



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

GIAC/GSNA

GIAC Systems and Network Auditor (GSNA)

Practical Assignment

Option #1, Version 3.0

The Cisco 3550 Intelligent Switch: An Auditor's Perspective.

Robert Winding

SANS 2003 New Orleans participant

© SANS Institute 2004, Author retains full rights.

1.	Research in Audit, Measurement Practice, and Control	3
1.1	System to be Audited	3
1.2	3550 Secure Configuration	7
1.3	Risks to the System	7
1.4	Current State of Practice	9
2.	Audit Checklist.....	11
3.	Audit.....	38
4.	Audit Report	69
4.1	Executive Summary	70
4.2	Audit Findings	71
4.3	Audit Recommendations	73
5.	References	76
6.	Appendix A – CIS RAT Example Audit Report	78
7.	Appendix B – CCSAT Example Audit Report	80

Summary

This practical is submitted in partial fulfillment of requirements for the GSNA Systems and Network Auditor certification. It examines a component of an enterprise IT architecture from an audit prospective. The component presented is a Cisco 3550 layer 2/3 switch. Switches, in larger organizations, are often relied upon to implement a layer of security as well as perform their traditional network distribution function. They have become fairly complex devices with the advent of routing capability, Access Control Lists (ACLs), Virtual Local Area Networks (VLANs), port security, Quality of Service (QOS), Resiliency, and management features. Since these devices operate at layer 2 and layer 3 they can be used to circumvent other security controls, depending on the design and management of the device. This can potentially negate the company's firewall policy, for example. Intelligent switches need to be properly configured, managed, and audited. IT Executives and managers should take time to understand the role these devices play in their company's network architecture to ensure adequate controls are placed on these devices. The establishment and maintenance of these controls is a required part of managements due diligence with respect to protecting corporate information assets.

Note: Typographical conventions used in this practical assignment are:

12 point Arial is used for standard text. 10 point Arial is used for command line output, program output and listings. Bold type is used to draw attention to specific text.

1. Research in Audit, Measurement Practice, and Control

1.1 System to be Audited

The device being audited is a Cisco 3550 layer 3 switch running IOS 12.1(19)EA1a as shown by excerpts of the devices version information.

```
OpsTempBanner1#sh ver
```

```
Cisco Internetwork Operating System Software
```

```
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(19)EA1a, RELEASE SOFTWARE (fc1)
```

```
Copyright (c) 1986-2003 by cisco Systems, Inc.
```

```
Compiled Tue 09-Dec-03 03:01 by yenanh
```

```
Image text-base: 0x00003000, data-base: 0x0069B37C
```

```
CLIPPED FOR BREVITY
```

```
cisco WS-C3550-48 (PowerPC) processor (revision J0) with 65526K/8192K bytes of memory.
```

```
Processor board ID CAT0745Z0E2
```

```
Last reset from warm-reset
```

```
Running Layer2/3 Switching Image
```

```
CLIPPED FOR BREVITY
```

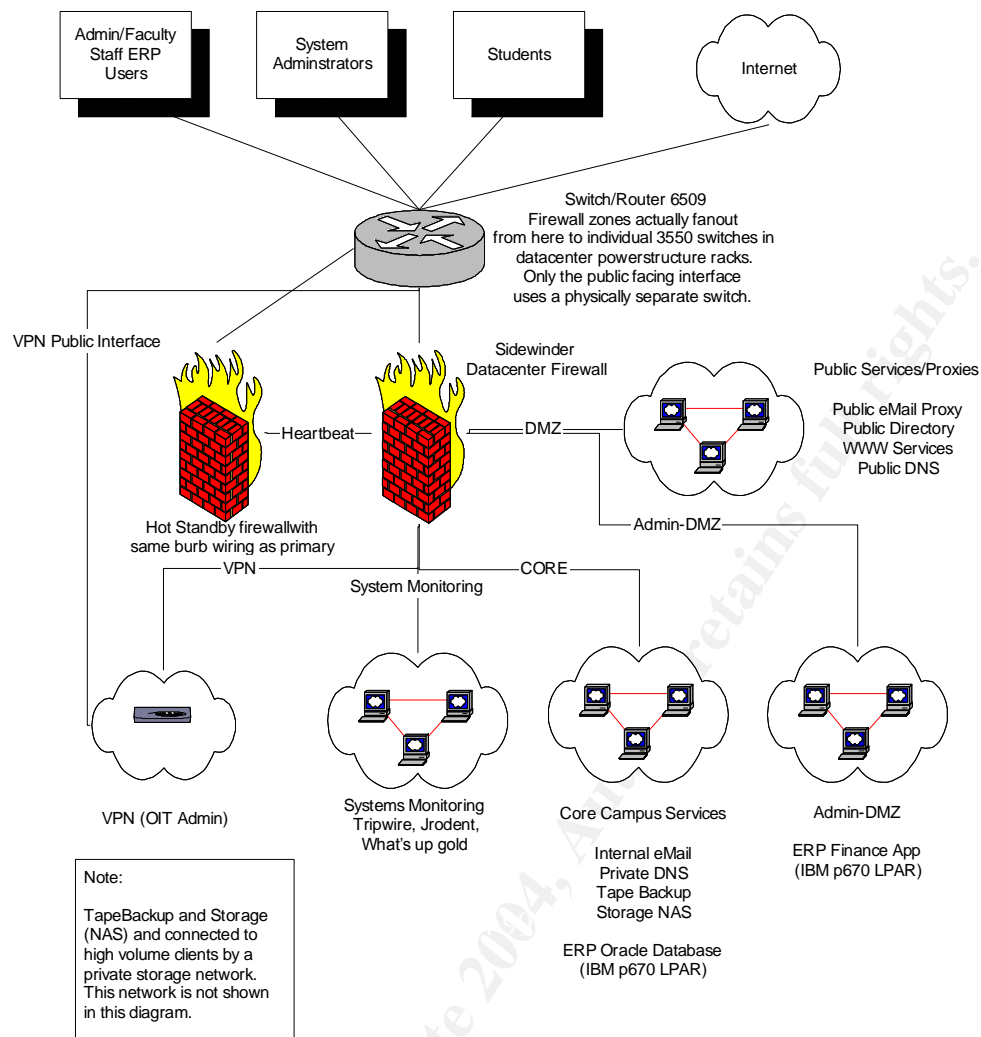
```
48 FastEthernet/IEEE 802.3 interface(s)
```

```
2 Gigabit Ethernet/IEEE 802.3 interface(s)
```

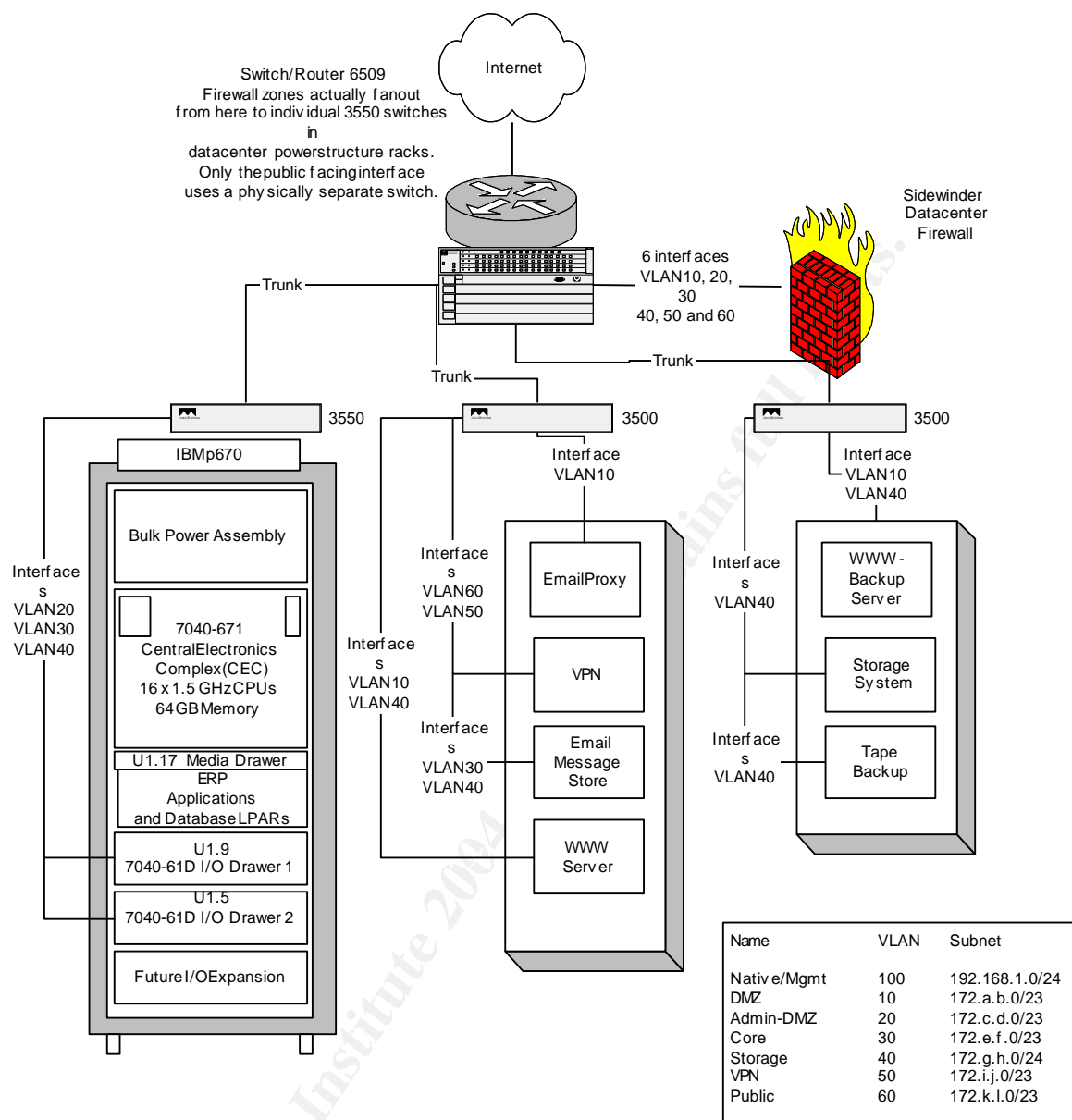
```
CLIPPED FOR BREVITY
```

```
switch1#
```

The device is used as an edge distribution switch within the corporate datacenter. It is used to provide connectivity to the company's mainframe. It links the mainframe to several firewall interfaces and a storage network. The datacenter uses many of these switches to distribute network connectivity to power structure racks where central servers are housed. These servers provide database, Enterprise Resource Planning (ERP) applications, public services such as web and mail servers, and access and control for system administration and management. The following figure depicts the logical datacenter architecture.



The next figure more accurately shows the physical architecture. The diagram is greatly simplified. The components included are to help illustrate the role the switches play and the issues regarding security.



In this machine room architecture each rack or collection of racks, based on machine density, has an associated switch. There are many racks, as this is a large datacenter. Using VLANs enables flexibility in installing and wiring servers. The VLANs remove constraints on physically locating servers or physically wiring them based on the firewall interface they are associated with. This eases maintenance as servers and services change rapidly and many services run in Virtual Machines (VMs) which are housed in larger machines with many network interfaces.

The above figure shows that all firewall interfaces are plugged into the same physical switch. This is a security risk. Of particular concern is the fact that the public interface is located on the same switch as the other firewall interfaces. The result is that the only thing preventing compromise of the firewall security policies is layer 2 VLAN enforcement on the 6509 switch. This is a major issue and is being changed so that the

public firewall interface will be placed on a physically separate switch. The remaining interfaces, which have different levels of security, reside on the same switch infrastructure for the flexibility reasons previously stated. Isolating the public interface on a separate switch requires at least two layers of security to be compromised to circumvent the firewall policies governing public to private traffic. The exception, of course, is compromising the firewall itself. A machine behind the firewall must be compromised in order to launch layer 2 attacks between the protected interfaces or an individual must gain physical access to the switch. This does not eliminate the risk but reduces it to a level that the management of this particular institution feel is an appropriate balance between security and flexibility.

The particular 3550 being considered in this audit is providing switching and layer 2 and 3 security functions for the IBM p670 mainframe. The p670 runs the institutions ERP systems, such as finance, payroll, and HR systems. This system is really a collection of systems running in separate instances of AIX 5.2L within IBM's Logical Partition (LPAR) environment. Each LPAR has two physical network interface cards, one that places the LPAR in the appropriate firewall zone, based on it's function, and a second which provides access to the storage network. The storage network provides Network File System (NFS) access to a Network Appliance Filer for data storage. The storage network is also utilized by other systems in the machine room. The network is privately addressed and is not routable. However, this network presents a security issue because it spans firewall interfaces. This is stated to be required due to the volume of data traffic on this network. To reduce the risks presented by this network the network is monitored by an IDS sensor and is protected by switch security policies that only allow traffic to flow between each server and the filer. No other peer-to-peer traffic is permitted. The IDS also monitors this, i.e. traffic must have a source or destination address of the filer.

Given this background information the 3550 has 4 principle roles:

- It provides a switched network infrastructure.
- It enforces isolation of network segments associated with different firewall interfaces and security policies.
- It enforces specific security policies of it's own on the Storage Network segment to control intra-segment traffic.
- It provides access for security scanning of machines and Intrusion Detection System (IDS) sensors.

Network scanning and IDS are not shown in the above diagrams. A port is designated for security scans. This involves scanning servers from the appropriate VLAN with tools like Nessus, Winfingerprint, and Nmap. Scans are done from both within the machines network segment and across firewall interfaces. This is done to verify the firewall policy, host firewall rules, and/or switch traffic controls within the network segment. IDSs monitor each firewall zone (network segment) and the storage network, as previously discussed.

1.2 3550 Secure Configuration

Proper configuration and management of the machine room network infrastructure is important to reduce risk and insure that other security mechanisms are not undermined or negated. Switches, like routers, firewalls, and VPNs, need to have appropriate physical, administrative, and technical controls in place to ensure that they are meeting their operational and security objectives. This is becoming more important as switches become more intelligent and companies like Cisco Systems unify their IOS and merge many of the functions of routers and switches. A secure configuration of the switch should accomplish the following:

- Prevent unauthorized modification to the switch configuration.
- Enforce isolation of network segments on the switch and across switches.
- Prevent unauthorized access to the network by accidental or intentional changes in wiring. I.e. plugging a notebook into the switch or plugging a server into the wrong port.
- Insure that the security policy is properly implemented and accomplishing its stated objectives.

1.3 Risks to the System

The increasing complexity of switches and their respective placement in the network architecture poses risk to the information assets of an institution. This is true of all technology. It is therefore important to understand the risks posed by a particular device and architecture and communicate those risks with alternative mitigation strategies to management. There will always be residual risk. The key is to balance the cost, complexity, and possible usability impacts of security measures with the potential impact of successful exploitation. The following tables will describe several vulnerabilities, threats, their possible impact, and the information assets at risk.

Risk Number	Vulnerability	Threat	Impact of Exploit
R1	Misconfigured port security on storage network VLAN	Careless or improperly trained Administrator	Firewall ruleset is negated. Data with different security policies can be captured/exposed. Machines in different firewall zones can be attacked on secondary network interfaces.
R2	VLAN configuration not providing proper network isolation.	Misconfiguration or maintenance.	Undetected server/machine could be sniffing traffic on VLAN.
R3	Port ACLs/Port Protection not enforcing traffic	Incorrect configuration or application of	Network traffic policy is not enforced. Information could inadvertently be exposed. Attacks could be launched against critical servers if other security

	policy	ACLs	layers are compromised.
R4	IOS software not maintained at current level or patched to prevent known exploits	Threat agent can take over the device or disrupt the device function by known vulnerabilities	Credentials and data can be stolen leading to further attacks. Corporate operations can be disrupted.
R5	Weak Passwords	Brute force and/or dictionary attack.	Compromise of device. All data assets traversing the device are subject to compromise/exposure.
R6	Rogue or Hacked system plugged into switch	Internal user/admin with malicious intent.	System can be used as a DOS attack point or sniffer. Information can be gained for use in subsequent attacks.
R8	Unauthorized physical access to the switch	An individual with malicious intent	Can disrupt operations. Possibly take control of the switch and reconfigure it. Possibly compromise all data going through the switch. Theft of device.
R9	Unauthorized virtual access to the switch	An individual with malicious intent	Can disrupt operations. Possibly take control of the switch and reconfigure it. Possibly compromise all data going through the switch.
R10	Telnet SNMP (less than v3)	Clear text protocols may expose credentials	Compromise of device. All data assets may become compromised or disclosed.

Information Asset	How Asset is Affected by Switch
Corporate Data including HR, payroll, customer records, financials, etc. This data is accessed through end user protocols such as HTTP, HTTPS.	Switch uses VLANs to isolate this network traffic to an administrative (internal) DMZ.
All corporate data stored in oracle and accessed through sqlnet.	Switch uses VLANs to isolate this network traffic to the core private network.
Publicly accessible data including purchase transactions for eCommerce. HTTP and HTTPS are the protocols used.	Switch uses VLANs to isolate this network traffic to the public DMZ.
Storage Network traffic for all systems database and configuration data. NFS protocol is used	The switch isolates traffic to a private network with a VLAN and uses ACLs to insure that traffic from servers can only be destined for the Network Fileer and that no

	peer communication can occur. This reduces the risk of crossover between protected networks behind the firewall.
--	--

1.4 Current State of Practice

Cisco intelligent switches, like the 3550, are utilizing IOS software that is converging with the router IOS. These switches have similar management and administrative abilities as routers. They also provide routing and ACL features. Therefore many aspects that are important to router management are applicable to the switches. Switches also have some unique configuration options that can affect security and need to be analyzed. These include port protection, VLANs, VLAN ACLs, and VLAN maps. Of course, this list is not inclusive and we will expand upon the range of security related configuration options later in this section.

Physical security is critical layer for machine rooms. "No amount of firewalls, encryption or access lists can stop a criminal who gets into a server room"[3]. There are several areas of physical controls. Areas containing switches, network equipment, and servers need to be protected from unauthorized access. Typically networking equipment can be found in wiring closets, networking areas of a machine room, and edge devices may be found located in equipment racks within the datacenter. The subject device of this audit is an edge switch located in a rack in the datacenter. Datacenters often have good physical security but there are a variety of controls that should be verified. Shon Harris's book, "CISSP Certification Exam Guide" [4] has a good discussion of issues of datacenter physical security as it is one of the ten CISSP domains. ISO 17799[24] is also a good reference. Some of the issues that arise are: Is the physical construction, locks, controlled access points (doors), reasonable and appropriate for the data assets being secured? The construction should not allow it to be easily bypassed, i.e. drop ceilings. Physical controls should insure that only authorized persons have access to the machine room. Note alarms, video surveillance equipment, and entrance and exit logs. There should be policies, procedures and logs for moving equipment in and out of the machine room. There are also some technical controls on the device itself that can augment physical controls. Examples are disabling password recovery, administrative shutdown of unused switchports, and port security.

Administrative controls deal with user and password management, Console and line access, web based device administration, software upgrade management, event notification and logging. Cisco switches have a variety of mechanism for password management. Out of the box, passwords are in the clear. The enable secret command will keep the enable password in a MD5 hash. This is not reversible but is subject to dictionary attack so it should be protected from distribution. The service password-

encryption command causes IOS to encrypt other passwords and credentials with a weak encryption. This provides some security from shoulder surfing but the passwords in the configuration file should be assumed to be stored as if in the clear because they can easily be reversed.

Technical controls will focus on VLANs, Port protection and security, and ACLs. SPAN ports, Etherchannels, flood control, VLAN maps, and routing are not used on the target switch and therefore are not included in this paper. They are however, important components of switch operation and an exhaustive check list would include them.

There are several checklists and books that were used for the basis of this audit checklist. The Network Infrastructure Security Checklist from the Defense Information Systems Agency [5] has some good items on VLAN, Trunking, and port configuration information.

KBeta Security Web, "Improving Security on Cisco Routers" [14] is a very extensive checklist for routers. It covers password management, controlling interactive access, management services, logging, secure routing, flood management, potentially unnecessary services, etc. This list gives a technical overview of each item as well as recommendations on configurations and why they are important. Although, the subject unit is not a router this check list covers many of the areas of IOS that are common to routers and intelligent switches.

Cisco Systems, "Securing the LAN with Catalyst 3550 and 2950 Series Switches" [8] is a presentation that enumerates many of the 3550 security features and presents them in the context of a layered approach to network security. Many of the items contained in the presentation can be converted to check list items based on their applicability to a particular device and its role. Cisco's, "Virtual LAN Security Best Practices"[15] and "SAFE Layer 2 Security In-depth Verion 2"[16] provide in depth information regarding switch attacks, risk mitigation techniques, and configuration best practices.

The Center for Internet Security <http://www.cisecurity.com> provides a Router Audit Tool (RAT) [19] complete with check list and configuration guides. The Gold Standard Benchmark for Cisco IOS Version 2.1 contains many configurations items that are applicable to intelligent switches as well as routers. Bill Zeng has also published a Cisco Configuration Security Auditing Tool (CCSAT) [23], it is available at <http://hotunix.com/tools>. The advantage of this and the CIS tools are that they are easily modified to support any checklist, and speed that process by having checks for the SANS and NSA security guides already built in. Automation of the process allows you to look at many individual switch configurations and note changes over time. With CCSAT you can also look at a large number of devices and look for aggregate statistics on device configurations.

2. Audit Checklist

The scope of the audit is directly affected by the role of the device in the organizations infrastructure. Section one found the Cisco 3550 intelligent switch/router under consideration to have 4 principle roles:

- It provides a switched network infrastructure.
- It enforces isolation of network segments associated with different firewall interfaces and security policies.
- It enforces specific security policies of it's own on the Storage Network segment to control intra-segment traffic.
- It provides access for security scanning of machines and Intrusion Detection System (IDS) sensors.

This device is not used for routing in this role. Therefore audit items regarding routing are omitted as not applicable.

Item Number	1
Item Title	Physical Installation and Removal
Purpose/Reference	Insure adequate physical controls are in place to prevent unauthorized installation and removal of equipment. Harris, S. CISSP Exam Guide [4] IOS 17799 [24]
Risk	R8 – Unauthorized physical access
Test Procedure/ Compliance Criteria	Review policies and procedures for installing and removing switches/network equipment from the machine room. <ol style="list-style-type: none">1. Is there approval required for installation and removal?2. Is the asset tracked, by an asset tag or serial number? Ask for evidence that the policies and procedures are being followed.
Test Nature	Objective
Evidence	
Findings	

Item Number	2
Item Title	Physical Access to Switch

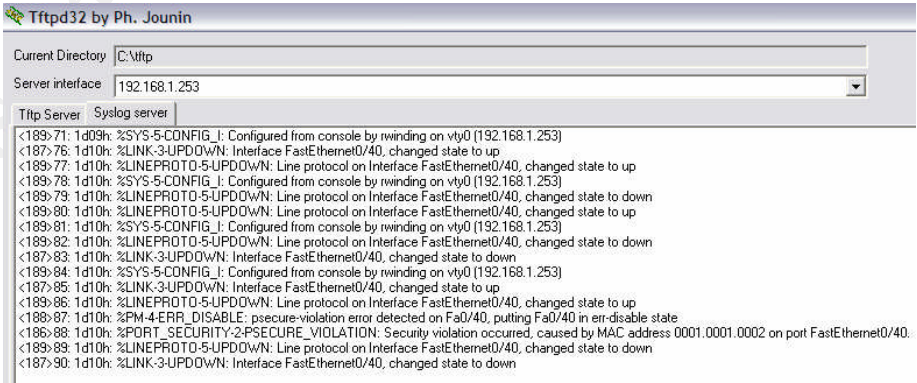
Reference	Insure adequate physical controls are in place to prevent unauthorized access. Harris, S. CISSP Exam Guide [4] IOS 17799 [24]
Risk	R8 – Unauthorized physical access
Test Procedure/ Compliance Criteria	Review physical security controls and access logs in machine room. Review walls, doors, locks, ceilings, flooring for potential unauthorized entrance opportunities. Inquire about surveillance of the facility. What is the coverage area and what is the duration of data retention. Review environment, i.e. temperature and humidity.
Test Nature	Subjective
Evidence	
Findings	

Item Number	3
Item Title	Change Control
Purpose/Reference	Insure that only authorized changes are implemented; minimize configuration entropy of systems over time. ISO/IEC 17799 [24].
Risk	R1, R2, R3 through misconfiguration or unintended side effects of changes.
Test Procedure/ Compliance Criteria	<p>Interview Network Engineers regarding current change control process for switches.</p> <ul style="list-style-type: none"> • Is there a written change control policy? • What configuration elements are under change control? • How are configurations backed up and restored? • What is the approval process? • What is done to insure adhoc changes are not made? • How are changes tested? <p>For each item discussed as for evidence that the process is actually being employed.</p>
Test Nature	Objective
Evidence	
Findings	

Item Number	4
Item Title	Design Documentation
Purpose/Reference	Insure that the design of the system is not being compromised over time. ISO 1779 [24].
Risk	R1, R2, R3 through misconfiguration or unintended side effects of changes.
Test Procedure/ Compliance Criteria	<p>Review network design documentation as it pertains to the audit target.</p> <ul style="list-style-type: none"> • Is there a network diagram showing the placement of the device? • Is there a map of VLANs and does it show devices that each VLAN on the switch is trunked to? • Is there documentation stating the purpose and objective of any VLAN ACLs and port security settings? <p>For each item discussed ask for evidence that the process is actually being employed.</p>
Test Nature	Subjective
Evidence	
Findings	

Item Number	5
Item Title	Logon Banner
Purpose/Reference	A logon banner provides notification that only authorized access is allowed and that actions may be monitored.
Risk	R9 – Unauthorized Virtual Access
Test Procedure/ Compliance Criteria	<p>Execute the “show run” command from the enable prompt. Search the configuration file for:</p> <pre>banner login ^C Don't login without permission ^C !</pre> <p>Login to switch (or observe someone else) and see that the banner is displayed.</p> <pre>login as: rwindig rwindig@192.168.1.254's password:</pre>

	Don't login without permission switch1>en
Test Nature	Objective
Evidence	
Findings	

Item Number	6
Item Title	Logging
Purpose/Reference	Logging is necessary to detect unauthorized changes and/or access and provide operational and troubleshooting information. Logging also needs to be controlled so it doesn't overwhelm the device. CIS RAT
Risk	R1, R2, R3, and R9 – Misconfiguration through unauthorized change and unauthorized virtual access
Test Procedure/ Compliance Criteria	<p>Verify (#sh run) that the configuration contains logging console critical</p> <p>This is appropriate for environments without a log infrastructure. Alternatively the device should be logging to a log server where tools can be used to review the logs and perform alerting. Check for logging 192.168.1.253</p> <p>This command may use hostname of IP address. If this is used ask to see the logs and verify activity, e.g.</p> 
Test Nature	Objective
Evidence	
Findings	

Item Number	7
Item Title	Password Management
Reference	Proper password management is a basic component of device security. Hardening Cisco Routers [13]
Risk	R5 – Weak passwords, R9 – Unauthorized virtual access
Test Procedure/ Compliance Criteria	<p>The following account/password configuration entries are found in the switch configuration using the “show run” command executed from the enable prompt on the switch. Verify that the passwords are encrypted to the extent possible and that enable secret is used. Make sure that uniquely identifiable user accounts are created. In this case locally. They will not appear together in the configuration file.</p> <pre> service password-encryption ! enable secret 5 \$1\$V5gO\$UhyUkUk9mf3wu5b677ua1 ! line con 0 password 7 050C090633455D01 line vty 0 4 access-class 10 in password 7 094B41000B0C041A login local transport input ssh line vty 5 15 access-class 10 in password 7 094B41000B0C041A login local transport input ssh ! end </pre> <p>Observe a network engineer logon to the switch. Insure that he/she is prompted for a userid.</p> <p>Note: Line aux is not applicable on the 3550. No central authentication system is currently utilized in this environment.</p>

Test Nature	Objective
Evidence	
Findings	

Item Number	8
Item Title	Password Strength
Purpose/Reference	Weak passwords are a common source of system compromise. Combating the Lazy User: An Examination of Various Password Policies and Guidelines [25]
Risk	R5 – Weak Passwords
Test Procedure/ Compliance Criteria	Interview network administrators regarding password selection and compare to published recommendations. Are passwords at least 8 characters? Contain the full range of character set? At least 5 different characters? Not derived from a single word, e.g. C0mput3R Are they changed every 60 days?
Test Nature	Objective
Evidence	
Findings	

Item Number	9
Item Title	Virtual Access - SSH
Purpose/Reference	Clear text protocols make capture of userids and password easy. This item determines what protocols are being used for administrative access. Failing to constrain access increases these risks. Hardening Cisco Routers[13]. CIS RAT Checklist [19].
Risk	R9 – Unauthorized virtual access, R10 - Telnet
Test Procedure/ Compliance Criteria	Verify that only SSH is allowed and that access is restricted by ACL to specific hosts. Insure that administrators are using SSHv2. Example: <i>access-list 10 permit 192.168.1.253</i>

```
access-list 10 deny any
```

```
!
```

```
line vty 0 4
```

```
access-class 10 in
```

```
password 7 094B41000B0C041A
```

```
login local
```

```
transport input ssh
```

```
line vty 5 15
```

```
access-class 10 in
```

```
password 7 094B41000B0C041A
```

```
login local
```

```
transport input ssh
```

```
!
```

Insure that SSH is the only service running on the switch. Do this by placing a computer on the management VLAN and using nmap to portscan the switches IP address.

```
C:\>nmap -sS -v -p 1-65535 -P0 192.168.1.254
```

Starting nmap V. 3.00 (www.insecure.org/nmap)

Host (192.168.1.254) appears to be up ... good.

Initiating SYN Stealth Scan against (192.168.1.254)

Adding open port 22/tcp

The SYN Stealth Scan took 72 seconds to scan 65535 ports.

Interesting ports on (192.168.1.254):

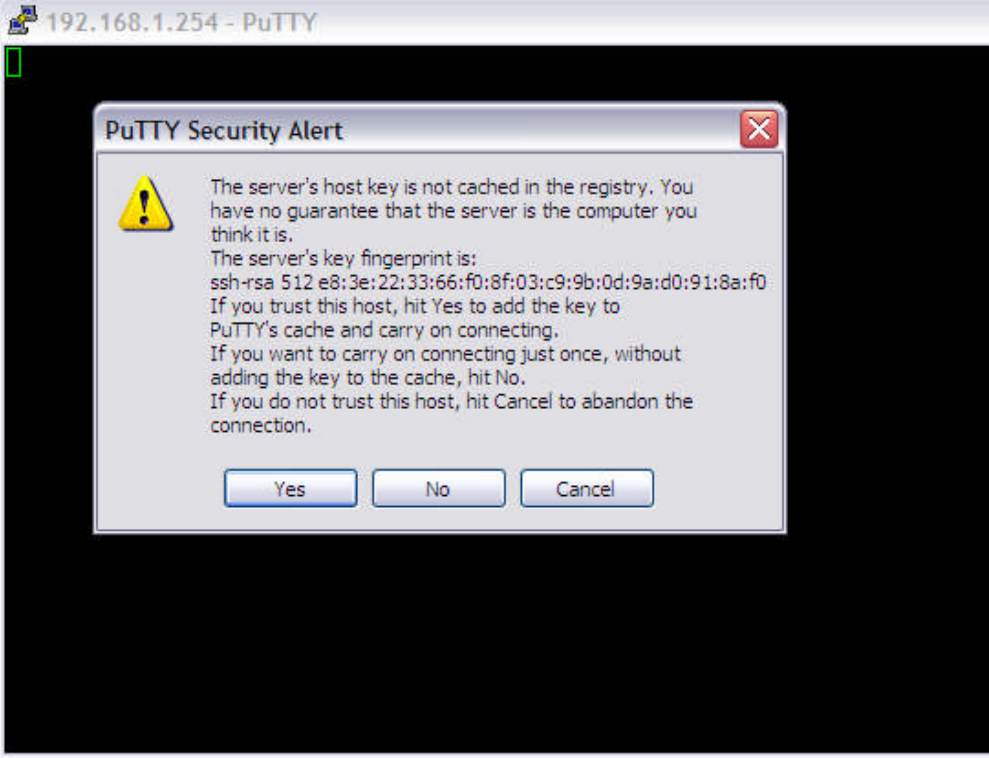
(The 65534 ports scanned but not shown below are in state: closed)

Port	State	Service
------	-------	---------

22/tcp	open	ssh
--------	------	-----

Nmap run completed -- 1 IP address (1 host up) scanned in 92 seconds

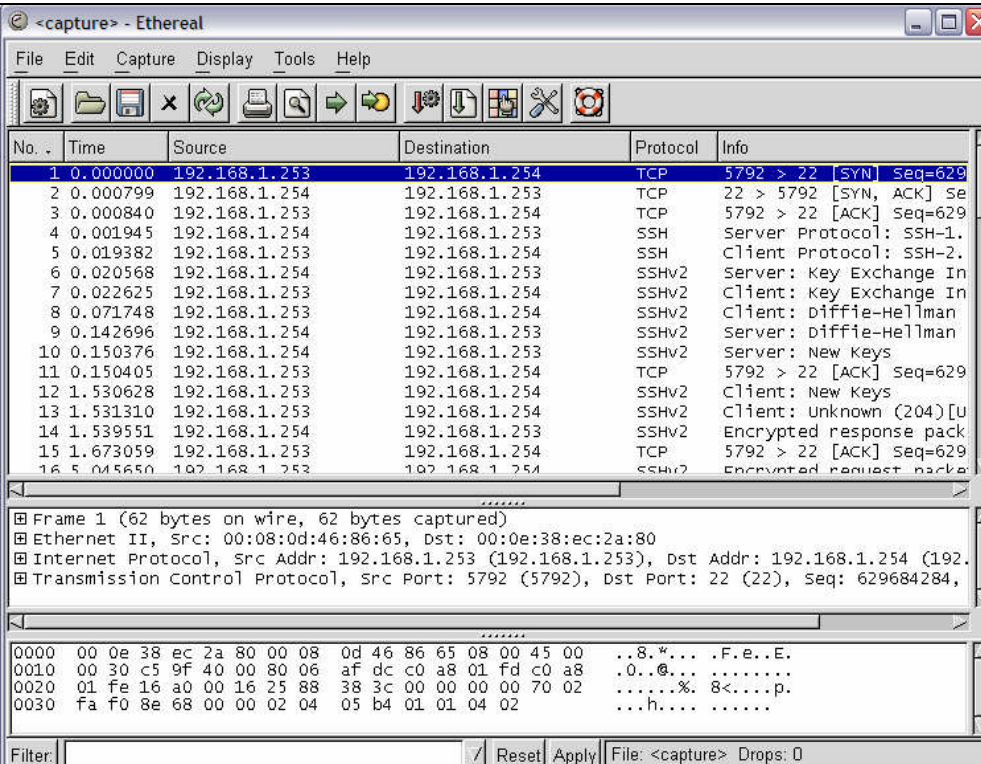
Use a tool like putty (ssh client) and observe a network engineer log in. Does the tool accept the certificate from SSH? Is the SSH session properly established? Note the key size in the window. In this example it is 512. A length of 1024 would be preferred.



The following logon was captured and analyzed with ethereal.

login as: rwindng
rwindng@192.168.1.254's password:

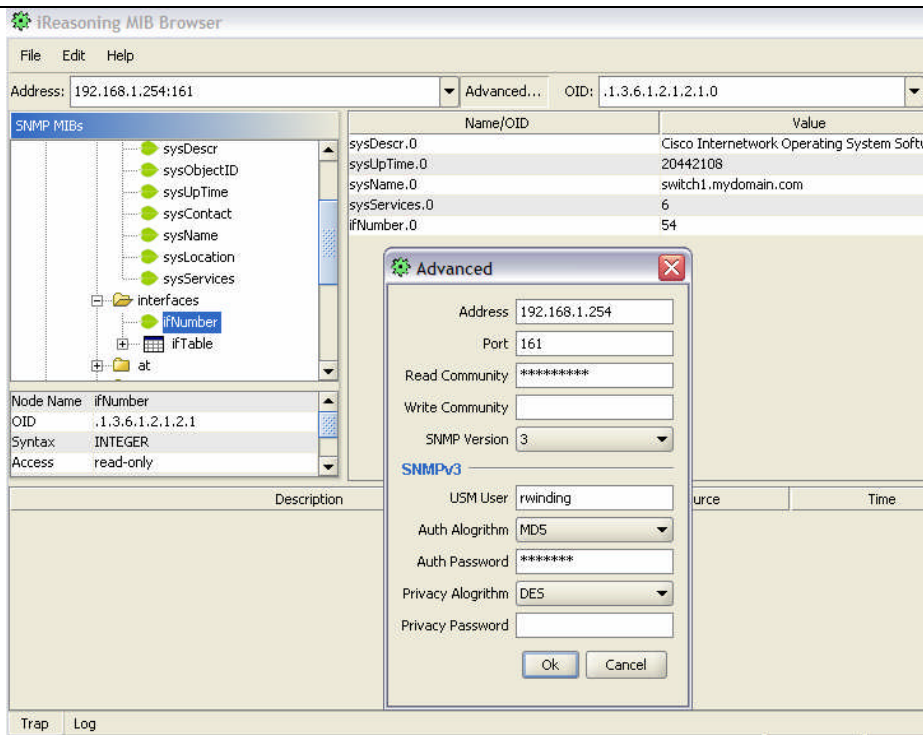
switch1>en
Password:
switch1#

	 <p>Note the SSHv2 in the example. This is the correct response. You must insure that the SSH client is configured for SSHv2 as the switch will allow SSHv1 connections.</p>
Test Nature	Objective
Evidence	
Findings	

Item Number	10
Item Title	IOS Version
Purpose/Reference	Insure that the IOS is being properly maintained to reduce the risk of exploits of known vulnerabilities. KBeta, Improving Security on Cisco Routers[14]
Risk	R4 – IOS Software not being maintained.
Test Procedure/Compliance Criteria	<p>The “show version” command issued at the enable prompt is used to determine the IOS version running on the device. The first few lines show the version and image file.</p> <p>Example:</p> <pre>switch1#show version</pre>

	<p>Cisco Internetwork Operating System Software</p> <p>IOS (tm) C3550 Software (C3550-I5K2L2Q3-M), Version 12.1(19)EA1c, RELEASE SOFTWARE (fc2)</p> <p>Copyright (c) 1986-2004 by cisco Systems, Inc.</p> <p>Compiled Tue 03-Feb-04 10:39 by yenanh</p> <p>Image text-base: 0x00003000, data-base: 0x009428D4</p> <p>ROM: Bootstrap program is C3550 boot loader</p> <p>switch1 uptime is 17 hours, 24 minutes</p> <p>System returned to ROM by power-on</p> <p>System image file is "flash:c3550-i5k2l2q3-mz.121-19.EA1c/c3550-i5k2l2q3-mz.121-19.EA1c.bin"</p> <p>Output truncated for brevity.</p> <p>Compare the version listed with the latest release. All IOS software can be found at http://www.cisco.com/kobayashi/sw-center . Following the lan switching software link the 3550 software can be found at http://www.cisco.com/cgi-bin/tablebuild.pl/cat3550 . The network engineer will need to provide access. Public access to product releases can be obtained by searching www.cisco.com, example: http://www.cisco.com/en/US/products/hw/switches/ps646/prod_bulletin09186a00801ce930.html however this is not always current.</p> <p>If the version running is not the current version interview engineer on IOS upgrade policy. Does the version reflect the policy?</p> <p>Check to see if there are any known vulnerabilities in the running version. Vulnerabilities can be found at http://www.cisco.com/warp/public/707/advisory.html , http://www.securityfocus.com/bid/vendor/ [21], and http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=cisco [22]</p>
Test Nature	Objective
Evidence	
Findings	

Item Number	11
Item Title	Simple Network Management Protocol (SNMP) use.
Purpose/Reference	Earlier versions of SNMP traffic data in clear text and use community names as authentication/authorization credentials. This can lead to configuration compromise and/or information leaks. Hardening Cisco Routers [13].
Risk	R10 - SNMP Versions earlier than v3.
Test Procedure/ Compliance Criteria	<p>Log onto switch in privileged mode (enable prompt #)</p> <p>Show the running configuration and examine the SNMP entries. See the examples below.</p> <p>This example shows weak restrictions on SNMP. There are no access list restriction, authentication, or encryption. The only thing preventing abuse of SNMP are the community string names, i.e. public and 1se45f&x . Public is the default. The RW is strong but since this is transmitted in the clear it is easily sniffed.</p> <p>Switch1#sh run ... omitted for brevity snmp-server community public RO snmp-server community 1se45f&x RW snmp-server location operations snmp-server contact Network Engineering</p> <p>A SNMP MIB browser can be used to discover if the default SNMP strings are set or if simple strings will allow access to the MIB information. You need a tool that can verify the use of various versions of SNMP. iReasoning provides such a tool. It can be downloaded at http://www.ireasoning.com/</p>



In this case variables can be read because the correct authentication credentials were supplied.

A better configuration would limit access to a set of specific monitoring machines.

```
Switch1#sh run
... omitted for brevity
access-list 10 permit 192.168.1.10
access-list 10 permit 192.168.1.20
snmp-server community monitor RO 10
snmp-server community 1se45f&x RW 10
snmp-server location operations
snmp-server contact Network Engineering
```

Finally, SNMPv3 with encryption is the best solution. This configuration will look like :

```
Switch1#sh run
... omitted for brevity
access-list 10 permit 192.168.1.10
access-list 10 permit 192.168.1.20
snmp-server group test-group v3 auth access 10
```

	snmp-server location operations snmp-server contact Network Engineering NOTE: If any SNMP community string commands are in the configuration you will be able to use those to gain info with snmpv2 or snmpv1 even through there is snmpv3 authentication enabled.
Test Nature	Objective
Evidence	
Findings	

Item Number	12
Item Title	Management VLAN Isolation
Purpose/Reference	Insure that management traffic is isolated from user traffic. Network Infrastructure Security Checklist [5].
Risk	R5 – Weak passwords, R6 – Rogue machine on network, R9 – Unauthorized virtual access.
Test Procedure/ Compliance Criteria	<p>Issue the “show run” command from the enable prompt. The VLAN used for management will have an IP address associated with it. The IP address can only be accessed by ports that belong to this VLAN.</p> <p>Example:</p> <pre>interface Vlan100 ip address 192.168.1.254 255.255.255.0 !</pre> <p>These lines are copied from the output of a switch configuration showing the management VLAN to be Vlan100. Insure that the management VLAN is not used as the native VLAN.</p> <p>Example:</p> <pre>interface FastEthernet0/1 description uplink to xyzswitch switchport trunk encapsulation dot1q switchport trunk native vlan 100</pre>

	<pre> switchport trunk allowed vlan 10,20,30,100,1002-1005 switchport mode trunk ! </pre> <p>Check that the VTY lines and SNMP interfaces are properly constrained by ACLs.</p> <p>Example:</p> <pre> access-list 10 permit 192.168.1.253 access-list 10 deny any snmp-server group test-group v3 auth access 10 line con 0 password 7 050C090633455D01 line vty 0 4 access-class 10 in password 7 094B41000B0C041A login local transport input ssh line vty 5 15 access-class 10 in password 7 094B41000B0C041A login local transport input ssh </pre> <p>Check the visibility of the management VLAN by using nmap to try to find the management interface on the management VLAN from outside the management VLAN (see if it is routed widely). Check for visibility of the SNMP interface using Reasoning's MIB browser or similar tool from outside the management network.</p>
Test Nature	Objective
Evidence	
Findings	

Item Number	13
Item Title	Default VLAN, i.e. Vlan1 management
Purpose/Reference	Vlan1 is the default VLAN and all ports default to use it. By disabling Vlan1 the risk of unauthorized access is reduced.

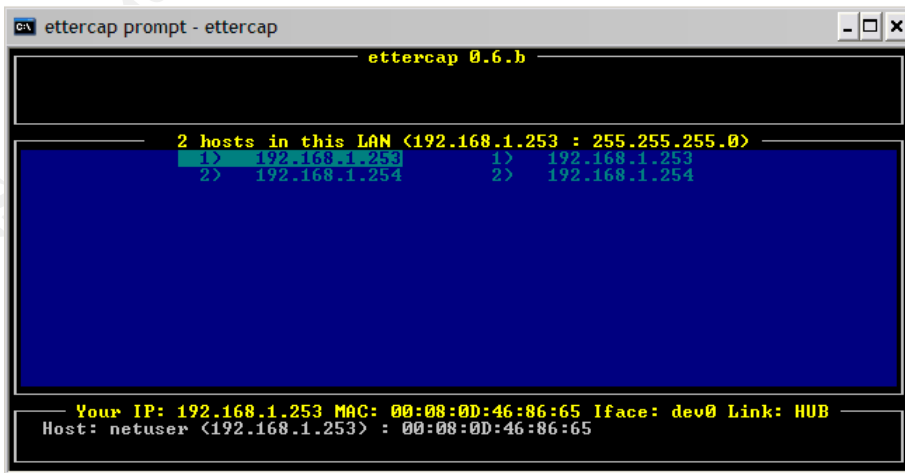
	Also unused ports should be assigned to an unused VLAN created for that purpose. Network Infrastructure Security Checklist [5]. Virtual LAN Security Best Practices [15].																														
Risk	R2 – VLAN not providing proper network isolation, R6 – Rogue Machine, R9 – Unauthorized virtual access.																														
Test Procedure/ Compliance Criteria	<p>Issue the “show vlan” command from the enable prompt. You should see output similar to the following:</p> <pre>switch1#sh vlan</pre> <table><thead><tr><th>VLAN Name</th><th>Status</th><th>Ports</th></tr></thead><tbody><tr><td>1 default</td><td>active</td><td>Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Fa0/25 Fa0/26, Fa0/43, Fa0/44, Fa0/45 Fa0/46, Fa0/47, Gi0/1, Gi0/2</td></tr><tr><td>2 storage-network</td><td>active</td><td></td></tr><tr><td>60 VLAN0060</td><td>active</td><td>Fa0/42</td></tr><tr><td>100 mgmt</td><td>active</td><td>Fa0/17, Fa0/27, Fa0/28, Fa0/29 Fa0/30, Fa0/31, Fa0/32, Fa0/41</td></tr><tr><td>200 unused</td><td>suspended</td><td>Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/18, Fa0/19, Fa0/20 Fa0/33, Fa0/34, Fa0/35, Fa0/36 Fa0/37, Fa0/38, Fa0/39, Fa0/40</td></tr><tr><td>1002 fddi-default</td><td>act/unsup</td><td></td></tr><tr><td>1003 token-ring-default</td><td>act/unsup</td><td></td></tr><tr><td>1004 fddinet-default</td><td>act/unsup</td><td></td></tr><tr><td>1005 trnet-default</td><td>act/unsup</td><td></td></tr></tbody></table> <p>... Truncated for Brevity</p> <pre>switch1#</pre> <p>Note that Vlan1 is active and has ports associated with it. This is incorrect. Vlan1 should be suspended with no associated ports. Vlan200 is named unused, is suspended, and has ports associated with it. This is correct.</p> <p>Next all ports in the suspended “unused” VLAN should be checked to insure they are in administrative shutdown. This is done by issuing the “show run” command at the enable</p>	VLAN Name	Status	Ports	1 default	active	Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Fa0/25 Fa0/26, Fa0/43, Fa0/44, Fa0/45 Fa0/46, Fa0/47, Gi0/1, Gi0/2	2 storage-network	active		60 VLAN0060	active	Fa0/42	100 mgmt	active	Fa0/17, Fa0/27, Fa0/28, Fa0/29 Fa0/30, Fa0/31, Fa0/32, Fa0/41	200 unused	suspended	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/18, Fa0/19, Fa0/20 Fa0/33, Fa0/34, Fa0/35, Fa0/36 Fa0/37, Fa0/38, Fa0/39, Fa0/40	1002 fddi-default	act/unsup		1003 token-ring-default	act/unsup		1004 fddinet-default	act/unsup		1005 trnet-default	act/unsup	
VLAN Name	Status	Ports																													
1 default	active	Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Fa0/25 Fa0/26, Fa0/43, Fa0/44, Fa0/45 Fa0/46, Fa0/47, Gi0/1, Gi0/2																													
2 storage-network	active																														
60 VLAN0060	active	Fa0/42																													
100 mgmt	active	Fa0/17, Fa0/27, Fa0/28, Fa0/29 Fa0/30, Fa0/31, Fa0/32, Fa0/41																													
200 unused	suspended	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/18, Fa0/19, Fa0/20 Fa0/33, Fa0/34, Fa0/35, Fa0/36 Fa0/37, Fa0/38, Fa0/39, Fa0/40																													
1002 fddi-default	act/unsup																														
1003 token-ring-default	act/unsup																														
1004 fddinet-default	act/unsup																														
1005 trnet-default	act/unsup																														

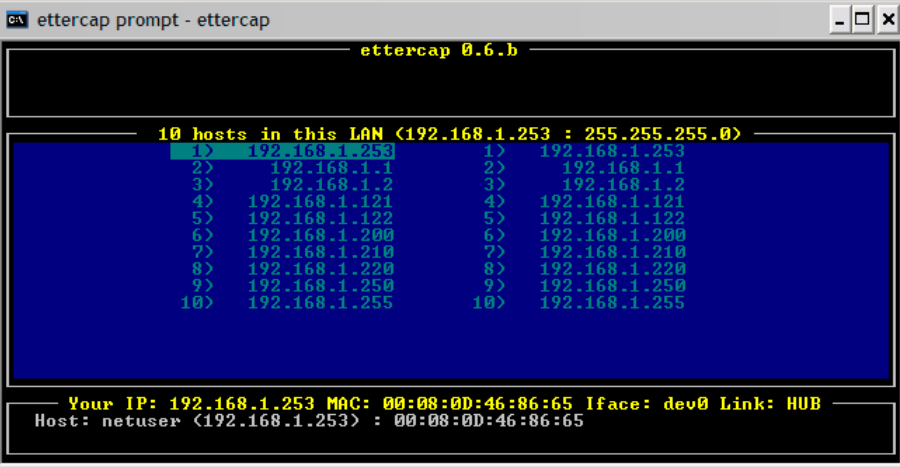
	<p>prompt and verifying the existence of the “shutdown” command for each interfaces. Show below are a couple of Vlan200 interfaces, for brevity. You can also see another way of telling that Vlan200 is suspended.</p> <pre> vlan 200 name unused state suspend ! ! interface FastEthernet0/1 switchport access vlan 200 switchport mode access no ip address shutdown ! interface FastEthernet0/2 switchport access vlan 200 switchport mode access no ip address shutdown ! </pre> <p>Inventory the unused ports and visually confirm that open all open ports are in the designated unused vlan.</p> <p>Plug a notebook into each open port; you should not observe a link light on your notebook or the switch.</p>
Test Nature	Objective
Evidence	
Findings	

Item Number	14
Item Title	Switchport Modes, Controlling Trunking
Purpose/Reference	The purpose of controlling trunking is to prevent a device from impersonating a switch and sniffing traffic on VLANs that it should not have access to. Trunking should also be constrained (pruning) so that VLANs don't propagate unintentionally and become exposed on switches that have insufficient controls applied. Virtual LAN Security Best

	Practices [15]. SAFE Layer 2 Security In-depth [16].
Risk	R1 – Misconfigured Port Security, R2 – VLAN not providing proper network isolation.
Test Procedure/ Compliance Criteria	<p>Verify that the switch infrastructure trunking is being properly restricted.</p> <p>Run the “show run” command from the enable prompt and examine the port configurations. They should all be either explicitly set in access mode or trunk mode.</p> <pre>switch1#sh run Building configuration... Current configuration : 5857 bytes ! interface FastEthernet0/1 switchport access vlan 200 switchport mode access no ip address shutdown ! interface FastEthernet0/19 switchport access vlan 30 switchport mode access no ip address ip access-group 100 in ! interface FastEthernet0/48 switchport trunk encapsulation isl switchport trunk allowed vlan 10,20,30,40,50,60,100 switchport mode trunk no ip address no cdp enable !</pre> <p>The first port is unused and is shutdown. The second is set to mode access and has a ACL applied to it. The third is in trunk mode, has VLAN trunking constrained by the “allowed” command and disables Cisco Discovery Protocol (CDP). These three examples are reasonable and what you should expect to find. If there is no “allowed” command restricting VLANs then all are trunked, which is a security issue.</p> <p>The following example is how ports appear by default. They</p>

	<p>should not be left this way, as they can be negotiated into trunk mode and will forward traffic for all VLANs.</p> <pre>interface FastEthernet0/45 switchport mode dynamic desirable no ip address !</pre>
Test Nature	Objective
Evidence	
Findings	

Item Number	15
Item Title	VLAN visibility
Purpose/Reference	Inventory machines on each trunked VLAN. Insure that machines discovered on the VLANs are supposed to be there. Inventory the management VLAN. Ref: Independent Idea and experience.
Risk	R2 – VLAN not providing proper network isolation.
Test Procedure/ Compliance Criteria	<p>You will need to use a port on the switch. Ask for change control records of what machines should be on each VLAN. Have the engineer set your access port to each VLAN in succession. For each VLAN run ettercap in arp flood mode and see if the ip addresses you find match the expected inventory. The following is a screen shots are the result of ettercap arp floods on a 3550 switch. The first is on the management VLAN (Vlan100).</p>  <p>Note just the sensing notebook and the switch management IP are seen. Next an arp flood of Vlan60.</p>

	 <p>This scan shows the sensing notebook and several other machines on this VLAN. Note that the management IP address is no longer visible. In a machine room environment with sensitive data it is important to insure that only known machines are on a particular VLAN</p> <p>Next use tcpdump or windump to listen for IP addresses that are not in the subnet range of the VLAN. This may uncover unexpected management traffic, misconfigured machines.</p>
Test Nature	Objective
Evidence	
Findings	

Item Number	16
Item Title	Port Security
Purpose/Reference	Port security will prevent a rogue machine from being plugged into a previously occupied port without proper authorization and coordination. It also limits the ability of a legitimate machine to do things like MAC flooding. This configuration is only used on the storage network by policy. Securing the LAN with Catalyst 3550 and 2950 Series Switches[8]. SAFE Layer 2 Security In-Depth [16]
Risk	R1, R2, R3 through misconfiguration or unintended side effects of changes.
Test Procedure/ Compliance Criteria	Run the "show run" command at the enable prompt. Review the ports in the VLAN of interest and make sure that they all have port security configure similar to the below example. interface FastEthernet0/45

```
switchport access vlan 40
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address 00c0.f040.5ec4
no ip address
!
```

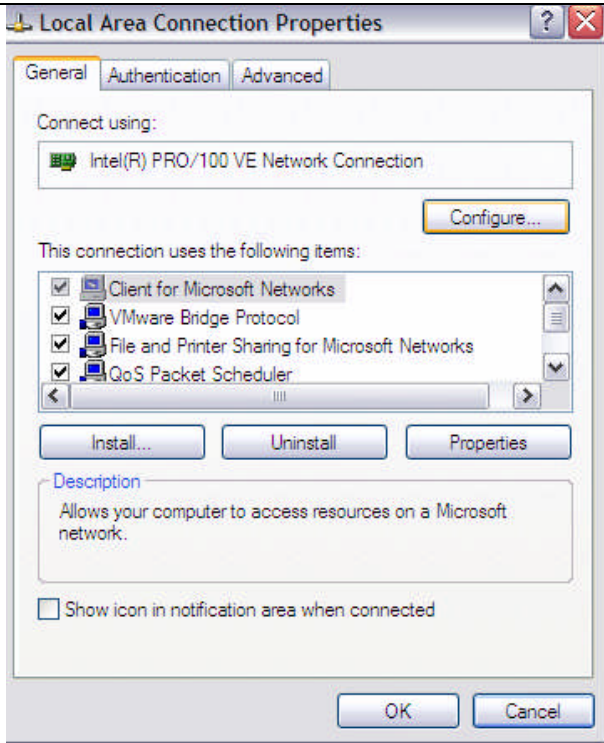
Note, there may be other entries such as ACL restrictions.

If possible try to verify the configuration by cloning it to a spare port, of course changing the MAC to one suitable for testing, say 0001.0001.0001.

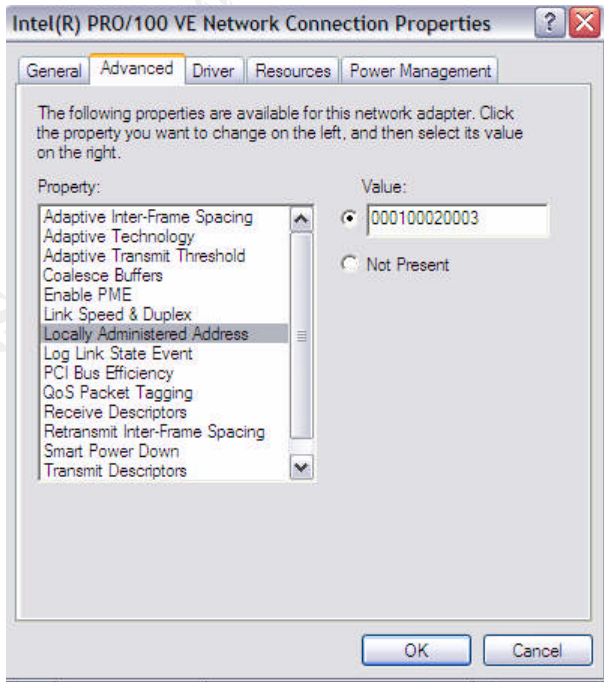
```
switch1(config)#int fa0/40
switch1(config-if)#interface FastEthernet0/40
switch1(config-if)# switchport access vlan 40
switch1(config-if)# switchport mode access
switch1(config-if)# switchport port-security
switch1(config-if)# switchport port-security violation restrict
switch1(config-if)# switchport port-security mac-address 0001.0001.0001
switch1(config-if)# no ip address
switch1(config-if)#exit
```

You can change the MAC on your notebook (usually) by doing the following:

Go to your network connection dialog and click "configure" under the hardware section.



Next under the advanced tab you can configure the Locally Administered Address (MAC) to the value you specified in the switchport configuration. This method may vary by NIC manufacturer but should be similar.



Having done that ping the gateway address or a machine on the

	<p>VLAN that will respond to ICMP echo requests. Next change your MAC and see if you become unable to ping. Have someone monitor the port security status using “sh port-security” from the enable prompt on the switch. Here’s what it looks like.</p> <p>switch1#sh port-security</p> <table><tr><th>Secure Port</th><th>MaxSecureAddr (Count)</th><th>CurrentAddr (Count)</th><th>SecurityViolation (Count)</th><th>Security Action</th></tr><tr><td>Fa0/40</td><td>1</td><td>1</td><td>6</td><td>Restrict</td></tr><tr><td>Fa0/45</td><td>1</td><td>1</td><td>0</td><td>Restrict</td></tr></table> <p>-----</p> <p>Total Addresses in System (excluding one mac per port) : 0</p> <p>Max Addresses limit in System (excluding one mac per port) : 5120</p> <p>switch1#sh port-security</p> <table><tr><th>Secure Port</th><th>MaxSecureAddr (Count)</th><th>CurrentAddr (Count)</th><th>SecurityViolation (Count)</th><th>Security Action</th></tr><tr><td>Fa0/40</td><td>1</td><td>1</td><td>24</td><td>Restrict</td></tr><tr><td>Fa0/45</td><td>1</td><td>1</td><td>0</td><td>Restrict</td></tr></table> <p>-----</p> <p>Total Addresses in System (excluding one mac per port) : 0</p> <p>Max Addresses limit in System (excluding one mac per port) : 5120</p> <p>You can see the security violations counted as the pings are attempted. The pings, of course fail. If any alerts are monitored for MAC address change, verify that this change is detected and acted upon. Finally change the MAC address back and verify that you can once again ping your target.</p> <p>The “ipconfig /all” command on a Windows XP, 2K machine will show MAC information. The “ifconfig –a” command on Linux/Unix variants accomplished the same thing.</p> <p>Note: this technique can be used to circumvent port security if the MAC addresses of the legitimate machines are known.</p>	Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action	Fa0/40	1	1	6	Restrict	Fa0/45	1	1	0	Restrict	Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action	Fa0/40	1	1	24	Restrict	Fa0/45	1	1	0	Restrict
Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action																											
Fa0/40	1	1	6	Restrict																											
Fa0/45	1	1	0	Restrict																											
Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action																											
Fa0/40	1	1	24	Restrict																											
Fa0/45	1	1	0	Restrict																											
Test Nature	Objective																														
Evidence																															
Findings																															

Item Number	17
Item Title	VLAN ACLs
Purpose/Reference	VLAN ACLs can be used to restrict access between hosts on the same VLAN or on the network in general. In the context of this audit all machines on the storage network (Vlan40) are restricted by ACL to only talk to the storage filer.
Risk	R1, R3 – Misconfiguration can result in non-compliance with the network traffic policy.
Test Procedure/ Compliance Criteria	<p>There are two principal reasons to use VLAN ACLs. One is to restrict a machine's traffic by explicitly permitting or denying the traffic by the policy implemented using ACLs. The second, used in this case, to prevent eavesdropping by restricting all machines on the VLAN to send traffic only to the network storage system. The machines are dual homed and only the storage interface is affected.</p> <p>Note: Switch ACLs are only assigned inbound to the interface. There are no outbound ACLs.</p> <p>In both cases, nmap can be used to scan the subnet to determine if the IP Addresses and ports are properly constrained by the policy. To do this, clone the configuration of an ACL restricted port to a spare port. Then perform the scan on the spare port. Verify that nmap cannot "see" any machines or services that the ACLs are designed to restrict.</p> <p>The second is a little trickier and is not really scalable. It requires that every port in the VLAN have the same ACL with respect to the secure data path. If a port on the VLAN isn't restricted in this way it can successfully execute a man in the middle attack and eavesdrop the data.</p> <p>To verify consistent configuration use the "show run" command on every switch that carries the VLAN in question. Verify that each port is correctly configured.</p> <p>Clone a port and use ettercap to see if you can perform a man in the middle attack. This must be carefully scheduled as such an attack could result in a service outage or significant performance degradation. For this reason a test which is used to simulate the audit tests for this paper.</p>
Test Nature	Objective
Evidence	
Findings	

Item Number	18
Item Title	VTP
Purpose/Reference	Prevent device misconfiguration. VTP carries a significant risk in that a misconfigured device can spread its configuration information to other devices. Virtual LAN Security Best Practices [15].
Risk	R1, R2 through VLAN configuration corruption.
Test Procedure/ Compliance Criteria	<p>The configuration should be checked to insure that VTP is disabled. Use the "show vtp status" command from the enable prompt to display the configuration.</p> <p>You will see the following output; VTP Operating Mode Transparent is what needs to be verified:</p> <pre>switch1#sh vtp status VTP Version : 2 Configuration Revision : 0 Maximum VLANs supported locally : 1005 Number of existing VLANs : 10 VTP Operating Mode : Transparent VTP Domain Name : VTP Pruning Mode : Disabled VTP V2 Mode : Disabled VTP Traps Generation : Disabled MD5 digest : 0x10 0xE4 0x76 0x8F 0x96 0x97 0x92 0x2E Configuration last modified by 192.168.1.254 at 0-0-00 00:00:00 switch1#</pre>
Test Nature	Objective
Evidence	
Findings	

Item Number	19
Item Title	CIS Router Audit tool
Purpose/Reference	The CIS router audit tool has significant applicability to all IOS, although it lacks switch specific items and may not be completely accurate in its findings. It is useful though as

	<p>programmatic check of the configuration file and can be used to benchmark/baseline the system to watch for changes or verify change control processes. It can be used as a cross check of the checklist items and as a way to insure common configuration items are not missed. [20]</p>
Risk	N/A
Test Procedure/ Compliance Criteria	<p>From the enable prompt issue the following command to copy the running configuration to a file on a tftp server. Tftpd32 is a free server that can be used for this purpose, it is trivial to configure.</p> <pre>switch1#copy running-config tftp://192.168.1.253/3550.txt Address or name of remote host [192.168.1.253]? Destination filename [3550.txt]? !!! 6176 bytes copied in 1.724 secs (3582 bytes/sec) switch1#config t Enter configuration commands, one per line. End with CNTL/Z. switch1(config)#logging console critical switch1(config)#exit switch1#copy running-config tftp://192.168.1.253/3550.txt Address or name of remote host [192.168.1.253]? Destination filename [3550.txt]? !!! 6182 bytes copied in 1.716 secs (3603 bytes/sec) switch1#</pre> <p>Install the RAT software. RAT can be downloaded from http://www.cisecurity.com free of charge. When installed run it from the command prompt.</p> <pre>C:\CIS\RAT\bin>rat 3550.txt auditing 3550.txt... Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/common.conf/ Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/cis-level-1.conf/ Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/cis-level-2.conf/ Checking: 3550.txt done checking 3550.txt. Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/common.conf/ Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/cis-level-1.conf/ Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/cis-level-2.conf/</pre>

	<p>ncat_report: writing 3550.txt.ncat_fix.txt.</p> <p>ncat_report: writing 3550.txt.ncat_report.txt.</p> <p>ncat_report: writing 3550.txt.html.</p> <p>ncat_report: writing rules.html (cisco-ios-benchmark.html).</p> <p>ncat_report: writing all.ncat_fix.txt.</p> <p>ncat_report: writing all.ncat_report.txt.</p> <p>ncat_report: writing all.html.</p> <p>C:\CIS\RAT\bin></p> <p>RAT produces a html report of all its tests complete with descriptions and mitigations.</p> <p>See Appendix A. for an example of the high level report.</p> <p>Use the tool to confirm or spot any inconsistencies in prior audit control steps.</p>
Test Nature	Objective
Evidence	
Findings	

Item Number	20
Item Title	CCSAT
Purpose/Reference	<p>The CCSAT is an IOS audit tool in the form a shell script. It is setup to audit all configuration files in a directory and generate an audit report on the configurations in aggregate. This can be helpful to verify manually conducted audit items as well as provide a quick assessment of a large number of configurations. It's simplicity enables it to be easily modified. It can be used as a basis for automating custom audit checks. Of course, any configuration file analysis tool is limited to looking for signature command strings. This is a significant limitation, since complex configurations can contain entries yet not actually implement the desired controls.</p>
Risk	N/A
Test Procedure/ Compliance Criteria	<p>As with RAT, the configuration file is copied via TFTP to a PC with CCSAT installed. The analysis computer has to support Unix shell commands and processing. Redhat vesion 9 is used in this example. The switch configuration file is copied into the configuration directory. Then CCSAT is run with the IOS version as a parameter.</p>

	<pre>[root@localhost ccsat]# ./ccsat.sh 12.1 Cisco Device Configuration Security Audit Copyright (C) 2003 Bill Zeng ===== Please make sure configuration file names contain no space and use the same extension - Otherwise this script will not run properly! ===== shutdown interfaces... I. General Configuration - checking.... IOS version... banner... II. Passwords and Authentication - checking.... service password-encryption... enable secret... enable password... line passwords... SNMP community public/private... AAA new-model... AAA authentication (tacacs+/radius/kerberos)... user privilege... III. Network Services - checking.... TCP small services... UDP small services... Bootp service... Finger service... HTTP service... CDP... Config service... SSH service... IV. IP Routing and Security - checking.... IP source route... CEF... IP directed broadcast... IP mask reply...</pre>
--	---

	<p>IP proxy ARP...</p> <p>use of RIP... (informational)</p> <p>RIP MD5 authentication...</p> <p>use of OSPF... (informational)</p> <p>OSPF MD5 authentication...</p> <p>use of EIGRP... (informational)</p> <p>EIGRP MD5 authentication...</p> <p>use of BGP... (informational)</p> <p>BGP neighbor passwords...</p> <p>Passwords for AS neighbors...</p> <p>V. Access Control and ACLs - checking....</p> <p>line timeout...</p> <p>transport input telnet...</p> <p>transport input ssh...</p> <p>ACLs for terminal lines...</p> <p>ACLs on interfaces...</p> <p>SNMP community readonly/readwrite...</p> <p>VI. Logging - checking....</p> <p>timestamps log...</p> <p>logging...</p> <p>SNMP host...</p> <p>NTP server...</p> <p>Done!</p> <p>[root@localhost ccsat]#</p> <p>Appendix B shows the resulting example audit report.</p>
Test Nature	Objective
Evidence	
Findings	

3. Audit

Item Number	2
Item Title	Physical Access to Switch
Reference	Insure adequate physical controls are in place to prevent unauthorized access. Harris, S. CISSP Exam Guide [4] IOS

	17799 [24]
Risk	R8 – Unauthorized physical access
Test Procedure/ Compliance Criteria	Review physical security controls and access logs in machine room. Review walls, doors, locks, ceilings, flooring for potential unauthorized entrance opportunities. Inquire about surveillance of the facility. What is the coverage area and what is the duration of data retention. Review environment, i.e. temperature and humidity.
Test Nature	Subjective
Evidence	The machine room that houses the switch being audited has floor to ceiling walls that cannot be easily compromised. There are four entrances to the machine room. Three are controlled by biometric devices. The fourth can only be opened from the inside and is alarmed. Access to the facility is logged by a computer running the biometric devices. There is also a manual sign in/out log. There is no video surveillance. Operators, however, man the machine room 7x24 except three days a year when the facility is locked down and patrolled by uniformed guards. There are temperature and humidity sensors. The environment is climate controlled. The fire suppression system is dry pipe water. There is an integrated electrical shutoff so that power is shutdown prior to the release of water. The rack doors, however, are unlocked and therefore anyone can gain entry to the racks and the machines and switches therein.
Findings (Needs Improvement)	The machine room is generally secure. However, it is easy to piggy back behind someone entering the facility. Also, there is no log out provided by the biometric device, only login. The manual sheet seems only to be used to track visitors. The water based fire suppression system would likely cause significant damage to equipment in the event of a fire that triggered the release of water.

Item Number	3
Item Title	Change Control
Purpose/Reference	Insure that only authorized changes are implemented; minimize configuration entropy of systems over time. ISO/IEC 17799 [24].
Risk	R1, R2, R3 through misconfiguration or unintended side effects of changes.

Test Procedure/ Compliance Criteria	<p>Interview Network Engineers regarding current change control process for switches.</p> <ul style="list-style-type: none"> • Is there a written change control policy? • What configuration elements are under change control? • How are configurations backed up and restored? • What is the approval process? • What is done to insure adhoc changes are not made? • How are changes tested? <p>For each item discussed as for evidence that the process is actually being employed.</p>
Test Nature	Objective
Evidence	<p>Change control policy:</p> <p>The following is an excerpt from the written change control policy.</p> <p>Network adds, moves, and changes NCR database – all adds moves and changes are tracked and recorded in the NCR database. Network Engineering is currently investigating new software programs to record this information, as well as additional capabilities. ACS database – all adds moves and changes are tracked and recorded in the ACS database. Network Engineering is currently investigating new software programs to record this information, as well as additional capabilities. LRINFO database - all adds moves and changes are tracked and recorded in the LRINFO database. Network Engineering is currently investigating new software programs to record this information, as well as additional capabilities. NETWORK database – all adds moves and changes are tracked and recorded in the MS Access database in the NETWORK file space. This database includes information on all network devices (routers, switches, wireless, etc...) on and off site. This file space is also utilized as a central location for the backup and storage of the running configurations of the network devices. Each running configuration that is made to a network device on campus is backed up to a TFTP server in the Networking lab. Once a week, the folder containing the running configurations is backed up to the NETWORK file space. The file space is then backed up to tape each night. This ensures a high level of redundancy, in the event of a problem with hardware, software or configurations.</p> <p>Network Addresses, end user jack assignments, device configurations, and IOS are under change control.</p> <p>The configurations are stored in central file space and backed up using that systems standard backup rotation.</p> <p>There is no approval process, engineers are free to make changes as they see fit.</p> <p>There is no enforcement or audit of the change control</p>

	process. IOS versions are tested using representative lab equipment. There is no formal testing process for configuration changes.
Findings (Needs Improvement)	Change control as it pertains to the device being audited could be strengthened. The IOS versions are adequately tested, applied in a timely fashion, and kept current. The configurations are backed up, but there is no history of change (version control). Also, because there are no individually identifiable accounts the person responsible for implementing a particular change cannot be determined. There is no approval or review of configuration changes.

Item Number	7
Item Title	Password Management
Reference	Proper password management is a basic component of device security. Hardening Cisco Routers [13]
Risk	R5 – Weak passwords, R9 – Unauthorized virtual access
Test Procedure/ Compliance Criteria	<p>The following account/password configuration entries are found in the switch configuration using the “show run” command executed from the enable prompt on the switch. Verify that the passwords are encrypted to the extent possible and that enable secret is used. Make sure that uniquely identifiable user accounts are created. In this case locally. They will not appear together in the configuration file.</p> <pre> service password-encryption ! enable secret 5 \$1\$V5gO\$UhyUkUk9mf3wu5b677ua1 ! line con 0 password 7 050C090633455D01 line vty 0 4 access-class 10 in password 7 094B41000B0C041A login local transport input ssh line vty 5 15 </pre>

	<pre>access-class 10 in password 7 094B41000B0C041A login local transport input ssh ! end</pre> <p>Observe a network engineer logon to the switch. Insure that he/she is prompted for a userid.</p> <p>Note: Line aux is not applicable on the 3550. No central authentication system is currently utilized in this environment.</p>
Test Nature	Objective
Evidence	<p>The following lines were extracted from the configuration file.</p> <pre>no service password-encryption enable secret 5 \$gdhddjksdirwororororororo/ line con 0 password in-the-clear line vty 0 4 password in-the-clear login line vty 5 15 login</pre> <p>No password entry for vty 5 15 was found. No login local or other individually identifying logon method (TACACS/RADIUS) was found.</p> <p>The following logon was observed.</p> <p>User Access Verification</p> <pre>Password: switch1>en Password: switch1#</pre>
Findings (FAIL)	<p>The most critical element “enable secret” is used. Users are not individually identifiable which makes it difficult to manage change control and/or insure the integrity of the configuration. It also reduces the effectiveness of logging. The login (non-privileged) passwords were in the clear. This is an issue, as it is easier to unintentionally disclose the passwords. Finally the passwords are not uniformly applied to all the vty interfaces in</p>

	the configuration.
--	--------------------

Item Number	9
Item Title	Virtual Access - SSH
Purpose/Reference	Clear text protocols make capture of userids and password easy. This item determines what protocols are being used for administrative access. Failing to constrain access increases these risks. Hardening Cisco Routers[13]. CIS RAT Checklist [19].
Risk	R9 – Unauthorized virtual access, R10 - Telnet
Test Procedure/Compliance Criteria	<p>Verify that only SSH is allowed and that access is restricted by ACL to specific hosts. Insure that administrators are using SSHv2.</p> <p>Example:</p> <pre> access-list 10 permit 192.168.1.253 access-list 10 deny any ! line vty 0 4 access-class 10 in password 7 094B41000B0C041A login local transport input ssh line vty 5 15 access-class 10 in password 7 094B41000B0C041A login local transport input ssh ! </pre> <p>Insure that SSH is the only service running on the switch. Do this by placing a computer on the management VLAN and using nmap to portscan the switches IP address.</p> <pre> C:\>nmap -sS -v -p 1-65535 -P0 192.168.1.254 </pre> <p>Starting nmap V. 3.00 (www.insecure.org/nmap) Host (192.168.1.254) appears to be up ... good. Initiating SYN Stealth Scan against (192.168.1.254) Adding open port 22/tcp</p>

The SYN Stealth Scan took 72 seconds to scan 65535 ports.

Interesting ports on (192.168.1.254):

(The 65534 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh

Nmap run completed -- 1 IP address (1 host up) scanned in 92 seconds

Use a tool like putty (ssh client) and observe a network engineer log in. Does the tool accept the certificate from SSH? Is the SSH session properly established? Note the key size in the window. In this example it is 512. A length of 1024 would be preferred.



The following logon was captured and analyzed with ethereal.

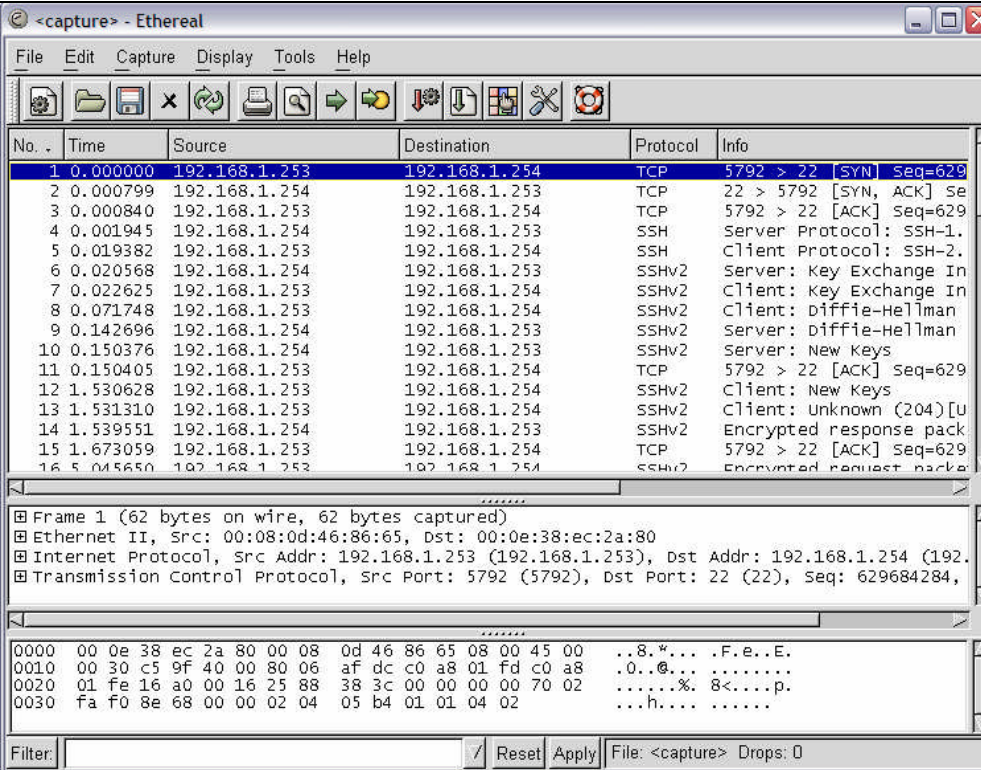
login as: rwindig

rwindig@192.168.1.254's password:

switch1>en

Password:

switch1#

	 <p>Note the SSHv2 in the example. This is the correct response. You must insure that the SSH client is configured for SSHv2 as the switch will allow SSHv1 connections.</p>
Test Nature	Objective
Evidence	<p>The configuration shows the following line definitions.</p> <pre> line vty 0 4 password in-the-clear login line vty 5 15 login </pre> <p>SSH is not being used. The default is telnet. This is confirmed by the below nmap scan. There are no access lists constraining the control plane (management VLAN).</p> <pre> C:\Program Files\Tripwire\TFS\bin>nmap -sS -P0 -p 1-65535 172.19.xxx.yyyy Starting nmap V. 3.00 (www.insecure.org/nmap) Interesting ports on (172.19.xxx.yyy): (The 65530 ports scanned but not shown below are in state: closed) Port State Service </pre>

	21/tcp filtered ftp 23/tcp open telnet 135/tcp filtered loc-srv 1002/tcp filtered unknown 1720/tcp filtered H.323/Q.931 Nmap run completed -- 1 IP address (1 host up) scanned in 163 seconds C:\Program Files\Tripwire\TFS\bin>
Findings (FAIL)	This switch is being accessed remotely via telnet only. This is a significant risk as telnet is a clear text protocol therefore the passwords, including the enable password can be sniffed by any computer on the control plane. Further, access is not restricted to a specific machine or set of machines. This enables a potential brute force password attack and/or facilitates access is the password is compromised. The additional services detected by nmap should be investigated and a determination made as to whether or not they should be running. Every service creates potential vulnerability.

Item Number	10
Item Title	IOS Version
Purpose/Reference	Insure that the IOS is being properly maintained to reduce the risk of exploits of known vulnerabilities. KBeta, Improving Security on Cisco Routers[14]
Risk	R4 – IOS Software not being maintained.
Test Procedure/ Compliance Criteria	The “show version” command issued at the enable prompt is used to determine the IOS version running on the device. The first few lines show the version and image file. Example: switch1#show version Cisco Internetwork Operating System Software IOS (tm) C3550 Software (C3550-I5K2L2Q3-M), Version 12.1(19)EA1c, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2004 by cisco Systems, Inc. Compiled Tue 03-Feb-04 10:39 by yenanh Image text-base: 0x00003000, data-base: 0x009428D4 ROM: Bootstrap program is C3550 boot loader

	<p>switch1 uptime is 17 hours, 24 minutes</p> <p>System returned to ROM by power-on</p> <p>System image file is "flash:c3550-i5k2l2q3-mz.121-19.EA1c/c3550-i5k2l2q3-mz.121-19.EA1c.bin"</p> <p>Output truncated for brevity.</p> <p>Compare the version listed with the latest release. All IOS software can be found at http://www.cisco.com/kobayashi/sw-center . Following the lan switching software link the 3550 software can be found at http://www.cisco.com/cgi-bin/tablebuild.pl/cat3550. The network engineer will need to provide access. Public access to product releases can be obtained by searching www.cisco.com, example: http://www.cisco.com/en/US/products/hw/switches/ps646/prod_bulletin09186a00801ce930.html however this is not always current.</p> <p>If the version running is not the current version interview engineer on IOS upgrade policy. Does the version reflect the policy?</p> <p>Check to see if there are any known vulnerabilities in the running version. Vulnerabilities can be found at http://www.cisco.com/warp/public/707/advisory.html , http://www.securityfocus.com/bid/vendor/ [21], and http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=cisco [22]</p>
Test Nature	Objective
Evidence	<p>The following version of IOS is running on the switch.</p> <pre>OpsSwitch#sh ver Cisco Internetwork Operating System Software IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(19)EA1a, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Tue 09-Dec-03 03:01 by yenanh Image text-base: 0x00003000, data-base: 0x0069B37C ROM: Bootstrap program is C3550 boot loader OpsSwitch uptime is 14 weeks, 6 days, 5 hours, 15 minutes System returned to ROM by power-on</pre>

System image file is "flash:c3550-i9q3l2-mz.121-19.EA1a/c3550-i9q3l2-mz.121-19.EA1a.bin"			
<i>! CLIPPED FOR BREVITY</i>			
OpsSwitch#			
Below is the most recent releases of IOS with Cryptographic software to support SSH.			
<u>Filename</u>	<u>Release</u>	<u>Date</u>	<u>Size (Bytes)</u>
c3550-i5k2l2q3-mz.121-20.EA1a.bin C3550 EMI IOS CRYPTO IMAGE	12.1.20.EA1a	21-APR-2004	4910444
c3550-i5k2l2q3-tar.121-20.EA1a.tar C3550 EMI IOS CRYPTO IMAGE AND CMS FILES	12.1.20.EA1a	21-APR-2004	8140800
c3550-i9k2l2q3-mz.121-20.EA1a.bin C3550 SMI IOS CRYPTO IMAGE	12.1.20.EA1a	21-APR-2004	4156564
c3550-i9k2l2q3-tar.121-20.EA1a.tar C3550 SMI IOS CRYPTO IMAGE AND CMS FILES	12.1.20.EA1a	21-APR-2004	7393280
c3550-i5k2l2q3-mz.121-19.EA1c.bin C3550 EMI IOS CRYPTO IMAGE	12.1.19.EA1c	19-FEB-2004	4864984
c3550-i5k2l2q3-tar.121-19.EA1c.tar C3550 EMI IOS CRYPTO IMAGE AND CMS FILES	12.1.19.EA1c	19-FEB-2004	7901696
c3550-i9k2l2q3-mz.121-19.EA1c.bin C3550 SMI IOS CRYPTO IMAGE	12.1.19.EA1c	19-FEB-2004	4114101
c3550-i9k2l2q3-tar.121-19.EA1c.tar C3550 SMI IOS CRYPTO	12.1.19.EA1c	19-FEB-2004	7151104

	<p>IMAGE AND CMS FILES</p> <p>Next a search is performed to determine if the current IOS version has any security issues. From http://www.cisco.com/warp/public/707/advisory.html :</p> <table><thead><tr><th>Title</th><th>First Published</th><th>Last Updated</th></tr></thead><tbody><tr><td>Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products</td><td>April 20, 2004</td><td>April 25, 2004</td></tr><tr><td>Cisco Security Advisory: Vulnerabilities in SNMP Message Processing</td><td>April 20, 2004</td><td>April 23, 2004</td></tr></tbody></table> <p>From http://www.securityfocus.com/bid/vendor/ :</p> <p>No new information.</p> <p>From http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=cisco</p> <p>No new information.</p>	Title	First Published	Last Updated	Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products	April 20, 2004	April 25, 2004	Cisco Security Advisory: Vulnerabilities in SNMP Message Processing	April 20, 2004	April 23, 2004
Title	First Published	Last Updated								
Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products	April 20, 2004	April 25, 2004								
Cisco Security Advisory: Vulnerabilities in SNMP Message Processing	April 20, 2004	April 23, 2004								
Findings (PASS)	<p>The IOS version is reasonably up to date. It is one version behind and potentially subject to the above described DOS attacks. However, there is a tradeoff between the urgency of an update, it's proven reliability in the field. GIAC Enterprises is using reasonable and appropriate judgment with respect to IOS currency. However a written policy was not available for review.</p>									

	<p>The IOS version being used doesn't support SSH.</p> <p>A robust upgrade policy should be used to determine the oldest version that would expected to be found on a switch. I.e. XYZ Enterprises upgrades to the latest version IOS no later than three months after its initial release. Of course, the criticality of the upgrade may require more rapid deployment.</p>
--	--

Item Number	12
Item Title	Management VLAN Isolation
Purpose/Reference	Insure that management traffic is isolated from user traffic. Network Infrastructure Security Checklist [5].
Risk	R5 – Weak passwords, R6 – Rogue machine on network, R9 – Unauthorized virtual access.
Test Procedure/ Compliance Criteria	<p>Issue the "show run" command from the enable prompt. The VLAN used for management will have an IP address associated with it. The IP address can only be accessed by ports that belong to this VLAN.</p> <p>Example:</p> <pre>interface Vlan100 ip address 192.168.1.254 255.255.255.0 !</pre> <p>These lines are copied from the output of a switch configuration showing the management VLAN to be Vlan100.</p> <p>Insure that the management VLAN is not used as the native VLAN.</p> <p>Example:</p> <pre>interface FastEthernet0/1 description uplink to xyzswitch switchport trunk encapsulation dot1q switchport trunk native vlan 100 switchport trunk allowed vlan 10,20,30,100,1002-1005 switchport mode trunk !</pre> <p>Check that the VTY lines and SNMP interfaces are properly constrained by ACLs.</p> <p>Example:</p>

	<pre> access-list 10 permit 192.168.1.253 access-list 10 deny any snmp-server group test-group v3 auth access 10 line con 0 password 7 050C090633455D01 line vty 0 4 access-class 10 in password 7 094B41000B0C041A login local transport input ssh line vty 5 15 access-class 10 in password 7 094B41000B0C041A login local transport input ssh </pre> <p>Check the visibility of the management VLAN by using nmap to try to find the management interface on the management VLAN from outside the management VLAN (see if it is routed widely). Check for visibility of the SNMP interface using Ireasoning's MIB browser or similar tool from outside the management network.</p>
Test Nature	Objective
Evidence	<p>The following excerpts of the 3550 configuration show the trunk ports and management VLAN designation.</p> <pre> interface FastEthernet0/48 switchport access vlan 100 switchport trunk encapsulation isl switchport trunk native vlan 100 switchport mode trunk no ip address ! interface Vlan100 ip address 172.x.y.31 255.255.254.0 ! </pre> <p>The management interface was accessible from a user network in the company. The device under audit was visible (172.x.y.31).</p>

Nmap -sT -p 22-23 172.x.y.0/23

Starting nmap V. 3.00 (www.insecure.org/nmap)

Interesting ports on (172.x.y.0):

Port	State	Service
------	-------	---------

22/tcp	filtered	ssh
--------	----------	-----

23/tcp	filtered	telnet
--------	----------	--------

Interesting ports on (172.x.y.1):

(The 1 port scanned but not shown below is in state: closed)

Port	State	Service
------	-------	---------

23/tcp	open	telnet
--------	------	--------

Interesting ports on (172.x.y.2):

(The 1 port scanned but not shown below is in state: closed)

Port	State	Service
------	-------	---------

23/tcp	open	telnet
--------	------	--------

CLIPPED FOR BREVITY

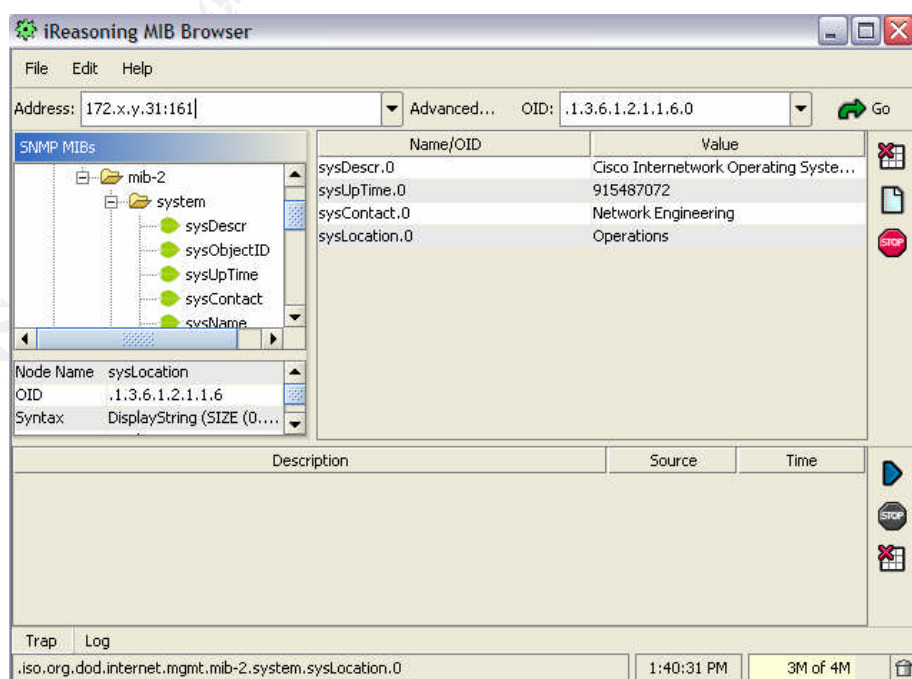
Interesting ports on (172.x.y.31):

(The 1 port scanned but not shown below is in state: closed)

Port	State	Service
------	-------	---------

23/tcp	open	telnet
--------	------	--------

SNMP test result:



Findings

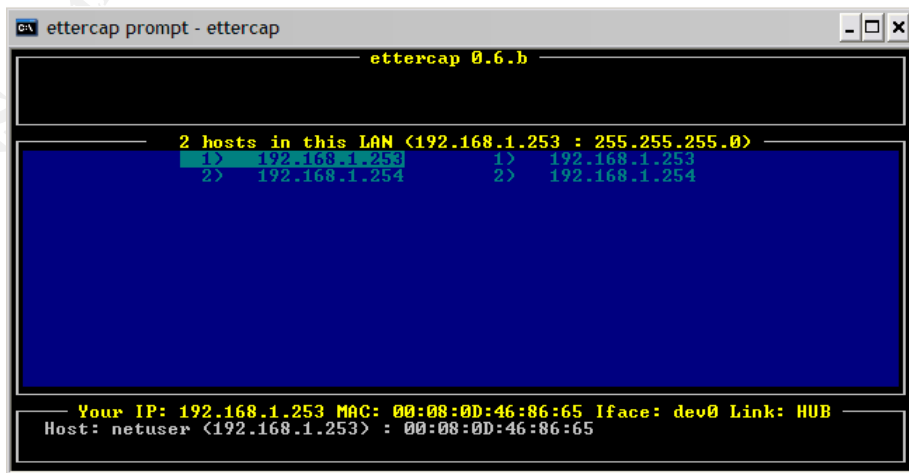
The management VLAN has been reassigned from 1 to 100. However, it is designated as the native VLAN which undermines

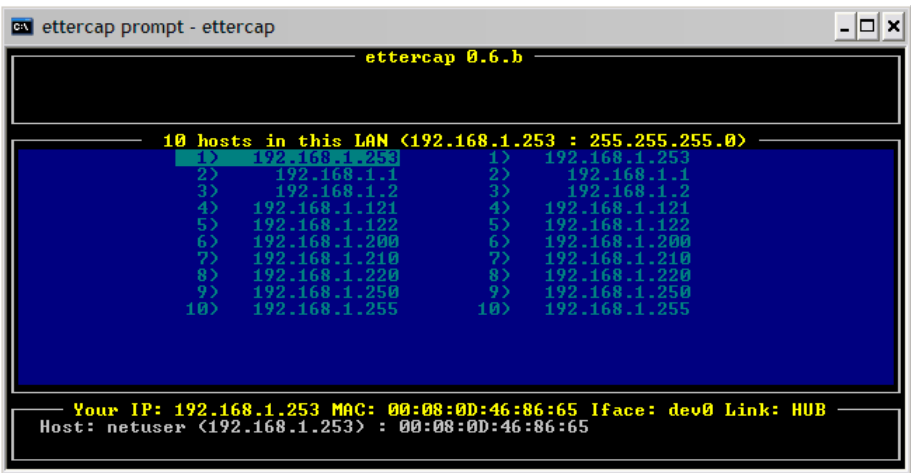
(FAIL)	the reason the VLAN number was changed. There are no restrictions limiting access to management interfaces. The management interface IP Address is routed within the organization and accessible from user networks within the company. This represents a significant risk of unauthorized access.
--------	--

Item Number	14
Item Title	Switchport Modes, Controlling Trunking
Purpose/Reference	The purpose of controlling trunking is to prevent a device from impersonating a switch and sniffing traffic on VLANs that it should not have access to. Trunking should also be constrained (pruning) so that VLANs don't propagate unintentionally and become exposed on switches that have insufficient controls applied. Virtual LAN Security Best Practices [15]. SAFE Layer 2 Security In-depth [16].
Risk	R1 – Misconfigured Port Security, R2 – VLAN not providing proper network isolation.
Test Procedure/ Compliance Criteria	<p>Verify that the switch infrastructure trunking is being properly restricted.</p> <p>Run the "show run" command from the enable prompt and examine the port configurations. They should all be either explicitly set in access mode or trunk mode.</p> <pre>switch1#sh run Building configuration... Current configuration : 5857 bytes ! interface FastEthernet0/1 switchport access vlan 200 switchport mode access no ip address shutdown ! interface FastEthernet0/19 switchport access vlan 30 switchport mode access no ip address ip access-group 100 in</pre>

	<pre>! interface FastEthernet0/48 switchport trunk encapsulation isl switchport trunk allowed vlan 10,20,30,40,50,60,100 switchport mode trunk no ip address no cdp enable !</pre> <p>The first port is unused and is shutdown. The second is set to mode access and has a ACL applied to it. The third is in trunk mode, has VLAN trunking constrained by the “allowed” command and disables Cisco Discovery Protocol (CDP). These three examples are reasonable and what you should expect to find. If there is no “allowed” command restricting VLANs then all are trunked, which is a security issue.</p> <p>The following example is how ports appear by default. They should not be left this way, as they can be negotiated into trunk mode and will forward traffic for all VLANs.</p> <pre>interface FastEthernet0/45 switchport mode dynamic desirable no ip address !</pre>
Test Nature	Objective
Evidence	<p>Two ports were found to be default configured,</p> <pre>interface GigabitEthernet0/1 switchport mode dynamic desirable no ip address !</pre> <pre>interface GigabitEthernet0/2 switchport mode dynamic desirable no ip address !</pre> <p>There is no “allowed” command restricting trunking. Cisco Discovery Protocol is enabled on the device.</p>
Findings (FAIL)	<p>Ports in default configurations can be tricked into trunking VLANs by devices that impersonate switches and negotiate trunking. In the case of a device with VLAN ACLs on ports this can completely undermine the security of the VLAN. An</p>

	<p>intruder can trunk the ACL secured VLAN and define a port with no ACLs. In this configuration ettercap in ARP spoof mode can affect a man in the middle attack and successfully eavesdrop on traffic that is thought to be secure.</p> <p>A similar situation can occur if someone has access to a switch that is trunked to the switch. With no restrictions a port can simply be defined for any VLAN of interest and then a variety of attacks can be made possible. For instance, it may be possible to circumvent firewall rules by placing a computer with two network interfaces in switchports configured to VLANs that should not be able to traverse traffic. The computer then acts as a router and bypasses the firewall.</p>
--	--

Item Number	15
Item Title	VLAN visibility
Purpose/Reference	Inventory machines on each trunked VLAN. Insure that machines discovered on the VLANs are supposed to be there. Inventory the management VLAN. Ref: Independent Idea and experience.
Risk	R2 – VLAN not providing proper network isolation.
Test Procedure/ Compliance Criteria	<p>You will need to use a port on the switch. Ask for change control records of what machines should be on each VLAN. Have the engineer set your access port to each VLAN in succession. For each VLAN run ettercap in arp flood mode and see if the ip addresses you find match the expected inventory. The following is a screen shots are the result of ettercap arp floods on a 3550 switch. The first is on the management VLAN (Vlan100).</p>  <p>The screenshot shows a terminal window titled 'ettercap prompt - ettercap' with the version 'ettercap 0.6.b'. It displays the results of an ARP flood on the management VLAN (Vlan100). The output indicates '2 hosts in this LAN (192.168.1.253 : 255.255.255.0)'. Below this, it lists two hosts: 1) 192.168.1.253 and 2) 192.168.1.254. At the bottom, it shows the user's IP as 192.168.1.253, MAC as 00:08:0D:46:86:65, interface as dev0, and link as HUB. The host being targeted is netuser (192.168.1.253) with MAC 00:08:0D:46:86:65.</p> <p>Note just the sensing notebook and the switch management IP</p>

	<p>are seen. Next an arp flood of Vlan60.</p>  <pre>ettercap prompt - ettercap ettercap 0.6.b 10 hosts in this LAN (192.168.1.253 : 255.255.255.0) 1> 192.168.1.253 1> 192.168.1.253 2> 192.168.1.1 2> 192.168.1.1 3> 192.168.1.2 3> 192.168.1.2 4> 192.168.1.121 4> 192.168.1.121 5> 192.168.1.122 5> 192.168.1.122 6> 192.168.1.200 6> 192.168.1.200 7> 192.168.1.210 7> 192.168.1.210 8> 192.168.1.220 8> 192.168.1.220 9> 192.168.1.250 9> 192.168.1.250 10> 192.168.1.255 10> 192.168.1.255 Your IP: 192.168.1.253 MAC: 00:08:0D:46:86:65 Iface: dev0 Link: HUB Host: netuser (192.168.1.253) : 00:08:0D:46:86:65</pre> <p>This scan shows the sensing notebook and several other machines on this VLAN. Note that the management IP address is no longer visible. In a machine room environment with sensitive data it is important to insure that only known machines are on a particular VLAN</p> <p>Next use tcpdump or windump to listen for IP addresses that are not in the subnet range of the VLAN. This may uncover unexpected management traffic, misconfigured machines.</p>
Test Nature	Objective
Evidence	The following is a list of IP addresses found on the storage network Vlan40.

```

ettercap prompt - ettercap
SOURCE: 172. .109 00:01:00:02:00:03

33 hosts in this LAN (172. .109 : 255.255.255.0)
1> 172. .109 172. .109
2> 172. .109 172. .109
3> 172. .109 172. .109
4> 172. .109 172. .109
5> 172. .109 172. .109
6> 172. .109 172. .109
7> 172. .109 172. .109
8> 172. .109 172. .109
9> 172. .109 172. .109
10> 172. .109 172. .109
11> 172. .109 172. .109
12> 172. .109 172. .109
13> 172. .109 172. .109
14> 172. .109 172. .109
15> 172. .109 172. .109
16> 172. .109 172. .109
17> 172. .109 172. .109
18> 172. .109 172. .109
19> 172. .109 172. .109
20> 172. .109 172. .109
21> 172. .109 172. .109
22> 172. .109 172. .109
23> 172. .109 172. .109
24> 172. .109 172. .109
25> 172. .109 172. .109
26> 172. .109 172. .109
27> 172. .109 172. .109
28> 172. .109 172. .109
29> 172. .109 172. .109
30> 172. .109 172. .109
31> 172. .109 172. .109
32> 172. .109 172. .109
33> 172. .109 172. .109

Your IP: 172. .109 MAC: 00:01:00:02:00:03 Iface: dev0 Link: HUB
Host: netuser (172. .109) : 00:01:00:02:00:03

```

Inventory of machines on this subnet/VLAN:

172.x.y.2	neta2.x.y.z	neta2
172.x.y.3	netb2.x.y.z	netab2
172.x.y.4	test3b.x.y	test3b
172.x.y.5	test4b.x.y	test4b
172.x.y.6	prod3b.x.y	prod3b
172.x.y.7	prod4b.x.y	prod4b
172.x.y.8	cletp4b.x.y	cletp4b
172.x.y.9	prodb.x.y.z	prodb
172.x.y.10	ffdsfsb.x.y.z	ffdsfsb
172.x.y.11	tp5b.x.y	tp5b
172.x.y.12	server2b.x.y.z	server2b
172.x.y.20	prodlb.x.y.z	prodlb
172.x.y.21	prod2b.x.y.z	prod2b
172.x.y.22	fender2.x.y.z	fender2
172.x.y.23	testb.x.y.z	testb
172.x.y.24	devb.x.y.z	devb
172.x.y.25	pprdb.x.y.z	pprdb
172.x.y.26	serverdb1.a.x.y	serverdb1

```
172.x.y.27 server1.a.x.y server1
172.x.y.28 serverb1.a.x.y serverb1
172.x.y.29 sdb2.a.x.y sdb2
172.x.y.30 spare1.b.x.y spare1
172.x.y.31 backup1.b.x.y backup1
172.x.y.32 ledbl.b.x.y ledbl
172.x.y.33 servera2.b.x.y servera2
172.x.y.34 serverb2.b.x.y serverb2
172.x.y.35 serverdb2.b.x.y serverdb2
172.x.y.36 serverappl.b.x.y serverappl
172.x.y.37 servercts1.b.x.y servercts1
172.x.y.38 spare2.b.x.y spare2
172.x.y.39 backup1.b.x.y backup1
```

Next, using windump or tcpdump, traffic is captured to see if any machines have IP address not in the subnet (misconfigured).

```
C:\>windump -i 1 -n not net 172.x.y.0/24
```

```
windump: listening on \Device\NPF_{D1FCF397-F77D-4FE0-92FB-99E00305BB4F}
```

```
11:15:38.484925 802.1d config 83a2.00:ff:ee:dd:10:80.8017 root
8000.00:05:31:38:
```

```
f9:a2 pathcost 25 age 3 max 20 hello 2 fdelay 15
```

```
11:15:40.484900 802.1d config 83a2.00:ff:ee:dd:10:80.8017 root
8000.00:05:31:38:
```

```
f9:a2 pathcost 25 age 3 max 20 hello 2 fdelay 15
```

```
11:15:42.486787 802.1d config 83a2.00:ff:ee:dd:10:80.8017 root
8000.00:05:31:38:
```

CUT FOR BREVITY

```
f9:a2 pathcost 25 age 3 max 20 hello 2 fdelay 15
```

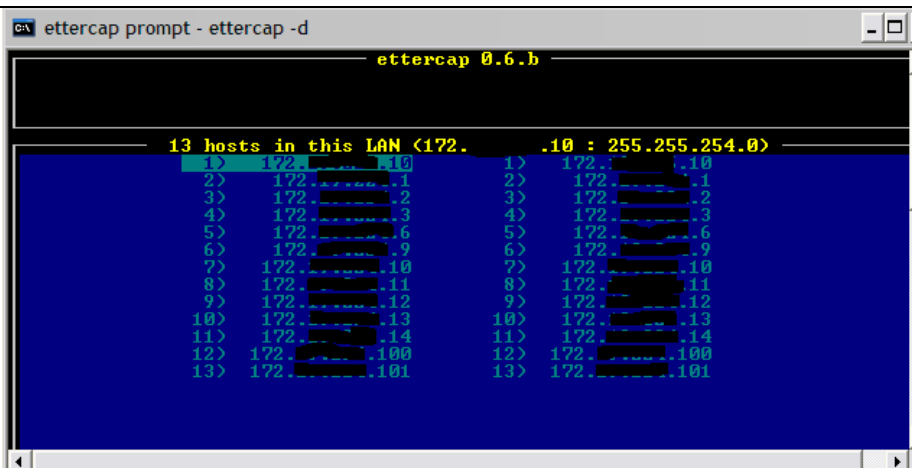
```
11:18:24.487619 802.1d config 83a2.00:ff:ee:dd:10:80.8017 root
8000.00:05:31:38:
```

```
f9:a2 pathcost 25 age 3 max 20 hello 2 fdelay 15
```

```
118 packets received by filter
```

```
0 packets dropped by kernel
```

The following is a list of IP addresses found on the Admin-DMZ network Vlan20.



From machine inventory:

Int1-admin-dmz 172.x.y.1
 int2-admin-dmz 172.x.y.2
 int3-admin-dmz-vip 172.x.y.3
 zprintsvc 172.x.y.10
 lumabcde3 172.x.y.11
 lumabcde4 172.x.y.12
 server-devl 172.x.y.13
 banabcdef1 172.x.y.100
 banabcdef2 172.x.y.101
 biztuvxyz1 172.x.y.115
 serverapp1 172.x.y.113

Listening for machines with IP that are not in the subnet (misconfigured):

C:\>windump -i 1 -n not net 172.x.y.0/23

windump: listening on \Device\NPF_{D1FCF397-F77D-4FE0-92FB-99E00305BB4F}

11:25:37.602625 arp who-has 192.168.1.3 tell 192.168.1.5

11:25:37.753211 802.1d config 83d3.00:ff:ee:dd:10:80.8017 root 8000.00:07:eb:cd:

ab:07 pathcost 25 age 3 max 20 hello 2 fdelay 15

11:25:39.753544 802.1d config 83d3.00:ff:ee:dd:10:80.8017 root 8000.00:07:eb:cd:

ab:07 pathcost 25 age 3 max 20 hello 2 fdelay 15

11:25:40.588546 arp who-has 192.168.1.3 tell 192.168.1.5

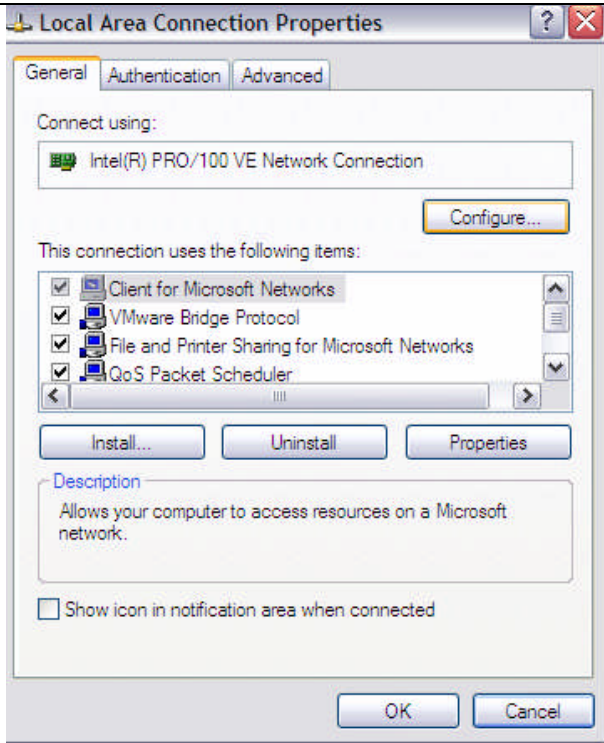
11:25:41.588367 arp who-has 192.168.1.3 tell 192.168.1.5

CUT FOR BREVITY

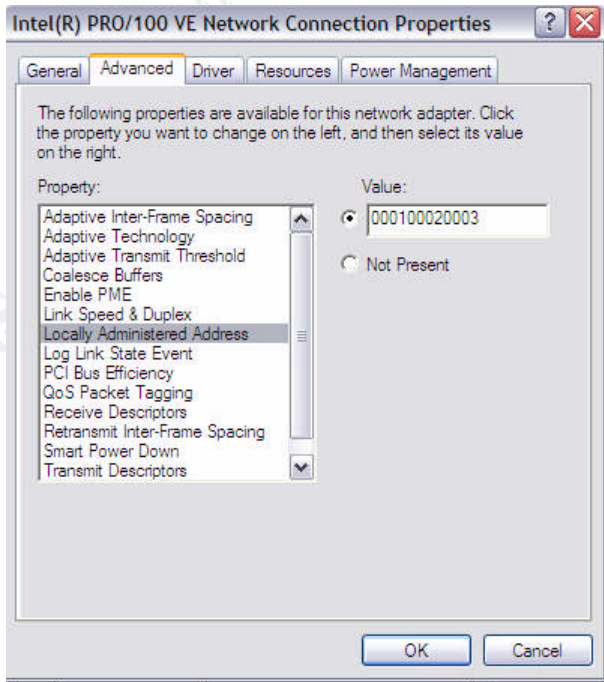
	<p>11:26:47.779792 802.1d config 83d3.00:ff:ee:dd:10:80.8017 root 8000.00:07:eb:cd:</p> <p>ab:07 pathcost 25 age 3 max 20 hello 2 fdelay 15</p> <p>93 packets received by filter 0 packets dropped by kernel</p> <p>The remaining VLANs yield no new findings and are omitted for brevity. They would be included in an actual audit.</p>
Findings (FAIL)	<p>There were thirty one machines listed in the subnet inventory for the storage network, Vlan40. Thirty two machines were found to respond to ARP requests on the LAN. One machine listed in inventory did not respond. Listening on the network for machines with IP addresses not in the network yielded no result.</p> <p>In the Admin-DMZ network, Vlan20 there were 13 IP addresses discovered by using ARP requests. Comparing that to the inventory there are 3 IP addresses that were discovered by ARP but not listed in the inventory. There were 2 machines listed in the inventory that do not appear to be on the network. Listening for machines with IP addresses that are not in the subnet detected a misconfigured machine ARP'ing for an invalid gateway address.</p> <p>The discovered inventory differed from the documented inventory. Controls should be strengthened to insure that all machines on machine room VLANs are known and documented.</p>

Item Number	16
Item Title	Port Security
Purpose/Reference	Port security will prevent a rogue machine from being plugged into a previously occupied port without proper authorization and coordination. It also limits the ability of a legitimate machine to do things like MAC flooding. This configuration is only used on the storage network by policy. Securing the LAN with Catalyst 3550 and 2950 Series Switches[8]. SAFE Layer 2 Security In-Depth [16]
Risk	R1, R2, R3 through misconfiguration or unintended side effects of changes.
Test Procedure/ Compliance Criteria	<p>Run the "show run" command at the enable prompt. Review the ports in the VLAN of interest and make sure that they all have port security configure similar to the below example.</p> <pre>interface FastEthernet0/45 switchport access vlan 40</pre>

	<pre>switchport mode access switchport port-security switchport port-security violation restrict switchport port-security mac-address 00c0.f040.5ec4 no ip address !</pre> <p>Note, there may be other entries such as ACL restrictions.</p> <p>If possible try to verify the configuration by cloning it to a spare port, of course changing the MAC to one suitable for testing, say 0001.0001.0001.</p> <pre>switch1(config)#int fa0/40 switch1(config-if)#interface FastEthernet0/40 switch1(config-if)# switchport access vlan 40 switch1(config-if)# switchport mode access switch1(config-if)# switchport port-security switch1(config-if)# switchport port-security violation restrict switch1(config-if)# switchport port-security mac-address 0001.0001.0001 switch1(config-if)# no ip address switch1(config-if)#exit</pre> <p>You can change the MAC on your notebook (usually) by doing the following:</p> <p>Go to your network connection dialog and click “configure” under the hardware section.</p>
--	---



Next under the advanced tab you can configure the Locally Administered Address (MAC) to the value you specified in the switchport configuration. This method may vary by NIC manufacturer but should be similar.



Having done that ping the gateway address or a machine on the

	<p>VLAN that will respond to ICMP echo requests. Next change your MAC and see if you become unable to ping. Have someone monitor the port security status using “sh port-security” from the enable prompt on the switch. Here’s what it looks like.</p> <pre>switch1#sh port-security</pre> <table><thead><tr><th>Secure Port</th><th>MaxSecureAddr (Count)</th><th>CurrentAddr (Count)</th><th>SecurityViolation (Count)</th><th>Security Action</th></tr></thead><tbody><tr><td>Fa0/40</td><td>1</td><td>1</td><td>6</td><td>Restrict</td></tr><tr><td>Fa0/45</td><td>1</td><td>1</td><td>0</td><td>Restrict</td></tr></tbody></table> <p>-----</p> <p>Total Addresses in System (excluding one mac per port) : 0 Max Addresses limit in System (excluding one mac per port) : 5120</p> <pre>switch1#sh port-security</pre> <table><thead><tr><th>Secure Port</th><th>MaxSecureAddr (Count)</th><th>CurrentAddr (Count)</th><th>SecurityViolation (Count)</th><th>Security Action</th></tr></thead><tbody><tr><td>Fa0/40</td><td>1</td><td>1</td><td>24</td><td>Restrict</td></tr><tr><td>Fa0/45</td><td>1</td><td>1</td><td>0</td><td>Restrict</td></tr></tbody></table> <p>-----</p> <p>Total Addresses in System (excluding one mac per port) : 0 Max Addresses limit in System (excluding one mac per port) : 5120</p> <p>You can see the security violations counted as the pings are attempted. The pings, of course fail. If any alerts are monitored for MAC address change, verify that this change is detected and acted upon. Finally change the MAC address back and verify that you can once again ping your target.</p> <p>The “ipconfig /all” command on a Windows XP, 2K machine will show MAC information. The “ifconfig –a” command on Linux/Unix variants accomplished the same thing.</p> <p>Note: this technique can be used to circumvent port security if the MAC addresses of the legitimate machines are known.</p>	Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action	Fa0/40	1	1	6	Restrict	Fa0/45	1	1	0	Restrict	Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action	Fa0/40	1	1	24	Restrict	Fa0/45	1	1	0	Restrict
Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action																											
Fa0/40	1	1	6	Restrict																											
Fa0/45	1	1	0	Restrict																											
Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action																											
Fa0/40	1	1	24	Restrict																											
Fa0/45	1	1	0	Restrict																											
Test Nature	Objective																														
Evidence	A review of the switch configuration showed that there are no switchports configured to use port security. A notebook was used to verify that the MAC could be changed with no loss of connectivity.																														

	<pre>C:\>ipconfig /all Windows IP Configuration Host Name : netuser Primary Dns Suffix : Node Type : Hybrid IP Routing Enabled. : No WINS Proxy Enabled. : No Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . : Description : Intel(R) PRO/100 VE Network Connecti on Physical Address. : 00-01-00-02-00-03 Dhcp Enabled. : No IP Address. : 172.x.y.253 Subnet Mask : 255.255.254.0 Default Gateway : 172.x.y.1 DNS Servers : a.b.c.d C:\> C:\>ping 172.x.y.1 Pinging 172.x.y.1 with 32 bytes of data: Reply from 172.x.y.1: bytes=32 time=1ms TTL=255 Reply from 172.x.y.1: bytes=32 time<1ms TTL=255 Reply from 172.x.y.1: bytes=32 time<1ms TTL=255 Reply from 172.x.y.1: bytes=32 time<1ms TTL=255 Ping statistics for 172.x.y.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre>
--	--

	<pre>C:\> C:\>ipconfig /all Windows IP Configuration Host Name : netuser Primary Dns Suffix : Node Type : Hybrid IP Routing Enabled. : No WINS Proxy Enabled. : No Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . : Description : Intel(R) PRO/100 VE Network Connecti on Physical Address. : 00-01-00-01-00-01 Dhcp Enabled. : No IP Address. : 172.x.y.253 Subnet Mask : 255.255.254.0 Default Gateway : 172.x.y.1 DNS Servers : a.b.c.d C:\> C:\>ping 172.x.y.1 Pinging 172.x.y.1 with 32 bytes of data: Reply from 172.x.y.1: bytes=32 time=1ms TTL=255 Reply from 172.x.y.1: bytes=32 time<1ms TTL=255 Reply from 172.x.y.1: bytes=32 time<1ms TTL=255 Reply from 172.x.y.1: bytes=32 time<1ms TTL=255 Ping statistics for 172.x.y.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),</pre>
--	--

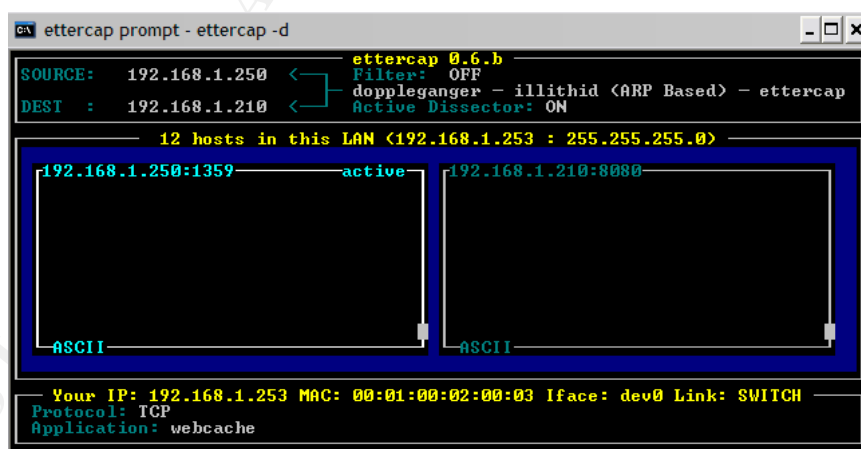
	<p>Approximate round trip times in milli-seconds:</p> <p>Minimum = 0ms, Maximum = 1ms, Average = 0ms</p> <p>C:\></p>
Findings (FAIL)	Port security is not used on this switch. This leaves the switch open to unauthorized access to sensitive VLANs.

Item Number	17
Item Title	VLAN ACLs
Purpose/Reference	VLAN ACLs can be used to restrict access between hosts on the same VLAN or on the network in general. In the context of this audit all machines on the storage network (Vlan40) are restricted by ACL to only talk to the storage filer.
Risk	R1, R3 – Misconfiguration can result in non-compliance with the network traffic policy.
Test Procedure/ Compliance Criteria	<p>There are two principal reasons to use VLAN ACLs. One is to restrict a machine's traffic by explicitly permitting or denying the traffic by the policy implemented using ACLs. The second, used in this case, to prevent eavesdropping by restricting all machines on the VLAN to send traffic only to the network storage system. The machines are dual homed and only the storage interface is affected.</p> <p>Note: Switch ACLs are only assigned inbound to the interface. There are no outbound ACLs.</p> <p>In both cases, nmap can be used to scan the subnet to determine if the IP Addresses and ports are properly constrained by the policy. To do this, clone the configuration of an ACL restricted port to a spare port. Then perform the scan on the spare port. Verify that nmap cannot "see" any machines or services that the ACLs are designed to restrict.</p> <p>The second is a little trickier and is not really scalable. It requires that every port in the VLAN have the same ACL with respect to the secure data path. If a port on the VLAN isn't restricted in this way it can successfully execute a man in the middle attack and eavesdrop the data.</p> <p>To verify consistent configuration use the "show run" command on every switch that carries the VLAN in question. Verify that each port is correctly configured.</p>

	Clone a port and use ettercap to see if you can perform a man in the middle attack. This must be carefully scheduled as such an attack could result in a service outage or significant performance degradation. For this reason a test which is used to simulate the audit tests for this paper.
Test Nature	Objective
Evidence	<p>An excerpt from the “show run” command indicates that all ports on the storage area network of switch one are configured consistently.</p> <pre> ! interface FastEthernet0/37 switchport access vlan 40 switchport mode access no ip address ip access-group 100 in spanning-tree portfast ! interface FastEthernet0/38 switchport access vlan 40 switchport mode access no ip address ip access-group 100 in spanning-tree portfast ! CLIPPED FOR BREVITY interface FastEthernet0/47 switchport access vlan 40 switchport mode access no ip address ip access-group 100 in spanning-tree portfast ! However, examination of an upstream switch with the storage network trunked to it shows unused ports configured on the storage network without the correct ACL applied. ! interface FastEthernet0/16 </pre>

```
switchport access vlan 40
switchport mode access
no ip address
spanning-tree portfast
!
interface FastEthernet0/17
switchport access vlan 40
switchport mode access
no ip address
spanning-tree portfast
!
```

The configuration of port fa0/47 is used on port fa0/23 (a port reserved for security purposes on the switch). The resulting ettercap command and screenshot, finds IP addresses but does not result in a successful man-in-the-middle attack. It does, however, have the effect of an intermittent DOS attack. As the ARP cache of the source machine is poisoned, its traffic is black holed until a cache refresh occurs. This could disrupt operations. Note: this step was performed in a lab environment, not on the production switch.



The above screen shows the attempted attack from 192.168.1.253 trying to eavesdrop on a http request from 192.168.1.250 to 192.168.1.210. The 192.168.1.210 is simulating the file server on the storage network and the 192.168.1.250 machine is simulating a client. ARP poisoning was effective but traffic could not be received do to consistent application of the ACLs. The machine making the request suffered from intermittent connectivity as it's ARP cache was poisoned and flushed.

Next the switchport the attacking machine is on is configured

without the ACL. All other ACLs are in place. This simulates a notebook being plugged into the unused and misconfigured jack on the upstream switch with the storage network VLAN on it. The below screen shots show that this configuration allows eavesdropping to occur.

The first screenshot shows the Ettercap 0.6.b interface with the following configuration:

```

SOURCE: 192.168.1.250 <
DEST : 192.168.1.210 <
Filter: OFF
doppleganger - illithid (ARP Based) - ettercap
Active Dissector: ON
  
```

Below the configuration, it lists 12 hosts in the LAN (192.168.1.253 : 255.255.255.0). The hosts are listed in a table with columns for IP, MAC, and Application. The applications are mostly 'webcache'.

The second screenshot shows the same interface with a captured packet. The packet is from 192.168.1.210:8080 to 192.168.1.253:8080. The application is 'webcache'. The packet content is a HTML document from '004 Cable News Network LP, LLLP'.

Findings
(FAIL)

The security of the data paths between servers and the filer on the storage network can be compromise by a misconfigured port. Such a port was found an upstream switch which carried the storage network VLAN. If VLAN ACLs are used for this purpose changes to the VLAN must be carefully controlled and verified not to undermine the stated security objectives of the VLAN.

4. Audit Report

4.1 Executive Summary

This audit was designed to determine the extent to which sound security practices are being applied to the switch infrastructure of GIAC Enterprises. The focus of the audit centers on the Cisco 3550 intelligent switch which is widely deployed in GIAC's machine room. The specific switch investigated is used to provide network connectivity and a layer of security to the company's IBM p670 mainframe. It is difficult to fully assess a switch in isolation. Where appropriate, the audit considers related switches that impact the objectives of controls placed on the target switch. The results of the audit, to a large extent, are representative of issues of the switch network architecture at large.

The objectives of the audit were to determine the following:

- That switch configuration and management practices follow documented policies and are representative of industry best practices.
- The switch is secured from threats that could be reasonably anticipated.
- The switch properly enforces isolation of network segments associated with different firewall interfaces.
- The switch prohibits peer-to-peer network traffic on the storage network.

The audit objectives were met. The findings will show that there is a significant gap between published best practices and the current configuration and management of the audited switch. Ten items were audited. Six were found to fail to be in compliance with industry best practices, three need significant improvement to the controls and practices, and one was found to be representative of both written policy and best practice.

The three most serious issues are:

- A general absence of documented policies, processes, and designs to minimize the reduction in security that can occur over time as changes accumulate.
- The storage network was found to be misconfigured and vulnerable to eavesdropping.
- Access to the switch for administration and management is accomplished with clear text credentials over the company's general network. This makes it very easy to obtain the credentials without authorization and compromise the network.

The audit recommendations will provide advice and alternatives to help reduce the risks identified in the findings. There are many references cited in this report for effective practices that can help reduce the risks. Security and management of the company's switched networks could benefit from leveraging these best practices to the extent

practical. It is recommended that the company consider adopting formal processes for the lifecycle management of the datacenter network.

4.2 Audit Findings

The following audit findings interpret and reference the evidence and findings of section 3. The following table summarizes the findings.

Item	Title	Pass/Needs Improvement/Fail
2	Physical Access to Switch	Needs Improvement
3	Change Control	Needs Improvement
7	Password Management	FAIL
9	Virtual Access - SSH	FAIL
10	IOS Version	PASS
12	Management VLAN Isolation	FAIL
14	Switchport Modes, Controlling Trunking	FAIL
15	VLAN visibility	FAIL
16	Port Security	FAIL
17	VLAN ACLs	FAIL

The basic physical security of the machine room was reviewed with respect to gaining access to the switch being audited, see item 2. The physical barriers, i.e. doors, ceilings, etc. are adequate. Biometric sensors at the doors provide entrance, but not exit records. It was observed that it was easy to piggy back into the room without logging entry at all. There was also no surveillance or escort after access was obtained. This makes the network vulnerable to disgruntled employees who make seek to gain unauthorized access to systems or data for malicious purposes. Most damage is caused intentionally or unintentionally by IT staff so appropriate controls should be put in place to balance risk and productivity. The water based fire suppression system could cause damage to equipment, in the event of a fire, possibly negating the very purpose of the system.

Maintaining currency of the IOS is a critical part protecting network equipment, the same as it is for other operating systems. Item 10 examined the version of IOS running on this switch and reviewed internet sources to determine the currency of the IOS and

whether or not there were vulnerabilities reported in the release. It was found that the IOS was one version behind and subject to several DOS attacks. This is an appropriate balance of reliability, features, and risk. Generally, it is good practice to stay current or as close to current as resources are available to properly test the IOS and introduce it into production. Item 3 references the change control and testing for new IOS versions. GIAC Enterprise seems to have a reasonable and appropriate informal process for IOS upgrades.

It is important to insure that only authorized individuals have access to switches. Because they operate at lower layers of the OSI network model they can be used to circumvent other security controls such as firewalls. This finding addresses administrative access to the switch. This includes, password management (item 7), virtual access (item 9). The most significant issue involving the items is the fact that the management VLAN is not isolated from user traffic and is routed within the company's network (item 12). A consequence of this is that any machine connected to the company's network can both attempt to access the switch and attempt to view the userid/passwords and/or SNMP community strings as they traverse the network. This is compounded by that fact that the company is using clear text protocols (telnet) to access and manage the switch. This exposes the credentials to the company's user network where it can easily be observed. The lack of individually identifiable userids makes discovery of a compromise harder and makes it impossible to track an accidental misconfiguration to its source.

VLANs are an important feature of intelligent switches. They can be used to isolate networks that span physical switches and can isolate traffic within a switch. Audit Item 14 reviewed switchport modes and VLAN trunking to ascertain how VLANs were being managed. GIAC Enterprises leverages this technology to provide flexibility in the physical installation and location of equipment, efficient allocation of switch ports, and network segment isolation. VLANs, however, also present a management and configuration challenge. The switch under review showed no restrictions (pruning) on the trunking function which enables traffic tagged with a VLAN to be transferred to another switch, maintaining the integrity of the VLAN. Several other switches were reviewed and the same evidence as shown in item 14 was found. This can result in losing track of exactly what machines are in a given VLAN. Since VLANs are performing an isolation function you could find machines that are potentially insecure on what otherwise is considered a secure network segment. This can potentially provide an attacker with a launch point to either sniff traffic or launch attacks against more critical equipment. It is therefore important to know the inventory of each VLAN and the switches that each VLAN is trunked to. Active discovery of machines on a VLAN to verify change records was conducted in item 15. This showed that the inventory was not up to date and that a misconfigured machine was active on one of the VLANs.

Item 16 addresses port security. It is consider a best practice to account explicitly for all ports on a switch. This helps insure that incidental exposures don't occur by someone

simply plugging a device or computer into a switch with the expectation that they will get some level of functionality. It has been our experience that individuals may plug notebooks into an open port, for example, to check email or sniff traffic for purposes of debugging a system. This may be appropriate if it occurs with proper authorization and there is a reasonable certainty that the computer being used does not contain a virus. The use should be known in advance and approved so that the risk of network disruption is reduced. There are formal processes for installing and removing servers in GIAC Enterprises datacenter. This is a sound practice. It would be beneficial to GIAC to include network switchport activation in that process.

The application of VLAN ACLs was tested in Item 17. The purpose of VLAN ACLs on the switch is to insure that servers with interfaces on the storage network VLAN can only send traffic to the central file server and that those data streams cannot be observed. If all ports on the VLAN are properly configured this can be achieved. However, it was found that ports on upstream switches were configured on the storage VLAN without the correct VLAN ACLs. This enables those machines to successfully eavesdrop data streams from other servers. This undermines the security zones enforced by the firewall.

4.3 Audit Recommendations

The network switching infrastructure is a component of the datacenter architecture that has security implications and functions. As with a server, firewall, VPN, or router, the switch infrastructure should be managed and maintained throughout its lifecycle to insure that the security requirements are not unknowingly compromised over time.

To help mitigate the risks identified in the audit and maintain the switch environment over time, we make the following recommendations regarding the target switch and the switch infrastructure as a whole:

- Documented policies for the installation, configuration, design, and maintenance of the switch infrastructure should be implemented. This will require significant effort. Based on the size of the organization this may require up to 120 hours of effort. This assumes 2-3 engineers and a manager working part-time over a period of a month. This will give sufficient time to vet interim versions of policies to the engineering and management staff and incorporate revisions.
- Review and revise the physical access controls and policies for the machine room. Physical access to the machine room should be carefully controlled. This may be mitigated with some simple procedural changes, such as locking racks and logging the issuance of keys, or it may require significant cost, such as installing additional biometrics to track exit times as well as entrance times.
- Consider converting to a non-water based fire suppression system such as FM-200. This would potentially cost more than a hundred thousand dollars to do and needs to be carefully weighed against the value of the assets in the machine

room. In considering this, evaluate the damage that might occur to equipment if a non-catastrophic fire occurred that triggered the release of water.

- Administrative and management access should be done via secure protocols where possible. Upgrade the IOS to a cryptographic version capable of running SSHv2. Use SNMPv3 for management. Separate management and administration from user traffic. If the cost of upgrade is prohibitive or the adoption of SNMPv3 is not feasible, then isolation of the management traffic will mitigate much of the risk associated with the protocols.
- Individually identifiable userids should be used. It is more manageable to do this centrally, but that requires implementation of a central authentication service. Alternatively, the accounts can be created locally on the switches themselves. This, of course, creates a management overhead with respect to changing passwords and creation and deletion of accounts as employees change over time. The cost of a central authentication services is closely linked to the company's account generation process and existing infrastructure. For example if you currently have an Active Directory service populated with all your accounts you can leverage that at very little cost. Perhaps 4-8 hours of effort. If you have to setup a separate service for network administrators it may require a few thousand in hardware and software, plus 16 hours of effort. If you have the resources, a central authentication mechanism will pay dividends in reducing the account management burden.
- A security minded base configuration template that utilizes applicable best practices should be used to initialize switches prior to installation. The configuration should be a default deny, i.e. ports are shutdown by default and activated as required. This should be able to be accomplished in 24-32 hours of effort by a network engineer.
- Switchport activation should be integrated into the server installation and activation process. This should require less than 4 hours effort to incorporate the change into the existing process and add 30 minutes to an hour for each server install. This would include maintaining an inventory database of server, switch, switchport, VLAN, MAC Address, and responsible administrator data fields. Periodic auditing of machines on each VLAN should be conducted to insure the database remains accurate.
- Develop a policy and methodology for managing VLAN and VLAN ACLs. It is critical that careful attention is given to what devices are switching traffic on what VLAN. This should be controlled by a strict change control process as errors in layer 2 isolation can circumvent all upper layer controls, such as firewalls. This will add some overhead to the process of assigning jacks. In addition, a periodic review of VLANs and VLAN ACLs should be conducted to insure compliance with policy and objectives. This could be expected to require 32 hours of effort by an engineer or IT auditor annually. Alternatively, you may want to consider if the risks of misconfiguration, cost of maintenance, and flexibility of VLANs are in appropriate balance for your organization. Configuration and maintenance can be reduced by having a physical mapping of the switch infrastructure to your

company's security and network isolation requirements. Of course this comes with the negative of physical constraints being placed on the location of equipment. Perhaps a hybrid of the two would strike an appropriate balance. Physical separation for sensitive data and VLAN convenience for everything else.

- Use a version control system for base configuration templates and specific device configurations. This way a history of changes can be maintained. Many such systems will indicate who made the change which is useful in trouble shooting.
- In conversation with engineering staff during the course of the audit it is apparent that they are fully aware of many of the best practices and recommendations presented in this audit. There appears to be no specific focus on the machine room infrastructure. Network engineers are charged with maintaining and managing the enterprise network at large and may be spread too thin in this regard. Management may want to consider evaluating whether or not it is prudent to increase staff in network engineering or align some staff with specific responsibilities, like management of the key assets in the datacenter. Certainly increasing staff is expensive and needs careful review. Management may want to consider the idea of assigning responsibility of datacenter networking to a specific individual and then supplement that individual with other permanent or temporary staff, as required.

There always needs to be a balance between the cost of protecting an asset and the value of that asset. These recommendations consider the fact that the switch infrastructure is part of a structured environment that houses high value information assets and equipment. Therefore, some of the recommendations might not be appropriate in an environment with less valuable assets. Please consider the value of the assets managed in your company's machine room as you consider the recommendations and make implementation decisions.

5. References

- [1] Cisco, Catalyst 3550 Series Intelligent Ethernet Switches, 07/2003, URL: http://www.cisco.com/en/US/products/hw/switches/ps646/products_data_sheet09186a00800913d7.html
- [2] Boney, J., CISCO IOS in a Nutshell, O'Reilly and Associates, 2002.
- [3] Greene, T., Let's get physical, Network World, 01/12/04, URL: http://216.239.51.104/search?q=cache:g_d-TonC1XIJ:www.nwfusion.com/careers/2004/0112man.html+switch+physical+security&hl=en&ie=UTF-8
- [4] Harris, S., CISSP Certification Exam Guide, McGraw-Hill, 2002.
- [5] Network Infrastructure Security Checklist, Version 5, Release 2, 30 October 2003, Defense Information Systems Agency.
- [6] Roberts, P., Cisco warns of hacking toolkit, IDG News Service, 03/29/04.
- [7] Cisco Systems, Data Sheet, "Protect the Network Infrastructure with Cisco IOS Security", URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_data_sheet09186a00801f98de.html
- [8] Cisco Systems, "Securing the LAN with Catalyst 3550 and 2950 Series Switches", URL: http://www.cisco.com/application/vnd.ms-powerpoint/en/us/guest/products/ps628/c1161/ccmigration_09186a00801168c1.ppt
- [9] Lusignan, R., "Managing Cisco Network Security", Syngress, 2000.
- [10] Cisco Systems, "Cisco Advisory: Cisco IOS Interface Blocked by IPv4 Packets", URL: <http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>
- [11] Stanford University, "Protocol Information on Cisco IOS Denial of Service -- 17 Jul 2003", URL: <http://securecomputing.stanford.edu/alerts/cisco-update-17jul2003.html>
- [12] Department of Health and Human Services, 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule, 2/2003.
- [13] Akin, T., "Hardening Cisco Routers", O'Reilly and Associates, 2002.

[14] KBeta Security Web, "Improving Security on Cisco Routers", URL:
<http://www.kbeta.com/SecurityTips/Checklists/ImprovingCiscoSecurity.htm>

[15] Cisco, "Virtual LAN Security Best Practices", 02/03/2003, URL:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

[16] Cisco, "SAFE Layer 2 Security In-depth Version 2", ©2000-2004, URL:
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfblu_wp.pdf

[17] @Stake, "Secure Use of VLANs: An @stake Security Assessment", 08/2002, URL:
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf

[18] Ettercap, URL: <http://ettercap.sourceforge.net/>

[19] Center for Internet Security, "CIS Level-1 / Level-2 Benchmark and Audit Tool for Cisco IOS Routers", URL: http://www.cisecurity.com/bench_cisco.html

[20] Google Search Engine, URL: www.google.com

[21] SecurityFocus.com, "Vulnerabilities by vendor", URL:
<http://www.securityfocus.com/bid/vendor/>

[22] The MITRE Corporation, "Common Vulnerabilities and Exposures", URL:
<http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Checkpoint>

[23] Zeng, B., "Cisco Configuration Security Auditing Tool", URL:
<http://hotunix.com/tools>

[24] ISO/IEC 17799, Information technology — Code of practice for information security management, 12/01/2000.

[25] Wilson, S., "Combating the Lazy User: An Examination of Various Password Policies and Guidelines", SANS GSEC Practical, 9/16/2002. URL:
<http://www.sans.org/rr/papers/6/142.pdf>

6. Appendix A – CIS RAT Example Audit Report

Router Audit Tool report for

all

Audit Date: Wed Apr 21 00:48:54 2004 GMT

Sort Order: importance,passfail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
10	pass	IOS - require line passwords	3550.txt		
10	pass	IOS - no ip http server	3550.txt		
10	pass	IOS - forbid SNMP community public	3550.txt		
10	pass	IOS - forbid SNMP community private	3550.txt		
10	pass	IOS - enable secret	3550.txt		
10	pass	IOS - Create local users	3550.txt		
10	FAIL	IOS - no snmp-server	3550.txt	n/a	319
10	FAIL	IOS - login default	3550.txt	vtty 5 15	330
10	FAIL	IOS - login default	3550.txt	vtty 0 4	325
10	FAIL	IOS - apply VTY ACL	3550.txt	vtty 5 15	328
10	FAIL	IOS - apply VTY ACL	3550.txt	vtty 0 4	323
10	FAIL	IOS - Use local authentication	3550.txt	n/a	2
10	FAIL	IOS - Define VTY ACL	3550.txt	n/a	2
7	pass	IOS 12 - no udp-small-servers	3550.txt		
7	pass	IOS 12 - no tcp-small-servers	3550.txt		
7	pass	IOS 12 - no directed broadcast	3550.txt		
7	pass	IOS - no service config	3550.txt		

7	pass	IOS - no ip source-route	3550.txt		
7	pass	IOS - no cdp run	3550.txt		
7	pass	IOS - exec-timeout	3550.txt		
7	pass	IOS - encrypt passwords	3550.txt		
5	pass	IOS 12.1,2,3 - no finger service	3550.txt		
5	pass	IOS - tcp keepalive service	3550.txt		
5	pass	IOS - forbid clock summer-time - GMT	3550.txt		
5	pass	IOS - enable logging	3550.txt		
5	FAIL	IOS - user password quality	3550.txt	rwinding	16
5	FAIL	IOS - set syslog server	3550.txt	n/a	2
5	FAIL	IOS - service timestamps logging	3550.txt	n/a	2
5	FAIL	IOS - service timestamps debug	3550.txt	n/a	2
5	FAIL	IOS - ntp server 3	3550.txt	n/a	2
5	FAIL	IOS - ntp server 2	3550.txt	n/a	2
5	FAIL	IOS - ntp server	3550.txt	n/a	2
5	FAIL	IOS - no ip bootp server	3550.txt	n/a	2
5	FAIL	IOS - logging buffered	3550.txt	n/a	2
5	FAIL	IOS - line password quality	3550.txt	vty 5 15	330
5	FAIL	IOS - line password quality	3550.txt	vty 0 4	325
5	FAIL	IOS - line password quality	3550.txt	con 0	322
5	FAIL	IOS - VTY transport telnet	3550.txt	vty 5 15	328
5	FAIL	IOS - VTY transport telnet	3550.txt	vty 0 4	323
3	pass	IOS - logging trap info or higher	3550.txt		
3	pass	IOS - logging console critical	3550.txt		
3	pass	IOS - disable aux	3550.txt		
3	FAIL	IOS - clock timezone - GMT	3550.txt	n/a	2

Summary for all

#Checks	#Passed	#Failed	%Passed
43	21	22	48

Perfect Weighted Score	Actual Weighted Score	%Weighted Score
288	145	50

Overall Score (0-10)

5

Note: PerfectWeightedScore is the sum of the importance value of all rules.

ActualWeightedScore is the sum of the importance value of all rules passed, minus the sum of the importance each instance of a rule failed.

7. Appendix B – CCSAT Example Audit Report

Cisco Device Configuration Security Audit: CCSAT Report

Copyright (C) 2003 Bill Zeng

(Script start time: Wed Apr 21 15:11:06 EST 2004)

The latest IOS version was entered as 12.1

Total number of audited devices = 1

Total number of interfaces = 53

Total number of shutdown interfaces = 17

Total number of open interfaces = 36

Total number of lines (con/vty/aux) = 3

Total number of console lines = 1

Total number of terminal lines = 2

Total number of auxiliary lines = 0

Total number of access lists = 3

Total number of snmp ro/rw rules = 0 (ro=0 + rw=0)

I. General Configuration

IOS version (latest 12.1) not up-to-date on:

0 of 1 devices

(12.0 or later supports all 3 snmp versions: SNMPv1, SNMPv2c and SNMPv3.)

banner not configured on...

1 of 1 devices

II. Passwords and Authentication

'service password-encryption' not configured on...

0 of 1 devices

'enable secret' not configured on...

0 of 1 devices

'enable password' (weak) still configured on...

0 of 1 devices

passwords not configured on the following router lines:

0 of 3 lines

3550.txt:line con 0

3550.txt:line vty 0 4

3550.txt:line vty 5 15

SNMP community default strings still configured on...

0 (ro) and 0 (rw) of 1 devices

'AAA new-model' not configured on...

1 of 1 devices

AAA authentication (TACACS+/Radius/Kerberos) not configured on...

1 of 1 devices (tacacs+)

or

1 of 1 devices (radius)

or

1 of 1 devices (kerberos)

user privilege not configured on...

1 of 1 devices

III. Network Services

'no service tcp-small-servers' not configured on...

1 of 1 devices

'no service udp-small-servers' not configured on...

1 of 1 devices

'no ip bootp server' not configured on...

1 of 1 devices

'no ip finger' not configured on...

1 of 1 devices

'no ip http server' not configured on...

0 of 1 devices

'no cdp run' not configured on...

0 of 1 devices

'no service config' not configured on...

1 of 1 devices

'ip ssh' not configured on...

-1 of 1 devices

IV. IP Routing and Security

'no ip source-route' not configured on...

0 of 1 devices

'ip cef' not configured on...

1 of 1 devices

'no ip directed-broadcast' not configured on the following router interfaces:

36 of 36 interfaces

3550.txt:interface FastEthernet0/1

3550.txt:interface FastEthernet0/2

3550.txt:interface FastEthernet0/3

3550.txt:interface FastEthernet0/4

3550.txt:interface FastEthernet0/5

3550.txt:interface FastEthernet0/6

3550.txt:interface FastEthernet0/7

3550.txt:interface FastEthernet0/8

3550.txt:interface FastEthernet0/9

3550.txt:interface FastEthernet0/33

3550.txt:interface FastEthernet0/34

3550.txt:interface FastEthernet0/35

3550.txt:interface FastEthernet0/36

3550.txt:interface FastEthernet0/37

3550.txt:interface FastEthernet0/38

3550.txt:interface FastEthernet0/39

3550.txt:interface FastEthernet0/46

'no ip mask-reply' not configured on the following router interfaces:

36 of 36 interfaces

3550.txt:interface FastEthernet0/1

3550.txt:interface FastEthernet0/2

3550.txt:interface FastEthernet0/3

3550.txt:interface FastEthernet0/4

3550.txt:interface FastEthernet0/5

3550.txt:interface FastEthernet0/6

3550.txt:interface FastEthernet0/7

3550.txt:interface FastEthernet0/8

3550.txt:interface FastEthernet0/9

3550.txt:interface FastEthernet0/33

3550.txt:interface FastEthernet0/34
3550.txt:interface FastEthernet0/35
3550.txt:interface FastEthernet0/36
3550.txt:interface FastEthernet0/37
3550.txt:interface FastEthernet0/38
3550.txt:interface FastEthernet0/39
3550.txt:interface FastEthernet0/46

'no ip proxy-arp' not configured on the following router interfaces:

36 of 36 interfaces

3550.txt:interface FastEthernet0/1
3550.txt:interface FastEthernet0/2
3550.txt:interface FastEthernet0/3
3550.txt:interface FastEthernet0/4
3550.txt:interface FastEthernet0/5
3550.txt:interface FastEthernet0/6
3550.txt:interface FastEthernet0/7
3550.txt:interface FastEthernet0/8
3550.txt:interface FastEthernet0/9
3550.txt:interface FastEthernet0/33
3550.txt:interface FastEthernet0/34
3550.txt:interface FastEthernet0/35
3550.txt:interface FastEthernet0/36
3550.txt:interface FastEthernet0/37
3550.txt:interface FastEthernet0/38
3550.txt:interface FastEthernet0/39
3550.txt:interface FastEthernet0/46

RIP configured on... (informational)

0 of 1 devices

RIP MD5 authentication not configured on...

0 of 0 devices

OSPF configured on... (informational)

0 of 1 devices

OSPF MD5 authentication not configured on...

0 of 0 devices

EIGRP configured on... (informational)

0 of 1 devices

EIGRP MD5 authentication not configured on...

0 of 0 devices

BGP configured on... (informational)

0 of 1 devices

BGP neighbor passwords not configured on...

0 of 0 devices

Only the following remote ASs are password-authenticated:

V. Access Control and ACLs

exec-timeout not configured on the following router lines:

3 of 3 lines

'transport input telnet' not configured on the following router vty lines:

2 of 2 vty lines

'transport input ssh' not configured on the following router vty lines:

0 of 2 vty lines

3550.txt:line vty 0 4

3550.txt:line vty 5 15

'access-class <ACL> in' not configured on the following router vty lines:

0 of 2 vty lines

3550.txt:line vty 0 4

3550.txt:line vty 5 15

'access-group <ACL> in/out' not configured on the following router interfaces:

35 of 36 interfaces (in & out on same I/F counted twice)

3550.txt:interface FastEthernet0/19

3550.txt:interface FastEthernet0/1

3550.txt:interface FastEthernet0/2

3550.txt:interface FastEthernet0/3

3550.txt:interface FastEthernet0/4

3550.txt:interface FastEthernet0/5

3550.txt:interface FastEthernet0/6

3550.txt:interface FastEthernet0/7

3550.txt:interface FastEthernet0/8

3550.txt:interface FastEthernet0/9
3550.txt:interface FastEthernet0/33
3550.txt:interface FastEthernet0/34
3550.txt:interface FastEthernet0/35
3550.txt:interface FastEthernet0/36
3550.txt:interface FastEthernet0/37
3550.txt:interface FastEthernet0/38
3550.txt:interface FastEthernet0/39
3550.txt:interface FastEthernet0/46

SNMP community (readonly/readwrite) not access-controlled on...
0 of 0 RO/RW rules

VI. Logging

'service timestamps log...' not configured on...
1 of 1 devices

'logging <server_IP>' not configured on...
0 of 1 devices

SNMP-server host not configured on...
1 of 1 devices

NTP server not configured on...
0 of 1 devices

(Script finish time: Wed Apr 21 15:11:09 EST 2004)