Global Information Assurance Certification Paper

CASE STUDY: SECURING CISCO'S IP CALL MANAGER

GIAK PRACTICAL ASSIGNMENT V1.1 (MAY 2002)

Issue: 1.1
Date: 25-Jan-2003
Author: Craig J. LaCava

GIAK Assignment 1 v1.1

TABLE OF CONTENTS

1 PURPOSE AND SCOPE I

1.1 Abstract i

1.2 Scope i

1.3 Acronyms i

2 BEFORE: THE INITIAL VOICE OVER IP ENVIRONMENT & NETWORK ARCHETECTURE II

2.1 Voice Over IP Call Management ii

2.2 Cisco Call Manager Architecture ii

2.3 Cisco Call Manager Vulnerabilities iii

2.3.1 Patching the CCM Units in a Timely Manner iii

2.3.2 CCM Vulnerability Scan iv

2.3.2.1 Purpose and Scope iv

2.3.2.2 Scanning Results and Analysis v

2.4 Cisco Call Manager Risk Assessment vi

2.4.1 Denial or Loss of Voice Services vi

2.4.2 Theft of Voice Services vi

3 DURING: EXPLORING AND ADDRESSING THE CISCO CALL MANAGER SECURITY ISSUES VIII

3.1 Risk Mitigation through Isolation viii

3.2 Voice over IP VLAN Design viii

3.3 Network Intrusion Detection x

3.4 Dedicated Management VLAN and Console xi

4 AFTER: IMPLEMENTATION OF THE RECOMMENDATIONS AND THEIR IMPACT XIII

4.1 Recommendations Taken Forward xiii

4.2 Post-Implementation Notes xiv

4.3 Lessons Learnt xiv

4.3.1 Network Routing Table Audit xiv

APPENDIX A REFERENCES 30

1 PURPOSE AND SCOPE

1.1 Abstract

This case study documents the steps that were taken to in order to mitigate the risks and address several vulnerabilities associated with an implementation of the Cisco Call Manager (CCM) within a new Voice over IP environment. The original Voice over IP network architecture, a high-level vulnerability and risk assessment of the CCM and the planning and design of an improved Voice over IP network architecture are all addressed within this document.

1.2 Scope

The CCM is a server based on Microsoft Windows 2000 and the MS SQL Server 2000. All of the vulnerabilities, risks and many of the same threats that apply to most any Microsoft Windows 2000 server also apply to the CCM.

Because there are many resources already available concerning securing a Windows 2000 server, this case study is more concerned about the uniqueness of the CCM as a service platform and the security associated with the network infrastructure that surrounds the CCM in a typical Voice over IP environment.

1.3 Acronyms

CCM	- Cisco Call Manager
DHCP	- Dynamic Host Configuration Protocol
DNS	- Domain Name Services
FTP	- File Transfer Protocol
HTTP	- Hyper Text Transfer Protocol
IDS	- Intrusion Detection System
IIS	- Microsoft's Internet Information Server
IP	- Internet Protocol
LAN	- Local Area Network
NNTP	- Network News Transfer Protocol
PBX	- Public Branch Exchange
PSTN	- Public Switched Telephone Network
RSVP	- Resource Reservation Protocol
RTP	- Real Time Protocol
SAFE	- Cisco's Security Blueprint for Enterprise Networks
SARA	- Security Auditors Research Assistant
SDP	- Session Description Protocol
SIP	- Session Initiation Protocol
TFTP	- Trivial File Transfer Protocol
UDP	- User Datagram Protocol
VLAN	- Virtual Local Area Network
WAN	- Wide Area Network

2 BEFORE: THE INITIAL VOICE OVER IP ENVIRONMENT & NETWORK ARCHETECTURE

2.1 Voice Over IP Call Management

A medium sized enterprise business has recently removed the majority of their legacy PBX systems and replaced them with a Cisco Voice over IP solution. All of the office employees at each of five locations now use IP phones and the majority of the interoffice voice traffic now traverses the corporate IP WAN. The functionality of the legacy PBX system is now split across two Cisco Call Manager (CCM) platforms and a Cisco Voice Gateway. The CCM platforms are both based on Windows 2000 and MS SQL Server 2000 while the voice gateway is actually a Cisco 3600 series router.

As with many companies that make the lead to VoIP, a reduction in operating costs was the primary goal of the implementation. Expensive, dedicated voice trunks have been decommissioned, equipment support and maintenance costs have been reduced, corporate phone bills have fallen and employee productivity has increased.

While the company has enjoyed a moderate return on investment with their new Voice over IP solution, a number of new security risks and vulnerabilities have been created since Voice over IP has been implemented. The most prominent risks within the new system are the call manager platforms.

2.2 Cisco Call Manager Architecture

The CCM is at the core of any Cisco VoIP solution. All of the IP phones within an office register and get their configurations from the CCM via TFTP. The CCM acts as the Voice over IP gatekeeper and redirects voice calls that originate locally to remote Voice over IP gateways, CCMs or other IP phones.

Each office location within the company has two CCM platforms: a Primary CCM and a Publisher CCM. Each IP phone within the office is configured to register first with the Primary CCM and then with the Publisher CCM if the primary is not available. The CCM that the IP phone registers with becomes the VoIP Gatekeeper for that user and all Voice over IP service requests are handled by this CCM.

The Publisher CCM is where the primary IP phone and user database is held as well as the IP Phone configuration TFTP server. When an IP phone is booted, it will first request an IP address from the DHCP server. Once the DHCP request is answered, the phone will attempt to contact the TFTP server in order to download its configuration file. The database hosted on the Publisher CCM is replicated to and synchronized with the Primary CCM.

The dual CCM architecture provides full redundancy for each office. If one of the CCM units fails, the one that remains is equipped to provide all the functionality provided by the dual CCM configuration. The IP Phones will detect when one of the CCMs has failed and will register with the remaining CCM.

Figure 1: Existing Logical Network and VoIP Architecture

The company has all of the VoIP elements and user workstations on a single switched Ethernet LAN as shown above in Figure 1. The Ethernet switches that support the LAN have plenty of capacity and processing power to handle all of the data and voice traffic produced by the office.

2.3 Cisco Call Manager Vulnerabilities

While there are vulnerabilities associated with the Cisco IP phones, the Cisco Voice Gateways and Voice Enabled Routers, the scope of this case study is only the CCM units.

2.3.1 Patching the CCM Units in a Timely Manner

Unlike a typical legacy PBX, the CCM is based on Microsoft Windows 2000 as well as MS SQL Server 2000 and is always connected to the company's IP network. Because the CCM is based on a Microsoft platform, the CCM is considered more of a target for attackers than a typical legacy PBX.

Most all of the MS Windows 2000 and MS SQL Server vulnerabilities that are discovered will affect the CCMs. However, patching the Windows platform that supports the CCM software is not as simple as keeping a typical Microsoft server up-to-date and secure with the latest software updates.

Cisco warns all registered CCM administrators that patches released by Microsoft should not be applied to their CCM servers until Cisco has verified and certified that the patches do not impact the functionality of the CCM software. Cisco often issues their own version of the Microsoft patch, sometimes with a small patch for the CCM software included.

Patching the CCM becomes a security issue because Cisco's versions of the Microsoft patches are usually not available for two to five days after the vulnerability is publicly announced. If an administrator patches the CCM with an unofficial software patch (i.e. any operating system or SQL server patch not certified by Cisco), then any SLA or warranty offered by Cisco for the CCM is null and void. The Cisco TAC will usually insist that the CCM be installed on a pure platform (i.e. a platform using only a certified operating system and patches) before in-depth technical support is available.

For example, Microsoft's Security Bulletin #MS02-018 (Cumulative Patch for Internet Information Services) was posted on April 10th, 2002, in response to a critical vulnerability within Microsoft's IIS. This particular vulnerability would allow an attacker to run any program or application on a comprised server. Cisco's certified version of this patch was not available until April 15th – five days later.

CCM administrators have to make a choice during this time. They could either void the Cisco SLA and warranty by installing the non-Cisco certified OS patch from Microsoft or wait five days before patching their CCM systems after this very critical and well publicized vulnerability was announced.

Many CCM administrators choose to wait until the official Cisco patch is released. Support and stability of the CCM usually wins out over the risk associated with the vulnerability window.

2.3.2 CCM Vulnerability Scan

2.3.2.1 Purpose and Scope

In order to add additional credibility and evidence to the vulnerabilities believed to be associated with the company's Voice over IP environment, a vulnerability scan was run one of the CCM units. The results of the scan were assessed and are included within this case study.

The two CCM units within each branch office are identical in hardware and software specifications. The only difference between the Primary and Publisher CCM is their configurations. It was decided that a test CCM would be built from one of the mirrored hard drives from a production CCM unit. The vulnerability scan would be conducted on the test CCM and not on the production units.

A number of vulnerability scanners were used to assessment the CCM:

- GFI LANguard Network Security Scanner v3.0
- Security Auditors Research Assistant (SARA) v4.1.3b
- nmap V2.54 Beta31

The test CCM was given a private IP address and connected to an isolated Ethernet LAN segment along with the vulnerability scanner and a single Cisco IP phone. The CCM is running Cisco's Call Manager Software version 3.1a. No other hardening has taken place on the CCM units at this time.

2.3.2.2 Scanning Results and Analysis

The vulnerability scanning tool found the following TCP ports open:

Table 1 – CCM Vulnerability Scan Results

TCP Port	Used For	Comments
80	HTTP	Used for CCM management console
23	Telnet	Not required and should be disabled
53	DNS	Not required and should be disabled
110	POP3	Not required and should be disabled
135	epmap DCE	Required for remote procedure calls between CCMs
139	SMB over Netbios	Not required and should be disabled
443	HTTPs	Used for secure CCM management console
445	SMB over TCP	Not required and should be disabled
1080	Socks	Used is conjunction with the HTTPs server
1433	MS SQL	Required for CCM database replication
2000	Cisco VoIP	Required for communications to IP phones
2001	Cisco VoIP	Required for communications to other CCM/Gatewa ys
3389	Term Services	Not required and should be disabled
8080	HTTP Proxy	Not required and should be disabled

Many unnecessary Windows 2000 services are enabled by default, even though the CCM units were built directly from Cisco's CCM CD distribution, which installs Windows 2000, MS SQL Server and the CCM software onto a new, clean server platform.

SARA was able to name several known vulnerabilities within the base CCM service platform. One Critical Vulnerability and three Targets for Abuse were identified.

Table 2 – SARA Scan Results for the CCM

Class	Vulnerability	Comments
Critical	telnetd buffer overflow	Disabling the telnet service is possible with the CCM
Warning	IIS buffer overflow	Multiple IIS vulnerabilities exist
Warning	MS SQL SA Abuse	Ensure the SQL SA account has a strong password
Warning	SMB Null Session	SMB null sessions can be exploited for info leeks

Services such as POP3, Telnet, DNS, HTTP Proxy and MS Terminal Services should be disabled because they are not required for normal CCM operations. Furthermore, SMB communication is not required for the CCM, so services such as the Alerter, Computer Browser, Messenger and Net Logon can all be disabled and the port (139 and 445) can be blocked. By taking these steps, both the telnetd and SMB vulnerabilities cited in Table 2 can be eliminated.

However, there are lingering vulnerabilities within IIS and MS SQL Server that can not be patched and these services are required for normal CCM operations. According to SARA, "MS SQL Server 2000 has been reported to contain multiple vulnerabilities. These include heap and stack based buffer overflows and network denial of service attacks. As of 27 May 2002, there are no patches from Microsoft available."

The LANguard scan also revealed that the default read-only community string ('publlic') was in use as a part of the default CCM installation. Using the default string, an attacker would be free to browse the CCM's entire management MIB and possibly use this information to formulate a successful attack on the CCM. Because no SNMP management is being conducted with the CCM units at this time, the SNMP service should be disabled or, at the very least, the community strings should be changed.

While a number of the vulnerabilities discovered during this assessment can be mitigated, there will still be a risk to the CCM units through various security holes within IIS and MS SQL Server.

2.4 Cisco Call Manager Risk Assessment

Threats to the CCMs can originate from the internal company network, externally from the Internet or from malicious code. While there is no direct Internet access at any of the company's branch locations, Internet access is provided via the company's headquarters over the WAN. There are already a number of controls in place around the company's Internet access.

There are two major risks and potential consequences associated with an attack on the CCM in a Cisco Voice over IP network.

2.4.1 Denial or Loss of Voice Services

With a typical Cisco Voice over IP configuration, if both of the CCM platforms were put out of service, all Voice over IP calls would be blocked and there would be a total loss of voice service within the affected office. Even calls between IP phones on the same LAN would become impossible.

Voice over IP calls that were already established before the attack would be permitted to continue even after the CCMs were made unavailable. The CCM is only involved with the setup of a Voice over IP call. Once a call has been established, only the endpoints participate in the transmission of IP packets.

2.4.2 Theft of Voice Services

If the CCM is compromised either by an internal or external attacker, it is possible for third parties to place unauthorized voice calls. Internal attackers can change an IP Phone's voice network access restrictions. For example, a phone located in a common area (such as the lobby or break room) is usually restricted to making only internal calls to other company phone extensions. If these restrictions were lifted, anyone could use the phone to call anywhere in the world, including premium services. The company would be responsible for the charges for all of the external calls.

A more popular attack concerning theft of voice services is the redirection of calls to unauthorized external phone numbers. If an attacker had access to the CCM's configuration, he or she could redirect an unused internal company phone number to any external phone number. While most companies set rules to forbid such practice, an attacker could configure the CCM to redirect a local number to a third party within another country. The attacker now only needs to make a local call into the company's voice

network, the call comes into the Voice Gateway and the CCM is asked where it should be routed to. The CCM tells the Gateway to redirect the call to the third party. While the attacker now only has to make a local call, the company is charged for the long distance call to the third party.

External attackers can also take advantage of completely free phone service, but only if they have a high-quality IP network connection between themselves and the company's Voice Gateway. If the attacker has in-depth knowledge of the CCM, he or she could make their calls appear as if they were originating from within the company from an authorized IP Phone. Unless there is a thorough audit of the Voice over IP call logs and/or external phone bills, such theft may not be easily noticed or recognized.

3 DURING: EXPLORING AND ADDRESSING THE CISCO CALL MANAGER SECURITY ISSUES

Once the vulnerabilities and risk assessment for the CCM units was socialized within the company, resources were dedicated to researching possible ways to improve the Voice over IP network and security architecture so that the CCM units would be better protected from attack. Any solution would have to either improve or maintain the current Voice over IP service and quality levels.

3.1 Risk Mitigation through Isolation

The Cisco Security Blueprint for Enterprise Networks (SAFE) makes several recommendations for securing a Voice over IP network. At the core of these recommendations is a paradigm that dictates that the Voice over IP traffic and CCM should be isolated from the rest of the IP data network in the local area. By partitioning off the IP data traffic, one can enhance the quality of service, performance and security of a Voice over IP implementation.

By strictly isolating the CCM units from all other networked IP hosts except for the Cisco IP phones, the risk and the probability of a successful attack on the CCMs are greatly reduced. There will be no access to the CCM from any of the user desktop workstations or from the company server farms. If an attack is perpetrated from the Internet onto the company LAN, the CCMs will be out of reach.

3.2 Voice over IP VLAN Design

Cisco recommends that a VLAN be created and utilized exclusively for Voice over IP traffic. Using all of the existing IP phones and Ethernet LAN switches, two logically separate VLANs can be created that will segregate all of the Voice over IP traffic from the rest of the IP data traffic in each branch office.

It is important to note that VLANs themselves are not inherently secure per se, but they can be used to create a more secure environment for the CCM units in conjunction with additional controls, processes and policies.

Cisco IP phones can act as a small Ethernet switch and can create a trunk between the user's workspace and the office's Ethernet LAN switch. There is only a need for a single physical connection from one of the office LAN switches to the Cisco IP Phone.

Currently, the IP phones are being used as Ethernet switches, but no VLAN tagging is taking place (i.e. all of the data and voice IP traffic is flowing across one VLAN as shown in Figure 1). Below Figure 2 shows the physical connectivity between the User's PC, their IP phone and the office's core Ethernet LAN switch.

Figure 2: Physical Connectivity to each User Workspace

By keeping this same physical configuration but enabling VLAN tagging on each IP phone and the office's core Ethernet switch, two separate VLANs can be created. The IP phones will tag each packet from the user's PC so that it is switched onto the Data VLAN while each packet from the IP phone itself will be tagged so that it is switched onto the Voice over IP VLAN. Even though both VLANs are being switched over the same physical hardware, the traffic on each VLAN will always be kept logically separate. Figure 3 shows the logical view of this configuration.

Figure 3: Logical Connectivity to each User Workspace

The top diagram in Figure 3 depicts the two VLAN trunks connecting to the IP Phone while only the IP data traffic from the IP Data VLAN is sent to the user's PC. The bottom diagram shows that the one Ethernet switch will actually provide two separate Ethernet VLANs.

Because the CCM units will not be connected to the office's IP data VLAN, the office users will not be able to connect to the CCMs via their workstation PCs. The CCM web interface will only be accessible via a dedicated CCM management PC (only physically and logically accessible locally by the network managers). The HTTP services for each CCM will be disabled on the interface that is connected to the Voice over IP LAN. Figure 4 shows a network diagram depicting the new Voice over IP architecture.

Figure 4: Improved Logical Network and Voice over IP Architecture

To further protect the CCM units, the configuration of the office LAN switch can be locked down so that each user's Ethernet port will not become active if the user plugs anything other than their allocated IP Phone into the office's core Ethernet switch port. This will prevent anyone from plugging any other IP device, PC or laptop directly into the office Ethernet switches.

Additionally, the CCM units are now inaccessible from any external network. The company's Internet traffic is now completely separated from the Voice over IP VLAN and the CCM units.

The HTTP management of the CCM units along with the SQL database replication will take place over a private, isolated LAN and not the Voice over IP VLAN. This LAN segment will only be accessible by the CCM units and the CCM management console as shown in Figure 4.

3.3 Network Intrusion Detection

Because the new network design has created a VLAN that will be used only for Voice over IP communications, it is possible to add another layer of security around the CCM through the use of a Network Intrusion Detection System (Network IDS).

The Voice VLAN should only carry IP traffic associated with Cisco's implementation of Voice over IP. Table 1 defines the traffic that can be expected on the Voice VLAN. This traffic is relatively easy to profile and the rules for the Network IDS will also be simple and straight forward.

For example, if the Network IDS ever saw any HTTP, FTP, NNTP, DNS, any Net Bios-based traffic or any other protocol or application that is not normally used between the Cisco IP phones and the CCM, the IDS would send an alarm to the network and security managers. Any attempt to connect to the CCM via HTTP from the Voice VLAN would be instantly detected.

OSI Network Layer	Protocols
Application Layer	TFTP
Presentation Layer	G.729, G.711*
Session Layer	H.323, SIP, SSCP, SDP
Transport Layer	UDP, RTP, RSVP
Network Layer	IP

Table 1: Traffic Expected on the Voice over IP VLAN

*In this instance, G.711 (64K per call) is used for Voice over IP between two IP phones on the same LAN. G.729 (8K per call) is used when a call must traverse the company's WAN infrastructure to either get to a remote IP phone or a remote Voice over IP gateway.

Another way to improve the IDS rules even further would be to differentiate the IP addressing ranges of all the company's IP phones. For example, the company currently uses a registered class B IP address range for all of its IP enabled devices including the IP phones. If all of the IP phones and CCM units were instead assigned addresses from a private IP address range (such as 10.0.0.0 /8), then one would always expect to only see source and destination IP addresses that fall within this private range of addresses. Because the 10.0.0.0 /8 IP network is not routed over the Internet nor is it used anywhere else within the company, the IDS could be set to raise an alarm if any other IP address were seen on the company's Voice over IP VLAN segments. Because there is no need for the IP phone to ever directly communicate with any external IP network, this address scheme also conserves public IP address space

3.4 Dedicated Management VLAN and Console

Because there are CCM support and management staff located at each of the company offices that are running Voice over IP and have a CCM, it is possible to restrict the management of the CCM to only a local terminal that is not remotely accessible. A dedicated management station has been directly connected to both CCMs via an isolated VLAN. The network interface used to management the CCMs is only accessible (via HTTP) by this management console.

Because the flow of traffic on this isolated management VLAN is very light, this same VLAN is used for all CCM database replication traffic and all other

communications that must run between the CCM units. Not only does this free up network resources for actual Voice over IP transactions, but it will also simplify the IDS rule base used on the Voice VLAN.

4 AFTER: IMPLEMENTATION OF THE RECOMMENDATIONS AND THEIR IMPACT

4.1 Recommendations Taken Forward

Out of all the recommendations made in the previous section of this document, only the Network IDS required additional capital expenditure. All of the other changes could be made with only the cost of the consulting manpower required for the planning and implementation of the new network on existing infrastructure components.

Because the cost of losing all voice connectivity to and from a given branch office during business hours is significant, a decision was made by the company to implement all of the controls and recommendations.

A pilot site was selected and a plan approved to implement the split VLAN network design. The migration was implemented as follows:

Phase 1 – Creation and Migration to the New IP VLANs

1. The new VLAN configurations were added to the office's core Ethernet LAN switch. VLAN trunking was enabled on all of the user ports throughout the office. The ports used by the office router and Voice Gateway were also reconfigured and set to the appropriate VLAN.
2. The IP phone configurations were updated so that each phone would begin tagging packets from the user's PC for the newly created IP Data VLAN and tagging the IP telephony packets for the Voice over IP VLAN.
3. The configuration of the office's WAN router was updated so that a secondary Ethernet interface was put into service (the interface already existed but was not in use). This new interface would be used to route to the Voice over IP VLAN only while the original interface is now connected to the IP Data VLAN.

At this point all of the new VLAN and routing configuration were complete. IP data connectivity was tested from a number of user PCs and service platforms to ensure IP communications were possible to the office's service farm, printers, the Internet and several services provided by the company's headquarters. At this point, all Voice over IP was still disabled due to the network changes.

Phase 2 – Migration to the New IP Addressing Scheme

1. The IP address ranges for the office's IP phones were changed to the private range of 10.0.1.0/24 along with the CCM units, the Cisco Voice Gateway and an Ethernet interface on the office's WAN router that was now dedicated to Voice over IP traffic. The IP phone configurations were updated so that each IP phone was aware of the new CCM IP addresses.
2. The IP phones were all rebooted in order to load the new configurations. The IP phones received their new IP addresses from a new DHCP server while the CCM units and routers required a manual configuration change.
3. The dynamic routing configuration on the office WAN router was updated so that the new Voice over IP network range was advertised to the other offices connected via the company's WAN.

4. A number of IP phones were then tested to make sure the initial migration to the new IP address range was successful.
5. Finally, the CCM management consoles were moved from the Voice over IP VLAN onto a new, isolated network segment which connected to two new network interfaces on the CCM units (separated from the Voice over IP VLAN).

At this point, all Voice over IP and IP data connectivity was restored and running as usual. Support staff remained at the pilot site for 24 hours to ensure there were no problems due to the migration. All of the new configurations were documented.

Phase 3 – Implementation of the Network IDS and Hardening of the CCM

Because the company already employed a Network IDS solution at the company headquarters, the same solution was then selected to be rolled out at each of the company's branch locations starting with the pilot site.

A project was then kicked off by the company's security group to implement the Network IDS. A network Sniffer was used to further profile the traffic on the Voice over IP VLAN. Some analysis was then conducted on the Sniffer's data capture so that the Network IDS rule set could be properly formulated.

Once the Network IDS went live at the pilot site, analysis of all of the rule exceptions and alarms took place over a one week period. Many of the alarms were superfluous and only actually indicated that the rule set required tuning. Testing also took place during the week as a rogue PC was allowed onto the Voice over IP VLAN at different times during the day in order to further test the Network IDS rule set.

Within three weeks, the Network IDS was fully tested and functional. The company's security group then placed the Network IDS system into production once the team was trained on how to handle the new class of alerts.

In accordance with the vulnerability scanning, the CCM units had several services disabled and several ports blocked via the Windows 2000 operating system (first in a test environment and then in production).

4.2 Post-Implementation Notes

The results from the implementation at the pilot site were very positive. Besides a few minor mistakes made by the consulting team during Phase 1 and 2 (all of which were easily fixed before the business day began), everything went to plan.

The majority of the end user population was unaware that the migration work took place. All of the application service levels at the pilot site stayed as they were before the migration to place.

4.3 Lessons Learnt

4.3.1 Network Routing Table Audit

When the pilot site's WAN router was configured to route the new 10.0.1.0 /24 IP address range for the Voice over IP VLAN, a route was already found in the routing table for 10.0.0.0 /8. This caused concern because there was now a possibility that this private address range may have already been in use elsewhere inside the company's network.

After tracing the 10.0.0.0 /8 network announcement and reviewing a number of audit documents that included the router making the announcement, it was discovered that the announcement was a historical trace from a development network that no longer existed.

Once the entire 10.0.0.0 /8 network range was pinged and no hosts besides a single router interface were found, it was decided that the migration would move ahead and a change request submitted to have the erroneous network advertisement removed. Because the pilot sight would be announcing a smaller IP network, the pilot site would always be preferred over the larger, class A announcement.

Some implementation risks and hours of wasted time could have been avoided during the night of the first migration if a routing table audit was conducted or at least reviewed (the company does perform a yearly routing table audit) before Phase 1 of the migration took place.

AUDIT PROGRAMME: CISCO CATALYST 5505

GIAK PRACTICAL ASSIGNMENT V1.1 (MAY 2002)

Issue: 1.1
Date: 25-Jan-2003
Author: Craig J. LaCava

GIAK Assignment 2 v1.1

TABLE OF CONTENTS

1 PURPOSE AND SCOPE 1
1.1 Introduction 1
1.2 Audit Program Scope 1
1.3 Objectives and Purpose 2
1.4 Document Layout 3
1.5 Acronyms 3

2 AUDIT CHECKLIST 4
2.1 Information Gathering Prior to the Audit 4
2.2 Cisco Catalyst 5505 Hardware Checklist 5
2.2.1 Power Supplies 5
2.2.2 LAN Switch Card Modules 5
2.3 Cisco Catalyst 5505 CatOS Checklist 5
2.4 Cisco Catalyst 5505 Configuration Checklist 6
2.4.1 Basic Switch Configuration 6
2.4.2 Verify that the correct sc0 interface, default route and other IP Information 6
2.4.3 SNMP Configuration 7
2.4.4 VMPS Configuration 7
2.4.5 DNS Configuration 8
2.4.6 TACACS+ Configuration 8
2.4.7 VTP Configuration 8
2.4.8 CGMP Configuration 9
2.4.9 System Log Configuration 9
2.4.10 NTP Configuration 10
2.4.11 IP Access Lists and the Span Port 10
2.4.12 VLAN Trunk Ports 11
2.4.13 Individual Switch Port Configurations 11

3 CATALYST 5505 AUDIT REPORT 14
3.1 Audit Program Scope 14
3.2 Objectives and Purpose 14

4 CATALYST 5505 AUDIT RESULTS 16
4.1 Cisco Catalyst 5505 Switch and Audit Information 16
4.2 Cisco Catalyst 5505 Hardware Audit 16
4.2.1 Power Supplies 16
4.2.2 LAN Switch Card Modules 16
4.3 Cisco Catalyst 5505 CatOS Checklist 16
4.4 Cisco Catalyst 5505 Configuration Audit 17
4.4.1 Basic Switch Configuration 17
4.4.2 Interface sc0, default route and other IP Information 18
4.4.3 SNMP Configuration Audit 18
4.4.4 VMPS Configuration Audit 19
4.4.5 DNS Configuration Audit 19
4.4.6 TACACS+ Configuration Audit 20

4.4.7 VTP Configuration Audit 21
4.4.8 CGMP Configuration Audit 21
4.4.9 System Log Configuration Audit 22
4.4.10 NTP Configuration Audit 22
4.4.11 IP Access Lists and Span Port Audit 23
4.4.12 VLAN Trunk Port Audit 24
4.4.13 Individual Switch Port Configuration Audit 24
4.5 Audit Results and Analysis 27
4.5.1 Secondary DNS Server IP Address Exception 27
4.5.2 Switch Port Configuration Exceptions 27

APPENDIX A SAMPLE LAN SWITCH PORT CONFIGURATION LISTING ..28

A.1 Port Configuration Listing 28

APPENDIX B REFERENCES 29

5 PURPOSE AND SCOPE

5.1 Introduction

In order to ensure the security and integrity of a typical enterprise local area network (LAN), several formalized audits should take place on a regular basis. While server and workstation audits are usually commonplace within many businesses, audits of the actual network infrastructure are rare.

When compared to servers or workstations, which are often thought of as the most vulnerable components of an office's IT system, low level network infrastructure components are a more subtle target for attackers. A LAN switch that has been compromised can be used to facilitate an eavesdropping attack, where all of the traffic traversing the switch can be captured and examined. Further more, a denial of service (DOS) attack launched from a LAN switch could affect an entire office's network or an entire business if a centralized server farm is attacked.

This audit program has been created using several references, all of which are documented at the end of this section. This audit is based on current IT industry best practices as well as the information security policy of this corporation. This program should be reviewed before the audit is executed and updated (if necessary) every six months.

This document describes an audit program for one of the most popular enterprise LAN switches in today's market place: the Cisco Catalyst 5505. Even though Cisco has recently announced the Catalyst 5000 and 5500 end-of-sale will be on June 30, 2003, the end-of-life date for these switches is not until June 30, 2008.

While some of the audit is specific to the Catalyst 5505's hardware configuration, the majority of the audit checklist can be used to audit most of the Cisco Catalyst 4000, 6500, and 8000 switch model lines (layer-2 only).

5.2 Audit Program Scope

This audit will cover a typical small business office LAN infrastructure. This infrastructure contains four Cisco Catalyst 5505 switches. The audit includes these four switches and logical connectivity to each desktop workstation and server within the physical office location.

The following items are included as a part of the audit program:

1. The hardware configuration of each Catalyst 5505 switch
2. The software (CatOS) installed on each switch supervisor card
3. The layer-2 configuration on each Catalyst 5505 switch
4. The logical hardware addresses associated with each switch port

The following items are not included in the audit program:

1. The physical cabling within the LAN infrastructure
2. The layer-3 routing functionality between virtual LANs (VLANs)
3. Any workstation or server LAN configuration (hardware or software)
4. Any routers connected to the LAN infrastructure

The item listed above have been excluded from this audit because they are covered by other audits programs that are concerned with end user workstations, service platforms, network routing elements and physical cable plants. While it is true that all of these areas are interrelated to the LAN switch elements and important to the overall security of the company's IT infrastructure, the audit programs have been separated for logistical and organizational reasons. To ensure that the audit of each of these areas is thorough, the scope of the audit programs has been separated.

The Cisco Catalyst switches examined within this audit can be classified in two categories: the majority of the switches are for user desktop workstation connectivity and one switch is typically used as a collapse point and for connectivity to the local server farm as well as the Internet.

The Catalyst switches within this program are not equipped with any layer-3 routing hardware or functionality. Only layer-2 (data link and media access control layer) functionality is examined here.

This audit program must be carried out once each quarter (every three months) for each of the company's office locations. Past reports are to be archived by the company Security Officer and stored for a minimum of three years. The results of each audit program are classified as Company Confidential.

5.3 Objectives and Purpose

The objectives of this audit program are:

1. To ensure each LAN switch is configured according to industry best practices provided by Cisco Systems and the worldwide IT community
2. To ensure that the company's LAN switch configuration standards and polices are being followed and implemented correctly
3. To reduce the risk and probability of a security incident involving the company's LAN infrastructure
4. To detect, report and correct unauthorized configuration changes within the company's LAN infrastructure

These objectives have been selected in order to ensure this audit program will verify that the LAN switch elements are configured in compliance with the company's LAN switch security policies and are utilizing industry best practices. By meeting these objectives, the company can mitigate the risks associated with an attack on the company's LAN infrastructure.

5.4 Document Layout

This document is divided into four sections:

Section 1 – Purpose and Scope: This section lays the foundation for the audit program. It sets the audit's objectives, defines the scope of the audit and provides the reader with an introduction to the program.

Section 2 – Audit Checklist: This section contains the checklist tasks that are used to audit each of the company's Cisco Catalyst 5505 switches. The checklist provides guidelines on how to conduct the audit and report on the audit's findings.

Section 3 and 4 – Audit Report: This section includes the audit report from the most recent audit program. Past reports should be archived and available via the company's security officer.

5.5 Acronyms

CAM	– Dynamic Content Addressable Memory
CGMP	– Cisco Group Management Protocol
DNS	– Domain Name Services
INS	– International Network Services
LAN	– Local Area Network
MOTD	– Message of the Day
MAC	– Media Access Control (Logical Address)
NTP	– Network Time Protocol
SNMP	– Simple Network Management Protocol
TACACS	– Terminal Access Control Access Control System
VLAN	– Virtual Local Area Network
VMPS	– VLAN Management Policy Server
VTP	– VLAN Trunking Protocol

6 AUDIT CHECKLIST

6.1 Information Gathering Prior to the Audit

In order to successfully perform this audit, the network management group must provide the auditor with certain information from the documentation archive and from the Cisco Catalyst 5505 switch itself.

The following information will be provided from the current network documentation archive. Each information pack is for a single LAN switch.

1. Switch name, location and network management contact
2. IP addressing information for interface sc0*
3. LAN Switch Port Configuration listing
4. SNMP community strings
5. DNS server addresses
6. TACACS+ server IP addresses
7. The syslog server IP addresses
8. NTP server IP addresses
9. Permitted IP networks
10. VLAN trunk listing

*The sc0 IP interface is the virtual network interface used by the Catalyst Switch management module.

The network management group must also provide various information from the switch itself. The auditor will be provided a log file from the switch to be audited with the output from the following commands:

1. show version – will display the IOS code versions
2. show module – will show what hardware is installed and serial numbers
3. show port – will show a list of switch ports and their configurations
4. show config – will show the switch's configuration
5. show cam dynamic – will show the MAC addresses from each port
6. show time – will show the date and time set on the switch itself (this will provide the auditor with a date and time reference for the log file)

6.2 Cisco Catalyst 5505 Hardware Checklist

6.2.1 Power Supplies

All Cisco Catalyst 5505 switches are equipped with slots for dual AC or DC power supplies. Each switch in production at all of the company's offices should be equipped with dual AC power supplies.

Verify that both power supplies are present, turned on and each shows a green status LED. Trace the AC power cables and verify that they are plugged into two different UPS units. Having both power supplies in working order will defend against a LAN failure in case of a single power supply failure.

Note: This checklist item supports audit program objectives (Section 1.3) 1 and 2.

6.2.2 LAN Switch Card Modules

Compare the LAN Switch Port Configuration Listing (an example of this report can be found in Appendix A) to the output from the 'show module' command from the switch log.

Verify that all of the same switch card modules are in the switch chassis that are noted in the configuration listing by comparing the two records and by physically observing the cards in the switch itself. Compare the serial numbers in the configuration listing to what is listed in the 'show module' output as well. Please note that some switches will have empty slots.

Verifying the switch hardware will ensure the proper records are being kept for network hardware maintenance and the company asset list. Erroneous hardware records can lead to prolonged outages when there is a hardware failure and replacement scenario.

Note: This checklist item supports audit program objective (Section 1.3) 1.

6.3 Cisco Catalyst 5505 CatOS Checklist

Compare the LAN Switch Port Configuration Listing (an example of this report can be found in Appendix A) to the output from the 'show version' command from the switch log. Compare the CatOS version number from the 'show version' output to the configuration listing.

The OS version can be found on the first line of the 'show version' output:

```
WS-C5550 Software, Version McpSW: 6.2(4) NmpSW: 6.2(4)
```

The CatOS version from the switch in the example above is 6.2(4). It is important that all of the company's LAN switches are using a stable, tested and secure version of CatOS code that has been certified for production by the network management and corporate security groups. Using a non-certified CatOS version can open the LAN switch up to certain attacks, operating faults and unexpected outages. All the Catalyst switches within The Company should be running the same version of CatOS.

Note: This checklist item supports audit program objectives (Section 1.3) 1 and 2.

6.4 Cisco Catalyst 5505 Configuration Checklist

6.4.1 Basic Switch Configuration

Verify the following configuration parameters for the switch:

```
set prompt <Command Line Prompt>
set length 24 default

! Verify the idle logout time is set to 5 minutes:
set logout 5
set banner motd <MOTD Text>
set system name  <Switch Name>
set system location <Switch Location>
set system contact  <Switch NMS Contact>
```

The correct command line prompt, switch name, MOTD (unauthorized access warning), location and contact will be provided by the Network Management group prior to the audit.

Verify that the idle logout session time is set to five minutes in order to prevent unauthorized access for idle terminal sessions.

Note: This checklist item supports audit program objectives (Section 1.3) 1 and 2.

6.4.2 Verify that the correct sc0 interface, default route and other IP Information

Verify that the correct sc0 interface, default route and other IP information is specified in the switch's configuration:

```
! Interface sc0 is used for IP connectivity:
set interface sc0 10 <Switch IP> <IP Subnet Mask> <Broadcast IP>

! Interface sl0 is for SLIP connectivity and is not used:
set interface sl0 down

! Misc IP settings - make sure IP redirect is disabled:
set arp agingtime 1200
set ip redirect   disable
set ip unreachable   enable
set ip fragmentation enable

! Be sure that the default route is set correctly:
set ip route 0.0.0.0         <Default Gateway>     1
```

The correct sc0 IP address, subnet mask, broadcast address as well as the correct default gateway for the default route can be obtained from the Network Management group.

Be sure to note that the IP redirect command is set to disable otherwise switch management traffic can be redirected to unauthorized destinations.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

6.4.3 SNMP Configuration

Verify that the switch's SNMP configuration matches the following:

```
! Set the SNMP community strings – read-write-all is not used:
set snmp community read-only      <RO Community String>
set snmp community read-write     <RW Community String>

! Set the types of SNMP traps that the switch  should report:
set snmp rmon disable
set snmp trap enable module
set snmp trap enable chassis
set snmp trap disable bridge
set snmp trap disable repeater
set snmp trap disable vtp
set snmp trap enable auth
set snmp trap enable ippermit

! Set the SNMP trap destination and community string:
set snmp trap nms.company.com     <Trap Community String>
```

Verify there are no other SNMP configuration lines on the switch other than what is listed above. The SNMP configuration lines will always be grouped together.

The current SNMP community strings must match the strings that are currently in deployment. The auditor can obtain the strings from the Network Management group with written permission from the Information Security group. Verify that the current strings comply with the company policy regarding strong passwords.

The company policy dictates that these community strings are to be changed every month by the network management group in order to prevent unauthorized access to the switch.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

6.4.4 VMPS Configuration

The company does not use VLAN Management Policy Servers (VMPS). Verify VMPS is turned off within the switch's configuration:

```
! Disable VMPS on the switch
set vmps state disable
```

With the VMPS state set to disable, all other VMPS configurations are ignored (though still present by default in the switch's configuration) and do not require auditing.

Note: This checklist item supports audit program objectives (Section 1.3) 2 and 3.

6.4.5 DNS Configuration

Verify that the switch is configured with the correct Domain Name Service (DNS) configuration:

```
set ip dns enable
set ip dns domain company.com
set ip dns server <Primary DNS> primary
set ip dns server <Secondary DNS>
```

The correct primary and secondary DNS server IP addresses will be provided by the Network Management group prior to the start of the audit.

Verify that the domain is set to company.com. These DNS settings are only used by people who are actually logged into the switch's management module.

Note: This checklist item supports audit program objectives (Section 1.3) 2 and 3.

6.4.6 TACACS+ Configuration

Verify that the switch is configured with the correct TACACS+ configuration:

```
set tacacs attempts 3
set tacacs directedrequest disable
set tacacs timeout 5

! Verify the correct TACACS+ encryption key is set
! as well as the IP address for the TACACS+ server:
set tacacs key <TACACS KEY>
set tacacs server <TACACS SERVER IP> primary
set tacacs server <TACACS SERVER IP> secondary

! Verify TACACS authentification is enabled:
set authentication login tacacs enable
set authentication login local enable
set authentication enable tacacs enable
set authentication enable local enable
```

The correct TACACS+ key and server IP addresses will be provided by the Network Management group prior to the start of the audit.

Verify that TACACS+ is turned on for both user level login and privileged enable mode. TACACS+ provides authentication for switch administrators and ensures that only authorized personnel access the switch's management module. TACACS+ will also log all switch access attempts at a central server.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

6.4.7 VTP Configuration

Verify that the switch is configured not to use the VLAN Trunking Protocol (VTP). VTP is not used within the company and should always be disabled.

```
! Verify the switch is in VTP transparent mode:
set vtp mode transparent
```

VTP can not be disabled. By configuring the switch to use VTP transparent mode, the switch will ignore any VTP traffic sent to the switch. Any other VTP configurations will be immaterial if the switch is configured for transparent mode. Malicious VTP commands could be used for a denial of service attack.

Note: This checklist item supports audit program objecti ves (Section 1.3) 2 and 3.

6.4.8 CGMP Con figuration

Verify that the switch is configured not to use the Cisco Group Management Protocol (CGMP). Multicast is not used within the company, thus CGMP should always be disabled.

```
! Verify that CGMP is disabled:
set cgmp disable
set cgmp leave disable
```

While there is no substantial risk in having CGMP enabled when it is not in use, CGMP should be disabled in accordance to the company policy on Cisco Catalyst switch configuration. Best practices dictate that any Catalyst OS feature not in use should be disabled.

Note: This checklist item supports audit program objectives (Section 1.3) 2 and 3.

6.4.9 System Log Configuration

Verify that the switch is configured to send System Log (syslog) messages to the correct syslog servers.

```
! Enable syslog messaging:
set logging server enable

! Set the primary and secondary syslog destination IP addresses:
set logging server <Primary syslog Server IP>
set logging server <Secondary syslog Server IP>
```

The correct syslog server IP addresses will be provided by the Network Management group prior to the start of the audit.

With syslog enabled, all of the switch's system messages are sent and logged permanently on both of the company's primary and secondary LAN switch syslog servers (usually on write-once media). The logs are reviewed in real time in order to alert operations about any potential LAN switch networking issues.

The remote logs are also stored for up to three years in case a review is required after a security incident. While many unauthorized attackers will clear the logs of a penetrated system locally, it is much more difficult to comprise the logs stored on the company's remote syslog servers.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

6.4.10 NTP Configuration

Verify that the switch is correctly configured to use the Network Time Protocol (NTP).

```
! Enable NTP and disable the switch as a NTP broadcast client:
set ntp client enable
set ntp broadcastclient disable

! Set the primary and secondary NTP server IP address:
set ntp server <Primary NTP Server IP>
set ntp server <Secondary NTP Server IP>

! Set the correct time zone:
set timezone GMT 0 0
```

The correct NTP server IP addresses will be provided by the Network Management group prior to the start of the audit.

NTP enables the company to ensure that all LAN switches are synchronized to a single time source. This will ensure that all of the syslog entries have the correct date and time stamp, which is essential when comparing events from different devices during an incident investigation.

The company policy states that all devices are set to the GMT time zone no matter where they are located.

Note: This checklist item supports audit program objectives (Section 1.3) 2 and 3.

6.4.11 IP Access Lists and the Span Port

Remote access to the switch's management module is restricted to certain networks belonging to the network management group. Remote access requests from all other IP networks are to be rejected.

```
! Turn on IP access lists for all IP connectivity:
set ip permit enable all

! Send SNMP traps to warn about unauthorized access attempts:
set snmp trap enable ippermit

! Set the permitted IP networks:
set ip permit <Permitted IP Network 1> <IP Subnet Mask>
set ip permit <Permitted IP Network 2> <IP Subnet Mask>
set ip permit <Permitted IP Network 3> <IP Subnet Mask>

! Ensure that no span port is active:
set span disable
```

The three permitted IP networks and subnet mask pairs will be provided by the network management group prior to the audit.

Verify that there are no other 'set ip permit' commands other than the three specified by the network management group. These IP permit statements help protect the switch from unauthorized access and help track unauthorized access attempts.

The span port allows a port on the switch to receive and monitor all of the traffic traversing the switch, a VLAN or a number of selected ports. While a span port is sometimes used for troubleshooting, it should always be disabled when not in use.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

6.4.12 VLAN Trunk Ports

Each switch should have only certain ports set to allow VLAN trunking. The network management group will provide a configuration listing before the start of the audit. This listing will dictate how each switch port should be configured and VLAN trunks.

The typical end-user access switch only allows trunking on the two Fast or Gigabit Ethernet ports located on the management module card within slot 1.

```
! Verify that the correct ports are set as VLAN trunks:
set trunk 1/1 on dot1q 1-1005
set trunk 1/2 on dot1q 1-1005
```

The above configuration example is from a typical switch from an office floor where only the two ports on the supervisor card in slot 1 are used for VLAN trunking. The trunking type is set to 802.1q, which is the corporate and industry standard for VLAN trunking. It is important to ensure only the connections between the LAN switches are used for VLAN trunking or else it is possible for unauthorized users to observe network traffic.

Note: This checklist item supports audit program objectives (Section 1.3) 2, 3 and 4.

6.4.13 Individual Switch Port Configurations

The final switch configuration audit activity is associated with the status and configuration of each switch port. The following port configurations are to be verified during the audit:

1. Status (enabled or disabled)
2. Name (user defined port name)
3. VLAN (number assigned to the port)
4. Duplex (half or full)
5. Speed (10MB, 100MB or 1000MB)

Finally, the Dynamic Content-Addressable Memory (CAM) tables are to be checked to make sure the expected Ethernet MAC address is associated with each end-user switch port. The CAM table will display the Ethernet MAC address it has learned from the traffic coming into each switch port. If the address does not match the end-user records or more than one address is

being displayed for an end-user port, there may be an unauthorized device attached to the switch.

The network management group will supply a port configuration listing and a switch CAM table prior to the start of the audit. Each port must be checked against these records. Appendix A supplies a sample port configuration listing and CAM table for end-user ports. The CAM table audit does not need to be applied to VLAN trunk ports.

The port configuration listing should be compare to the results of the CatOS 'show port' command and 'show cam dynamic' command. An example of each is shown below.

```
Cat OS Prompt> show port
Port  Name               Status     Vlan       Level  Duplex   Speed  Type
----- ------------------ ---------- ---------- ------ ------   -----  -----------
 1/1   Tr1 uk1-esw-01/1.1 connected             normal  a-full a-1000  1000BaseFX
 1/2   Tr1 uk1-esw-01/2.1 connected             normal  a-full a-1000  1000BaseFX
 2/1   User 63782         connected  200        normal  a-full a-100 10/100BaseTX
 2/2   User 63783         connected  200        normal  a-full a-100 10/100BaseTX
 2/3   User 63784         connected  200        normal  a-full a-100 10/100BaseTX
 2/4   User 63785         connected  200        normal  a-full a-100 10/100BaseTX
 2/5   User 63786         connected  200        normal  a-full a-100 10/100BaseTX
 2/6   User 63787         connected  200        normal  a-full a-100 10/100BaseTX
 2/7   User 63788         connected  200        normal  a-full a-100 10/100BaseTX
 2/8   User 63789         connected  200        normal  a-full a-100 10/100BaseTX
 2/9                      disabled   200        normal   auto  auto  10/100BaseTX
 2/10  User 63791         connected  200        normal  a-full a-100 10/100BaseTX
. . .
```

The partial output of a 'show port' command from a LAN switch within the company is shown above. Notice that the users are all connected to module 2, and module 1 is used to connect to another switch via a VLAN trunk. This is a typical configuration for an office floor, end-user LAN switch.

The port names correspond to user numbers. Each of the users connected to this switch are assigned to VLAN 200. Port 2/9 is disabled and not in use at this time. All of the users have Ethernet network adaptors that are capable of full duplex 100MB network connectivity. The VLAN trunk ports on module 1 are Gigabit Ethernet ports (1000MB).

```
Cat OS Prompt> sh cam dynamic
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ------------------------------------------
200   00-01-02-bc-e2-2f             2/1  [ALL]
200   00-01-02-bc-ab-55             2/2  [ALL]
200   00-01-02-bc-6e-38             2/3  [ALL]
200   00-01-02-bc-2e-77             2/4  [ALL]
200   00-01-02-bc-0a-85             2/5  [ALL]
200   00-01-02-bc-4b-32             2/6  [ALL]
200   00-01-02-bc-cb-11             2/7  [ALL]
```

```
200   00-01-02-bc-ae-90            2/8  [ALL]
200   00-01-02-bc-45-03            2/10 [ALL]
```

Above is a partial output of a 'show cam dynamic' command from the same LAN switch. For each user port, there should be only one Ethernet MAC address associated with the port and this address should correspond to port configuration listing provided by the network management group.

By verifying each port configuration and the MAC addresses in use by the user population, unauthorized access and unauthorized devices on the company LAN can be detected and corrected before a security incident occurs.

Note: This checklist item supports audit program objectives (Section 1.3) 2, 3 and 4.

7 CATALYST 5505 AUDIT REPORT

Please note that this report has been added into the audit program as an example only. An actual Audit Results Report would ordinarily be produced, submitted and filed as a separate document.

7.1 Audit Program Scope

This infrastructure contains four Cisco Catalyst 5505 switches within building UK1. The audit includes one LAN switch and logical connectivity to each desktop workstation and server within the physical office location.

The following items are included as a part of the audit program:

1. The hardware configuration of each Catalyst 5505 switch
2. The software (CatOS) installed on each switch supervisor card
3. The layer-2 configuration on each Catalyst 5505 switch
4. The logical hardware addresses associated with each switch port

The following items are not included in the audit program:

1. The physical cabling within the LAN infrastructure
2. The layer-3 routing functionality between virtual LANs (VLANs)
3. Any workstation or server LAN configuration (hardware or software)
4. Any routers connected to the LAN infrastructure

The item listed above have been excluded from this audit because they are covered by other audits programs that are concerned with end user workstations, service platforms, network routing elements and physical cable plants. While it is true that all of these areas are interrelated to the LAN switch elements and important to the overall security of the company's IT infrastructure, the audit programs have been separated for logistical and organizational reasons. To ensure that the audit of each of these areas is thorough, the scope of the audit programs has been separated.

The Catalyst switch within this audit is not equipped with any layer-3 routing hardware or functionality. Only layer-2 (data link and media access control layer) functionality is examined here.

7.2 Objectives and Purpose

The objectives of this audit program are:

1. To ensure each LAN switch is configured according to industry best practices provided by Cisco Systems and the worldwide IT community

2. To ensure that the company's LAN switch configuration standards and polices are being followed and implemented correctly
3. To reduce the risk and probability of a security incident involving the company's LAN infrastructure
4. To detect, report and correct unauthorized configuration changes within the company's LAN infrastructure

These objectives have been selected in order to ensure this audit program will verify that the LAN switch elements are configured in compliance with the company's LAN switch security policies and are utilizing industry best practices. By meeting these objectives, the company can mitigate the risks associated with an attack on the company's LAN infrastructure.

8 CATALYST 5505 AUDIT RESULTS

8.1 Cisco Catalyst 5505 Switch and Audit Information

This audit report can also be modified and used as a checklist worksheet for this audit program. One worksheet is required per switch.

Switch name:	uk1-ews-01
Switch IP address (sc0):	xxx.yyy.142.121
Date of Audit:	12-Nov-2002

8.2 Cisco Catalyst 5505 Hardware Audit

8.2.1 Power Supplies

All Cisco Catalyst 5505 switches are equipped with slots for dual AC or DC power supplies. Each switch in production at all of the company's offices should be equipped with dual AC power supplies.

Verify that both power supplies are present, turned on and each shows a green status LED. Trace the AC power cables and verify that they are plugged into two different UPS units. Having both power supplies in working order will defend against a LAN failure in case of a single power supply failure.

Note: This checklist item supports audit program objectives (Section 1.3) 1 and 2.

8.2.2 LAN Switch Card Modules

Compare the LAN Switch Port Configuration Listing (an example of this report can be found in Appendix A) to the output from the 'show module' command from the switch log.

Verify that all of the same switch card modules are in the switch chassis that are noted in the configuration listing by comparing the two records and by physically observing the cards in the switch itself. Compare the serial numbers in the configuration listing to what is listed in the 'show module' output as well. Please note that some switches will have empty slots.

Verifying the switch hardware will ensure the proper records are being kept for network hardware maintenance and the company asset list. Erroneous hardware records can lead to prolonged outages when there is a hardware failure and replacement scenario.

Note: This checklist item supports audit program objective (Section 1.3) 1.

8.3 Cisco Catalyst 5505 CatOS Checklist

Compare the LAN Switch Port Configuration Listing (an example of this report can be found in Appendix A) to the output from the 'show version' command from the switch log. Compare the CatOS version number from the 'show version' output to the configuration listing.

The OS version can be found on the first line of the 'show version' output:

```
WS-C5550 Software, Version McpSW: 6.2(4) NmpS W: 6.2(4)
```

The CatOS version from the switch in the example above is 6.2(4). It is important that all of the company's LAN switches are using a stable, tested and secure version of CatOS code that has been certified for production by the network management and corporate security groups. Using a non-certified CatOS version can open the LAN switch up to certain attacks, operating faults and unexpected outages. All the Catalyst switches within The Company should be running the same version of CatOS.

Note: This checklist item supports audit program objectives (Section 1.3) 1 and 2.

Cisco Catalyst 5505 Hardware Audit Results

Power supplies both present	**Pass**
Power supplies both functioning	**Pass**
Power supplies plugged into diverse UPS units	**Pass**
LAN Switch Cards present and functioning	**Pass**
Cisco CatOS version is correct	**Pass**

8.4 Cisco Catalyst 5505 Configuration Audit

8.4.1 Basic Switch Configuration

Verify the following configuration parameters for the switch:

```
set prompt <Command Line Prompt>
set length 24 default

! Verify the idle logout time is set to 5 minutes:
set logout 5
set banner motd <MOTD Text>
set system name  <Switch Name>
set system location <Switch Location>
set system contact  <Switch NMS Contact>
```

The correct command line prompt, switch name, MOTD (unauthorized access warning), location and contact will be provided by the Network Management group prior to the audit.

Verify that the idle logout session time is set to five minutes in order to prevent unauthorized access for idle terminal sessions.

Note: This checklist item supports audit program objectives (Section 1.3) 1 and 2.

Basic Switch Configuration Audit Results

Logout time is set to 5 minutes	**Pass**
The switch's MOTD is correct	**Pass**
The switch name is configured correctly	**Pass**
The switch location is configured correctly	**Pass**
The system contact is configured correctly	**Pass**

8.4.2 Interface sc0, default route and other IP Information

Verify that the correct sc0 interface, default route and other IP information is specified in the switch's configuration:

```
! Interface sc0 is used for IP connectivity:
set interface sc0 10 <Switch IP> <IP Subnet Mask> <Broadcast IP>

! Interface sl0 is for SLIP connectivity and is not used:
set interface sl0 down

! Misc IP settings - make sure IP redirect is disabled:
set arp agingtime 1200
set ip redirect   disable
set ip unreachable   enable
set ip fragmentation enable

! Be sure that the default route is set correctly:
set ip route 0.0.0.0         <Default Gateway>     1
```

The correct sc0 IP address, subnet mask, broadcast address as well as the correct default gateway for the default route can be obtained from the Network Management group.

Be sure to note that the IP redirect command is set to disable otherwise switch management traffic can be redirected to unauthorized destinations.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

Interface sc0, default route and other IP Information Audit Results

Interface sc0 is configured correctly	**Pass**
Interface sl0 is configured correctly	**Pass**
The switch's miscellaneous IP settings are correct	**Pass**
The switch's default route settings are correct	**Pass**

8.4.3 SNMP Configuration Audit

Verify that the switch's SNMP configuration matches the following:

```
! Set the SNMP community strings - read-write-all is not used:
set snmp community read-only      <RO Community String>
set snmp community read-write     <RW Community String>

! Set the types of SNMP traps that the switch should report:
set snmp rmon disable
set snmp trap enable module
set snmp trap enable chassis
set snmp trap disable bridge
set snmp trap disable repeater
set snmp trap disable vtp
set snmp trap enable auth
set snmp trap enable ippermit
```

```
! Set the SNMP trap destination and community string:
set snmp trap nms.company.com      <Trap Community String>
```

Verify there are no other SNMP configuration lines on the switch other than what is listed above. The SNMP configuration lines will always be grouped together.

The current SNMP community strings must match the strings that are currently in deployment. The auditor can obtain the strings from the Network Management group with written permission from the Information Security group. Verify that the current strings comply with the company policy regarding strong passwords.

The company policy dictates that these community strings are to be changed every month by the network management group in order to prevent unauthorized access to the switch.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

SNMP Configuration Audit Results

The switch's SNMP RO community string is correct	**Pass**
The switch's SNMP RW community string is correct	**Pass**
RMON is disabled on the switch	**Pass**
All of the correct SNMP traps are enabled/disabled	**Pass**
The SNMP trap destination and community string is correct	**Pass**

8.4.4 VMPS Configuration Audit

The company does not use VLAN Management Policy Servers (VMPS). Verify VMPS is turned off within the switch's configuration:

```
! Disable VMPS on the switch
set vmps state disable
```

With the VMPS state set to disable, all other VMPS configurations are ignored (though still present by default in the switch's configuration) and do not require auditing.

Note: This checklist item supports audit program objectives (Section 1.3) 2 and 3.

VMPS Configuration Audit Results

VMPS is disabled on the switch	**Pass**

8.4.5 DNS Configuration Audit

Verify that the switch is configured with the correct Domain Name Service (DNS) configuration:

```
set ip dns enable
set ip dns domain company.com
set ip dns server <Primary DNS> primary
set ip dns server <Secondary DNS>
```

The correct primary and secondary DNS server IP addresses will be provided by the Network Management group prior to the start of the audit.

Verify that the domain is set to company.com. These DNS settings are only used by people who are actually logged into the switch's management module.

Note: This checklist item supports audit program objectives (Section 1.3) 2 and 3.

DNS Configuration Audit Results

DNS is enabled on the switch	**Pass**
The DNS domain is configured correctly	**Pass**
The primary DNS server is configured correctly	**Pass**
The primary DNS server is configured correctly	**Fail**

The address of the secondary DNS server is incorrect. The effect of this abnormality would only be felt if and when the primary DNS server was either down or not reachable from the switch's management module. This exception is minor and does not pose much of a

To remediate this audit exception, a change request will be made with the network operations group to change the switch's secondary DNS server configuration to the correct IP address.

8.4.6 TACACS+ Configuration Audit

Verify that the switch is configured with the correct TACACS+ configuration:

```
set tacacs attempts 3
set tacacs directedrequest disable
set tacacs timeout 5

! Verify the correct TACACS+ encryption key is set
! as well as the IP address for the TACACS+ server:
set tacacs key <TACACS KEY>
set tacacs server <TACACS SERVER IP> primary
set tacacs server <TACACS SERVER IP> secondary

! Verify TACACS authentification is enabled:
set authentication login tacacs enable
set authentication login local enable
set authentication enable tacacs enable
set authentication enable local enable
```

The correct TACACS+ key and server IP addresses will be provided by the Network Management group prior to the start of the audit.

Verify that TACACS+ is turned on for both user level login and privileged enable mode. TACACS+ provides authentication for switch administrators and ensures that only authorized personnel access the switch's management module. TACACS+ will also log all switch access attempts at a central server.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

TACACS+ Configuration Audit Results

The TACACS+ number of attempts setting is correct	**Pass**
The TACACS+ directed request setting is correct	**Pass**
The TACACS+ request timeout setting is correct	**Pass**
The TACACS+ key configuration is correct	**Pass**
The primary TACACS+ server is set correctly	**Pass**
The secondary TACACS+ server is set correctly	**Pass**
TACACS+ authentication for switch logon is enabled	**Pass**
TACACS+ authentication for switch enable mode is enabled	**Pass**
Local authentication (secondary) is enabled for logon	**Pass**
Local authentication (secondary) is enabled for enable mode	**Pass**

8.4.7 VTP Configuration Audit

Verify that the switch is configured not to use the VLAN Trunking Protocol (VTP). VTP is not used within the company and should always be disabled.

```
! Verify the switch is in VTP transparent mode:
set vtp mode transparent
```

VTP can not be disabled. By configuring the switch to use VTP transparent mode, the switch will ignore any VTP traffic sent to the switch. Any other VTP configurations will be immaterial if the switch is configured for transparent mode. Malicious VTP commands could be used for a denial of service attack.

Note: This checklist item supports audit program objectives (Section 1.3) 2 and 3.

VTP Configuration Audit Results

The switch's VTP mode is set to transparent	**Pass**

8.4.8 CGMP Configuration Audit

Verify that the switch is configured not to use the Cisco Group Management Protocol (CGMP). Multicast is not used within the company, thus CGMP should always be disabled.

```
! Verify that CGMP is disabled:
set cgmp disable
set cgmp leave disable
```

While there is no substantial risk in having CGMP enabled when it is not in use, CGMP should be disabled in accordance to the company policy on Cisco Catalyst switch configuration. Best practices dictate that any Catalyst OS feature not in use should be disabled.

Note: This checklist item supports audit program objectives (Section 1.3) 2 and 3.

CGMP Configuration Audit Results

CGMP is disabled on the switch	**Pass**
CGMP leave is disabled on the switch	**Pass**

8.4.9 System Log Configuration Audit

Verify that the switch is configured to send System Log (syslog) messages to the correct syslog servers.

```
! Enable syslog messaging:
set logging server enable

! Set the primary and secondary syslog destination IP addresses:
set logging server <Primary syslog Server IP>
set logging server <Secondary syslog Server IP>
```

The correct syslog server IP addresses will be provided by the Network Management group prior to the start of the audit.

With syslog enabled, all of the switch's system messages are sent and logged permanently on both of the company's primary and secondary LAN switch syslog servers (usually on write-once media). The logs are reviewed in real time in order to alert operations about any potential LAN switch networking issues.

The remote logs are also stored for up to three years in case a review is required after a security incident. While many unauthorized attackers will clear the logs of a penetrated system locally, it is much more difficult to comprise the logs stored on the company's remote syslog servers.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

Syslog Configuration Audit Results

System logging is enabled on the switch	**Pass**
The primary syslog server is set correctly	**Pass**
The secondary syslog server is set correctly	**Pass**

8.4.10 NTP Configuration Audit

Verify that the switch is correctly configured to use the Network Time Protocol (NTP).

```
! Enable NTP and disable the switch as a NTP broadcast client:
set ntp client enable
set ntp broadcastclient disable

! Set the primary and secondary NTP server IP address:
set ntp server <Primary NTP Server IP>
set ntp server <Secondary NTP Server IP>

! Set the correct time zone:
set timezone GMT 0 0
```

The correct NTP server IP addresses will be provided by the Network Management group prior to the start of the audit.

NTP enables the company to ensure that all LAN switches are synchronized to a single time source. This will ensure that all of the syslog entries have the correct date and time stamp, which is essential when comparing events from different devices during an incident investigation.

The company policy states that all devices are set to the GMT time zone no matter where they are located.

Note: This checklist item supports audit program objectives (Section 1.3) 2 and 3.

NTP Configuration Audit Results

NTP is enabled on the switch	**Pass**
NTP broadcast is disabled on the switch	**Pass**
The primary NTP server is set correctly	**Pass**
The secondary NTP server is set correctly	**Pass**

8.4.11 IP Access Lists and Span Port Audit

Remote access to the switch's management module is restricted to certain networks belonging to the network management group. Remote access requests from all other IP networks are to be rejected.

```
! Turn on IP access lists for all IP connectivity:
set ip permit enable all

! Send SNMP traps to warn about unauthorized access attempts:
set snmp trap enable ippermit

! Set the permitted IP networks:
set ip permit <Permitted IP Network 1> <IP Subnet Mask>
set ip permit <Permitted IP Network 2> <IP Subnet Mask>
set ip permit <Permitted IP Network 3> <IP Subnet Mask>

! Ensure that no span port is active:
set span disable
```

The three permitted IP networks and subnet mask pairs will be provided by the network management group prior to the audit.

Verify that there are no other 'set ip permit' commands other than the three specified by the network management group. These IP permit statements help protect the switch from unauthorized access and help track unauthorized access attempts.

The span port allows a port on the switch to receive and monitor all of the traffic traversing the switch, a VLAN or a number of selected ports. While a span port is sometimes used for troubleshooting, it should always be disabled when not in use.

Note: This checklist item supports audit program objectives (Section 1.3) 1, 2 and 3.

IP Access Lists and Span Port Audit Results

IP access lists are enabled on the switch for all IP traffic	**Pass**
SNMP traps are enabled for unauthorized access attempts	**Pass**
All of the correct IP permit lists are configured	**Pass**
No additional IP permit lists are configured	**Pass**
The switch's span port is disabled	**Pass**

8.4.12 VLAN Trunk Port Audit

Each switch should have only certain ports set to allow VLAN trunking. The network management group will provide a configuration listing before the start of the audit. This listing will dictate how each switch port should be configured and VLAN trunks.

The typical end-user access switch only allows trunking on the two Fast or Gigabit Ethernet ports located on the management module card within slot 1.

```
! Verify that the correct ports are set as VLAN trunks:
set trunk 1/1 on dot1q 1-1005
set trunk 1/2 on dot1q 1-1005
```

The above configuration example is from a typical switch from an office floor where only the two ports on the supervisor card in slot 1 are used for VLAN trunking. The trunking type is set to 802.1q, which is the corporate and industry standard for VLAN trunking. It is important to ensure only the connections between the LAN switches are used for VLAN trunking or else it is possible for unauthorized users to observe network traffic.

Note: This checklist item supports audit program objectives (Section 1.3) 2, 3 and 4.

VLAN and Trunk Port Audit Results

The switch's trunk ports are all configured correctly	**Pass**
No additional trunk ports are all configured on the switch	**Pass**

8.4.13 Individual Switch Port Configuration Audit

The final switch configuration audit activity is associated with the status and configuration of each switch port. The following port configurations are to be verified during the audit:

6. Status (enabled or disabled)
7. Name (user defined port name)
8. VLAN (number assigned to the port)
9. Duplex (half or full)
10. Speed (10MB, 100MB or 1000MB)

Finally, the Dynamic Content-Addressable Memory (CAM) tables are to be checked to make sure the expected Ethernet MAC address is associated with each end-user switch port. The CAM table will display the Ethernet MAC address it has learned from the traffic coming into each switch port. If the address does not match the end-user records or more than one address is being displayed for an end-user port, there may be an unauthorized device attached to the switch.

The network management group will supply a port configuration listing and a switch CAM table prior to the start of the audit. Each port must be checked against these records. Appendix A supplies a sample port configuration listing and CAM table for end-user ports. The CAM table audit does not need to be applied to VLAN trunk ports.

The port configuration listing should be compare to the results of the CatOS 'show port' command and 'show cam dynamic' command. An example of each is shown below.

```
Cat OS Prompt> show port
Port  Name               Status     Vlan       Level  Duplex  Speed  Type
----- ------------------ ---------- ---------- ------ ------- -----  -----------
 1/1   Tr1 uk1-esw-01/1.1 connected             normal  a-full a-1000  1000BaseFX
 1/2   Tr1 uk1-esw-01/2.1 connected             normal  a-full a-1000  1000BaseFX
 2/1   User 63782         connected  200        normal  a-full a-100 10/100BaseTX
 2/2   User 63783         connected  200        normal  a-full a-100 10/100BaseTX
 2/3   User 63784         connected  200        normal  a-full a-100 10/100BaseTX
 2/4   User 63785         connected  200        normal  a-full a-100 10/100BaseTX
 2/5   User 63786         connected  200        normal  a-full a-100 10/100BaseTX
 2/6   User 63787         connected  200        normal  a-full a-100 10/100BaseTX
 2/7   User 63788         connected  200        normal  a-full a-100 10/100BaseTX
 2/8   User 63789         connected  200        normal  a-full a-100 10/100BaseTX
 2/9                      disabled   200        normal   auto  auto  10/100BaseTX
 2/10  User 63791         connected  200        normal  a-full a-100 10/100BaseTX
. . .
```

The partial output of a 'show port' command from a LAN switch within the company is shown above. Notice that the users are all connected to module 2, and module 1 is used to connect to another switch via a VLAN trunk. This is a typical configuration for an office floor, end-user LAN switch.

The port names correspond to user numbers. Each of the users connected to this switch are assigned to VLAN 200. Port 2/9 is disabled and not in use at this time. All of the users have Ethernet network adaptors that are capable of full duplex 100MB network connectivity. The VLAN trunk ports on module 1 are Gigabit Ethernet ports (1000MB).

```
Cat OS Prompt> sh cam dynamic
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ------------------------------------------
200   00-01-02-bc-e2-2f             2/1  [ALL]
200   00-01-02-bc-ab-55             2/2  [ALL]
200   00-01-02-bc-6e-38             2/3  [ALL]
200   00-01-02-bc-2e-77             2/4  [ALL]
200   00-01-02-bc-0a-85             2/5  [ALL]
200   00-01-02-bc-4b-32             2/6  [ALL]
200   00-01-02-bc-cb-11             2/7  [ALL]
200   00-01-02-bc-ae-90             2/8  [ALL]
200   00-01-02-bc-45-03             2/10 [ALL]
```

Above is a partial output of a 'show cam dynamic' command from the same LAN switch. For each user port, there should be only one Ethernet MAC address associated with the port and this address should correspond to port configuration listing provided by the network management group.

By verifying each port configuration and the MAC addresses in use by the user population, unauthorized access and unauthorized devices on the company LAN can be detected and corrected before a security incident occurs.

Note: This checklist item supports audit program objectives (Section 1.3) 2, 3 and 4.

Individual Switch Port Configuration Audit Results

Each of the switch ports are configured correctly **Fail**

1. The MAC address on port 2/5 does not match the configuration records.
2. Port number 2/11 is enabled, but not active at this time.
3. There are multiple MAC address associated with port 2/20.

While exceptions 1 and 2 are minor, exception 3 could constitute a serious breach of the company LAN security policy.

To remediate this audit exception, a change request will be made with the network operations group to change the switch's secondary DNS server configuration to the correct IP address.

8.5 Audit Results and Analysis

The audit was conducted successfully and resulted in only four checklist exceptions, most of which are associated with the switch port configuration audit. Only one of the exceptions was classified as a serious exception.

The audit process was followed without exception and worked well. The audit was conducted within just over four hours (for the one switch). All of the switch configuration information was provided in a timely manner to the auditor prior the audit taking place.

8.5.1 Secondary DNS Server IP Address Exception

While only a minor exception, this configuration error could cause a loss of connectivity from the switch's management module – only if the primary DNS server was unavailable and only if the module required a domain name lookup. Because most all of the switch's configuration uses IP addresses and not domain names, the impact of this exception is very low.

By reviewing change control records, it was discovered that the exception was cause by the failure of a change control script and process. A CiscoWorks 2000 configuration management script failed to change the secondary DNS server configuration on this switch. The change control verification process also failed to notice the error.

8.5.2 Switch Port Configuration Exceptions

There were three exceptions in this audit area. Two of them were very low impact exceptions: a mismatched MAC address and an inactive port during the audit. The MAC address was caused by a fault in the change control process. The end-user that is connected to this port had their workstation's Ethernet card replaced. The new MAC address was not properly recorded with the network management group. The inactive port was simply due to an end-user not being at work on the day of the audit. His or her workstation was powered off at the time.

The third exception is much more serious. After further investigation, it was discovered that a user had connected an Ethernet hub to their desk LAN port and connected two unauthorized laptop PCs to the company LAN network. This is why multiple MAC addresses were seen by the Cisco switch's CAM.

Because these laptops did not use the company's standard build, they introduce a security risk to the company's network. This is a blatant breach of company policy. A formal incident report was filed and the information security team removed the hub from the network.

This incident has spurred a discussion on the possibility of further locking down LAN switch ports so that they are only active when an authorized MAC address is detected on the port.

APPENDIX A SAMPLE LAN SWITCH PORT CONFIGURATION LISTING

A.1 Port Configuration Listing

Switch Name: uk1-esw-02

IP Address: xxx.yyy.142.121

Cisco Cat OS Version: 6.3(2)

Hardware Modules:

	Card model and description:		Serial No:
Slot 1:	WS-5550	– Supervisor IIIG	xxxyyy03345
Slot 2:	WS-X5234-RJ45	– 24 port 10/100TX	xxxyyy06986
Slot 3:	WS-X5234-RJ45	– 24 port 10/100TX	xxxyyy06987
Slot 4:	WS-X5234-RJ45	– 24 port 10/100TX	xxxyyy06988
Slot 5:	WS-X5234-RJ45	– 24 port 10/100TX	xxxyyy06989

End-User Port Configuration:

Port	Name	Status	VLAN	Speed	MAC Address
2/1	User 63782	Connected	200	100-Full	00-01-02-bc-e2-2f
2/2	User 63783	Connected	200	100-Full	00-01-02-bc-ab-55
2/3	User 63784	Connected	200	100-Full	00-01-02-bc-6e-38
2/4	User 63785	Connected	200	100-Full	00-01-02-bc-2e-77
2/5	User 63786	Connected	200	100-Full	00-01-02-bc-0a-85
2/6	User 63787	Connected	200	100-Full	00-01-02-bc-4b-32
2/7	User 63788	Connected	200	100-Full	00-01-02-bc-cb-11
2/8	User 63789	Connected	200	100-Full	00-01-02-bc-ae-90
2/9		Disabled			None
2/10	User 63791	Connected	200	100-Full	00-01-02-bc-45-03

. . .

APPENDIX B REFERENCES

1. Craig J. LaCava. Corporate Security Policy for Network Infrastructure for The Company. 12-Jan-2000.

2. Sean Convery and Bernie Trudel, Cisco Systems. “SAFE: A Security Blueprint for Enterprise Networks.” URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm (10-Dec-2002).

3. Fraser, Barbara. “RFC 2196: Site Security Handbook.” IETF: September 1997.

4. Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons (1st Edition), 2000.

5. Cisco Systems. “Cisco Catalyst 5000 Series Switches”. URL: http://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_chapter09186a00800d9f17.html (10-Dec-2002).

APPENDIX C REFERENCES

1. Hochmuth, Phil. “Is VoIP Vulnerable?”. Network World Fusion. 24 June 2002. URL: http://www.nwfusion.com/news/2002/0624voip.html (24 January 2003).

2. Liebmann, Lenny. “Real World Voice Over IP Migation.” Business Communications Review. May 2001. URL: http://www.bcr.com/bcrmag/2001/05/p44.asp (23 January 2003).

3. Halpern, Jason – Cisco Systems. “SAFE: IP Telephony Security in Depth”. 30 July 2002. URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.htm (12 December 2002)

4. Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons (1st Edition), 2000.

5. Padjen, Robert et. al. Cisco AVVID and IP Telephony Design & Implementation. Rockland, Mass: Syngress Publishing, Inc., 2001.

6. Cox, Philip. “Hardening Windows 2000 – Version 1.0” System Experts 30 March 2001. URL: http://www.systemexperts.com/tutors/HardenW2K101.pdf (20 Jan 2003).