device-list
 permit host 0000.0101.0011 any
 permit host 0000.0101.0012 any
 permit host 0000.0101.0013 any
 permit host 0000.0101.0014 any
 permit host 0000.0010.0003 any
 permit host 0000.0020.0005 any
!
!
vlan 5
!
vlan 6
 name ADMINISTRATION-VLAN
!
vlan 10
 name NET10-VLAN
!
vlan 20
 name NET20-VLAN
!
vlan 101
 name IP-PHONE-SUBNET
!
vlan 995
 name **BIT-BUCKET-trunk-with-Cat122**
!
vlan 998
 name **BIT-BUCKET-trunk-with-Cat121**
!
vlan 999
 name ***BIT-BUCKET-for-unused-ports**
!
!
```

```
interface Null0
 no ip unreachables
!
interface FastEthernet0/1
 description Host 10.1.10.3
 switchport access vlan 10
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 no ip address
 ip access-group ip-device-list in
 mls qos cos override
 dot1x port-control auto
 dot1x guest-vlan 999
 dot1x host-mode multi-host
 mac access-group mac-device-list in
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface FastEthernet0/2
 description IP PHONE x1011
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport voice vlan 101
 switchport port-security
 switchport port-security maximum 2
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 no ip address
 ip access-group ip-device-list in
 mls qos trust device cisco-phone
 mls qos trust dscp
 dot1x port-control auto
 dot1x guest-vlan 999
 dot1x host-mode multi-host
 mac access-group mac-device-list in
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
```

```
interface FastEthernet0/3
 description IP PHONE x1012
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport voice vlan 101
 switchport port-security
 switchport port-security maximum 2
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 no ip address
 ip access-group ip-device-list in
 mls qos trust device cisco-phone
 mls qos trust dscp
 dot1x port-control auto
 dot1x guest-vlan 999
 dot1x host-mode multi-host
 mac access-group mac-device-list in
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface FastEthernet0/4
 description IP PHONE x1013
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport voice vlan 101
 switchport port-security
 switchport port-security maximum 2
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 no ip address
 ip access-group ip-device-list in
 mls qos trust device cisco-phone
 mls qos trust dscp
 dot1x port-control auto
 dot1x guest-vlan 999
 dot1x host-mode multi-host
 mac access-group mac-device-list in
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
```

```
interface FastEthernet0/5
 description IP PHONE x1014 & HOST 10.1.20.5
 switchport access vlan 20
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 20
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport voice vlan 101
 switchport port-security
 switchport port-security maximum 3
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 no ip address
 ip access-group ip-device-list in
 mls qos trust device cisco-phone
 mls qos trust dscp
 dot1x port-control auto
 dot1x guest-vlan 999
 dot1x reauthentication
 mac access-group mac-device-list in
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
!
interface FastEthernet0/6
 description *** UNUSED Port ***
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 no ip address
 ip access-group ip-device-list in
 shutdown
 mls qos cos override
 storm-control broadcast level 0.00
 storm-control multicast level 0.00
 storm-control unicast level 0.00
 dot1x port-control force-unauthorized
 dot1x guest-vlan 999
 dot1x host-mode multi-host
 mac access-group mac-device-list in
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
```

```
!
interface FastEthernet0/23
 description TRUNK to Cat122
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 995
 switchport trunk allowed vlan 6,10,20,101
 switchport mode trunk
 switchport nonegotiate
 no ip address
 mls qos trust dscp
 no cdp enable
 spanning-tree portfast disable
 spanning-tree bpdufilter disable
 spanning-tree bpduguard disable
 spanning-tree guard none
!
interface FastEthernet0/24
 description TRUNK to Cat121
 switchport access vlan 999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 998
 switchport trunk allowed vlan 6,10,20,101
 switchport mode trunk
 switchport nonegotiate
 no ip address
 mls qos trust dscp
 spanning-tree portfast disable
 spanning-tree bpdufilter disable
 spanning-tree bpduguard disable
 spanning-tree guard none
!
interface Vlan1
 description *** DEFAULT VLAN - Do NOT Use! ***
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 shutdown
 ntp disable
!
interface Vlan6
 description ADMINISTRATION VLAN
 ip address 10.1.6.141 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
!
interface Vlan995
 description **BIT-BUCKET-trunk-with-Cat122**
 no ip address
 no ip redirects
 no ip unreachables
```

```
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 shutdown
 ntp disable
!
interface Vlan998
 description **BIT-BUCKET-trunk-with-Cat121**
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 shutdown
 ntp disable
!
interface Vlan999
 description **BIT BUCKET for unused ports**
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 shutdown
 ntp disable
!
ip default-gateway 10.1.6.121
ip classless
no ip http server
!
ip access-list extended ip-device-list
 permit ip host 10.1.101.11 any
 permit ip host 10.1.101.12 any
 permit ip host 10.1.101.13 any
 permit ip host 10.1.101.14 any
 permit ip host 10.1.10.3 any
 permit ip host 10.1.20.5 any
 deny   tcp any range 0 65535 any range 0 65535 log-input
 deny   udp any range 0 65535 any range 0 65535 log-input
 deny   ip any any log-input
!
!
logging history warnings
logging trap informational
logging facility local0
logging 10.1.6.89

no access-list 1
access-list 1 remark Permit access from ADMINISTRATION addresses
access-list 1 permit 10.1.6.1 log
access-list 1 permit 10.1.6.2 log
access-list 1 deny   any log
```

```
no access-list 2
access-list 2 remark Permit access from NTP Server addresses
access-list 2 permit 10.1.6.121
access-list 2 deny   any log
!
no access-list 3
access-list 3 remark Deny access from any address
access-list 3 deny   any log

tacacs-server host 10.1.6.88 key <key>
radius-server host 10.1.6.88 auth-port 1812 acct-port 1813
radius-server key <key>

banner exec #

Connected to $(hostname).$(domain) on $(line-desc) $(line).
Use of this system constitutes your consent to monitoring.

#

banner login #
Session established with AUTHENTICATION Servers.

Provide the following tokens for User Access Verification
#

banner motd #

                                NOTICE TO USERS

===============================================================================
   This is an official computer system and is the property of the
   ORGANIZATION.  It is for authorized users only.  Unauthorized users are
   prohibited.  Users (authorized or unauthorized) have no explicit or
   implicit expectation of privacy.  Any or all uses of this system may be
   subject to one or more of the following actions:  interception,
   monitoring, recording, auditing, inspection and disclosing to security
   personnel and law enforcement personnel, as well as authorized officials
   of other agencies, both domestic and foreign.  By using this system, the
   user consents to these actions.  Unauthorized or improper use of this
   system may result in administrative disciplinary action and civil and
   criminal penalties.  By accessing this system you indicate your awareness
   of and consent to these terms and conditions of use.  Discontinue access
   immediately if you do not agree to the conditions stated in this notice.
===============================================================================

Contacting AUTHENTICATION Servers...#

banner prompt-timeout #
Session timed-out with AUTHENTICATION Servers. Goodbye!#
!
line con 0
 exec-timeout 9 0
 privilege level 0
 password <password>
 authorization commands 15 aaa-config
 logging synchronous
```

```
 login authentication aaa-fallback
 length 50
 notify
 transport preferred none
line vty 0 4
 access-class 1 in
 exec-timeout 9 0
 privilege level 0
 password <password>
line vty 5 15
 access-class 3 in
 exec-timeout 0 10
 privilege level 0
 password <password>
 no exec
!
scheduler interval 500
ntp authentication-key 124 md5 <key>
ntp authenticate
ntp trusted-key 124
ntp access-group peer 2
ntp server 10.1.6.121 key 124 prefer
end
```

# 16 Acronyms and Glossary

**AAA: Authentication, Authorization and Accounting**
AAA is Cisco's framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

**ACL: Access Control List**
An ACL is a filter on a network system that determines whether or not a network connection will be allowed through or to the network system.

**ARP: Address Resolution Protocol**
ARP is a TCP/IP protocol used to obtain a node's physical address. A client station broadcasts an ARP request onto the network with the IP address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted. ARP returns the Layer 2 address for a Layer 3 address.

**BPDU: Bridge Protocol Data Unit**
A BPDU is a data message that is exchanged across the switches within an extended LAN that uses an STP topology.

**CAM: Content Addressable Memory**
CAM is a kind of memory that includes comparison logic with each bit of memory. CAM can operate as a data parallel processor. In a switch, CAM is often used for the MAC address table.

**CDP: Cisco Discovery Protocol**
CDP is a Layer 2 protocol that runs on all Cisco products (e.g., routers, switches and access servers). Using CDP, an administrator can view information about all the Cisco systems on a given subnet.

**DHCP: Dynamic Host Configuration Protocol**
DHCP is a protocol that automatically assigns IP addresses to client stations logging onto a TCP/IP network. It eliminates having to manually assign IP addresses.

**DMZ: Demilitarized Zone**
A DMZ is a small subnet that sits between a trusted internal network, such as a government agency LAN, and an untrusted external network, such as the Internet. Typically, the DMZ contains publicly accessible systems (e.g., Web servers, file servers, mail servers and DNS servers). It usually is located at the perimeter of the trusted internal network.

**DNS: Domain Name System**
DNS is a protocol that translates domain names into IP addresses using DNS servers. Each DNS server maintains a database of domain names (hostnames) and their corresponding IP addresses.

**DTP: Dynamic Trunking Protocol**
DTP is a protocol that provides the ability to negotiate the trunking method with another network system.

**FTP: File Transfer Protocol**
FTP is a form of file transfer used on computer networks. It uses TCP as a transport mechanism and port 21 (control connections) and port 20 (data connections) by default. It can be configure with usernames and passwords for identification and authentication.

**FWSM: Firewall Services Module**
The FWSM is a stateful inspection firewall capability based on Cisco PIX technology. The FWSM creates a connection table entry for each session flow. The FWSM controls all inbound and outbound traffic by applying the security policy to these connection table entries.

**HTTP: Hyper Text Transfer Protocol**
HTTP is the protocol used by web browsers and web servers to transfer files. It uses TCP as a transport mechanism and port 80 by default. It can be configure with usernames and passwords for identification and authentication.

**ICMP: Internet Control Message Protocol**
ICMP is a TCP/IP protocol used to send error and control messages. For example, a switch uses ICMP to notify the sender that its destination node is not available. A ping utility sends ICMP echo requests to verify the status of an IP address.

**IDSM: Intrusion Detection System Service Module**
The IDSM passively monitors network segments and traffic for malicious attacks. The IDSM is a signature-based network intrusion detection capability that inspects copies of packets thru either a VACL capture or SPAN configuration.

**IEEE: Institute of Electrical and Electronics Engineers**
The IEEE is one of the world's largest technical professional societies. The institute fosters the development of standards that often become national and international standards.

**IOS: Internetworking Operating System**
IOS is the operating system used on many of Cisco's routers and Catalyst switches.

**IP: Internet Protocol**
IP is one of the main protocols used on computer networks at Layer 3 of the OSI RM. IP, a connectionless protocol, is the method by which data (e.g., packets) is sent from one computer to another on the Internet. IP focuses only on the delivery of the packets in any order and relies on other mechanisms (e.g., TCP) to put the packets back in the proper order.

**ISL: Inter-Switch Link**
ISL is a Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.

**KDC: Key Distribution Center**
KDC is a system that distributes and manages shared and private keys for authentication.

**LAN: Local Area Network**
A LAN is a computer network that spans a relatively small area. Most LANs are confined to a single building or a group of buildings.

**MAC: Media Access Control**
MAC relates to the hardware address that uniquely identifies each node on a network at Layer 2 of the OSI RM.

**MGCP: Media Gateway Control Protocol**
MGCP is a VoIP protocol.

**MIB: Management Information Base**
MIB is a data structure used by SNMP that defines what is obtainable from a system and what can be controlled.

**MLS: Multi-Layer Switching**
MLS provides hardware-based Layer 3 switching. IP MLS offloads the processor-intensive packet routing from network routers by switching unicast IP data packet flows between IP subnets using application-specific integrated circuit switching hardware. Standard routing protocols, such as OSPF, EIGRP, RIP and IS-IS are used for route determination.

**MPLS: Multi-Protocol Label Switching**
MPLS is a standard for routing packets over the Internet from the IETF. MPLS uses labels, or tags, that contain forwarding information, which are attached to IP packets by a router that sits at the edge of the network known as a label edge router (LER). The LERs perform the complex packet analysis and classification, but do it only once before the packet enters the core of the network. The routers within the core, known as label switch routers (LSRs), examine the label quickly and forward the packet without having to make any forwarding decisions. The receiving LER removes the label.

**NTP: Network Time Protocol**
NTP is a protocol used to synchronize the clock in a computer with a trusted timeserver. It uses UDP as a transport mechanism and port 123 by default.

**OSI RM: Open System Interconnection Reference Model**
The OSI RM describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI RM is a conceptual model composed of seven layers, each layer specifying particular network functions. Switches typically work at Layer 2 (Data link); more advanced switches work at Layer 3 (Network) and at Layer 4 (Transport).

**PACL: Port Access Control List**
A PACL is applied on Layer 2 interfaces for inbound traffic and filters all packets regardless of any VLAN associations that might exist. A PACL will filter on all VLANs present when applied to a trunk port.

**PAD: Packet Assembler/Disassembler**
A PAD is a functional unit that enables data terminal equipment not equipped for packet switching to access a packet-switched network.

**PVLAN: Private VLAN**
A PVLAN provides Layer 2 isolation between hosts within a common subnet.

**QoS: Quality of Service**
QoS refers to the mechanisms in the network software that make the actual determination of which packets have priority. CoS (class of service) refers to feature sets, or groups of services, which are assigned to users based on company policy. If a feature set includes priority transmission, then CoS is implemented in QoS functions within the routers and switches in the network.

**RACL: Router Access Control List**
A RACL can restrict packets into or out of a given Layer 3 interface. A RACL is configured and applied identically to a router ACL, except a RACL is applied to a VLAN interface.

**RADIUS: Remote Authentication Dial-in User Service**
RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

**RAM: Random Access Memory**
RAM is a type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the previous bytes.

**RSA: Rivest, Shamir, Adleman**
RSA is an encryption and authentication system that uses public key cryptography. RSA was developed by Ron Rivest, Adi Shamir and Leonard Adleman.

**SCCP: Skinny Client Control Protocol**
SCCP is a VoIP protocol.

**SIP: Session Initiation Protocol**
SIP is a VoIP protocol.

**SNAC: System and Network Attack Center**
The SNAC is a Department of Defense office dedicated to network security research and evaluations.

**SNMP: Simple Network Management Protocol**
SNMP is a widely used network monitoring and control protocol. Data are passed from SNMP agents, which are hardware and/or software processes reporting activity in each network system (e.g., router, switch) to the workstation console used to oversee the network. The agents return information contained in a MIB. It uses UDP as a transport mechanism and port 161 (SNMP polls) and port 162 (SNMP traps) by default.

**SSH: Secure Shell**
SSH is a Unix-based command interface and protocol for securely getting access to a remote computer. It uses TCP as a transport mechanism and port 22 by default. It uses public key cryptography for both connection and authentication and uses encryption algorithms to protect connections to remote computers.

**STP: Spanning Tree Protocol**
STP is a Layer 2 protocol that is part of the IEEE 802.1 standard for MAC bridges. Using the spanning tree algorithm, STP provides path redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations.

**SVI: Switch Virtual Interface**
An SVI represents a VLAN of switch ports as one interface to the routing or bridging function in the system.

**TACACS+: Terminal Access Controller Access Control System +**
TACACS+ is an authentication protocol that allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network. TACACS+ is a Cisco proprietary protocol based on TACACS, a standards-based authentication protocol.

**TCP: Transmission Control Protocol**
TCP is one of the main protocols used on computer networks at Layer 4 of the OSI RM. TCP, a connection-oriented protocol, enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data.

**TFTP: Trivial File Transfer Protocol**
TFTP is a simple form of file transfer. It uses UDP as a transport mechanism and port 69 by default. It provides no security features.

**UDLD: Unidirectional Link Detection**
UDLD is a Layer 2 protocol that works with Layer 1 mechanisms to determine the physical status of a link. At Layer 1, auto-negotiation takes care of physical signaling and fault detection. UDLD performs tasks that auto-negotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When the administrator enables both auto-negotiation and UDLD, Layers 1 and 2 detections work together to prevent physical and logical unidirectional connections. Also, these detections work together to prevent the malfunctioning of other protocols.

**UDP: User Datagram Protocol**
UDP is one of the main protocols used on computer networks at Layer 4 of the OSI RM. UDP, a connectionless protocol, provides very few error recovery services for a connection between two hosts.

**VACL: VLAN Access Control List**
A VACL can restrict packets into, through or out of a given VLAN. Apply a VACL to filter VLAN traffic.

**VLAN: Virtual Local Area Network**
A VLAN is a group of systems on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same medium (e.g., Ethernet), when in fact they are located on a number of different LAN segments.

**VMPS: VLAN Management Policy Server**
VMPS allows an administrator to assign switch ports to VLANs dynamically, based on the source MAC address of the system connected to the port. When the administrator moves a host from a port on one switch in the network to a port on another switch in the network, the switch assigns the new port to the proper VLAN for that host dynamically.

**VoIP: Voice over Internet Protocol**
VoIP is the capability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network.

**VPNSM: Virtual Private Network Services Module**
The VPNSM feature enables both site-to-site and remote-access IPSEC VPN capability. The VPNSM adds hardware-based encryption, authentication and integrity to network services such as integrated voice, video and data.

**VTP: VLAN Trunking Protocol**
VTP is a Cisco-proprietary protocol that simplifies the administration of VLANs on a computer network. An administrator can configure a new VLAN on one VTP server, and then this VLAN is distributed through all switches in the VTP domain. This reduces the need to configure the same VLAN everywhere.

# 17 References

[1] @stake. Secure Use of VLANs: An @stake Security Assessment, August 2002. (Available at http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf)

[2] Cisco Systems. Catalyst 3550 Multilayer Switch Command Reference, 12.1(19)EA1. (Available at http://www.cisco.com/en/US/products/hw/switches/ps646/products_command_reference_book09186a00801cdef8.html)

[3] Cisco Systems. Cisco IOS Security Configuration Guide, Release 12.2. (Available at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/cc_ipsec.htm )

[4] Cisco Systems. Cisco Product Security Advisories and Notices. (Available at http://www.cisco.com/go/safe)

[5] Cisco Systems. Cisco SAFE: A Security Blueprint for Enterprise Networks. (Available at http://www.cisco.com/go/psirt)

[6] Cisco Systems. Firewall Services Module (FWSM). (Available at http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/ps4452/prodlit/fwsm_ds.htm http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/ps4452/index.shtml)

[7] Cisco Systems. Multi-Protocol Label Switching (MPLS). (Available at http://www.cisco.com/en/US/tech/tk436/tk428/tech_protocol_family_home.html http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800a3e69.shtml)

[8] Cisco Systems. Understanding Cisco IOS ACL Support – Cisco Catalyst 6500 Series Switches. (Available at http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00801609f6.html)

[9] Cisco Systems. Virtual LAN Security Best Practices. (Available at http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.htm)

[10] Cisco Systems. Virtual Private Network Services Module (VPNSM). (Available at http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/ps4221/index.shtml http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/ps4221/prodlit/vpnsm_ds.htm)

[11] NSA. Router Security Configuration Guide, Version 1.1b, 5 December 2003. (Available at http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf)

[12] Passmore, David, and Freeman, John. The Virtual LAN Technology Report, 1996. (Available at http://www.3com.com/nsc/200374.html)

[13] Taylor, David. "Are there Vulnerabilities in VLAN Implementations?" SANS Institute, July 2000. (Available at http://www.sans.org/resources/idfaq/vlan.php)

# 18 Cisco IOS Switch Security Checklist

The following is a general security checklist recommended by the SNAC for Cisco IOS switches at every layer (e.g., core, distribution, access) for every type of network traffic (e.g., data, voice, video).

- ✓ Include section on switches in network security policy.
- ✓ Control physical access to the switch to only authorized personnel.
- ✓ Install the latest stable version of the IOS on each switch.
- ✓ Create an "enable secret" password.
- ✓ Manage switches out-of-band (separated from data traffic). If out-of-band management is not feasible, then dedicate a separate VLAN number for in-band management.
- ✓ Set timeouts for sessions and configure privilege levels.
- ✓ Configure a banner to state that unauthorized access is prohibited.
- ✓ Disable unnecessary network services (e.g., tcp small servers, HTTP).
- ✓ Enable necessary network services and configure these services securely.
- ✓ Utilize SSH instead of telnet and set a strong password for SSH.
- ✓ If SNMP is necessary, set a strong community string for SNMP.
- ✓ Implement port security to limit access based on MAC address. Disable auto-trunking on ports.
- ✓ Utilize the switch's port mirroring capability for IDS access.
- ✓ Disable unused switch ports and assign them a VLAN number not in use.
- ✓ Assign trunk ports a native VLAN number that is not use by any other port.
- ✓ Limit the VLANs that can be transported over a trunk to only those that are necessary.
- ✓ Utilize static VLAN configuration.
- ✓ If possible, disable VTP. Otherwise, set the following for VTP: management domain, password and pruning. Then set VTP into transparent mode.
- ✓ Use access control lists where appropriate.
- ✓ Enable logging and send logs to a dedicated, secure log host.
- ✓ Configure logging to include accurate time information, using NTP and timestamps.
- ✓ Review logs for possible incidents and archive them in accordance with the security policy.
- ✓ Use AAA features for local and remote access to switch.
- ✓ Maintain the switch configuration file off-line and limit access to it to only authorized administrators. The configuration file should contain descriptive comments for the different settings to provide perspective.