Global Information Assurance Certification Paper

VLAN Auditing: From An Auditors Perspective

GSNA Practical Version: 2.1 (amended July 5 2002)

Author: Ken Laurie

Date: February 2004

Table of Contents

List of Tables

List of Figures

Assignment 1 – Research in Audit, Measurement Practice and Control

Identify The System To Be Audited

I am auditing a VLAN as implemented on CISCO 3500 series routers running Cisco's Internetwork Operating System (IOS) version 12.1(12). The VLAN to be audited segments traffic between a number of environments with an emphasis being on separating the production and office environments. The VLAN is also used to add an extra layer of network security by reducing the exposure of the production environment to those in the office environment.

GIAC Enterprises is a small sized organisation of less than 250 staff operating 24 x 7 in a constant state of availability. The organisation has an office located in each of three cities, with these cities being located in three separate States. There is a computer centre located in each of the offices with two of the computer centres being a replica of each other. The two replicated sites work in a co-primary scenario as either one can be the primary site at any time. This co-primary scenario is vital to be able to provide the constant availability required by the customers. Customers connect to the organisation's network via a private network, which then gives them access to selected servers within a Demilitarised Zone (DMZ). The customers connect to the network from a Point of Presence (POP) located in the city closest to them and are then routed to the active site's servers.

Due to the nature of the organisation and the distributed environment of having multiple offices in multiple states, staff are required to move between these offices and continue to work without any disruption. The use of VLANs means that staff can move between the offices and continue to have access to all their network resources without any requirement to reconfigure. When moving to another office the staff member can connect their notebook to the network and are then connected to the correct VLAN that then provides them with the appropriate resources and network access.

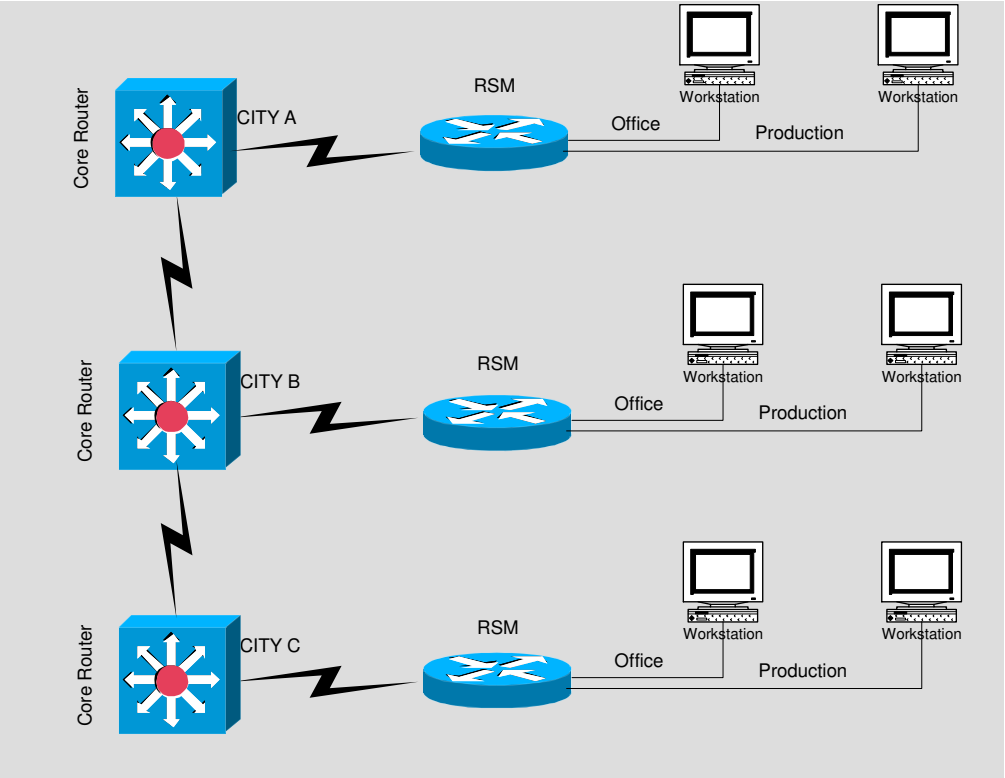


Figure 1: GIAC Enterprises VLAN Structure

Definitions of A VLAN:

Webopedia defines a VLAN as “Short for virtual LAN, a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.”

Whilst What Is defines a VLAN as “A virtual (or logical) LAN is a local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application). The virtual LAN controller can change or add workstations and manage load balancing and bandwidth allocation more easily than with a physical picture of the LAN. Network management software keeps track of relating the virtual picture of the local area network with the actual physical picture.”

Evaluate The Risk

There are risks associated with implementing and managing a VLAN environment. Many of these risks are similar to a standard LAN environment and the associated equipment, such as a router. As routers are used to define and manage the VLAN environment, many of the risks are actually associated with the routers.

What can go wrong	Likelihood	Consequences	Severity
Incorrect configuration allowing unauthorised traffic to flow between the VLANS.	High	The network is not working as designed. This may allow the general office PCs to gain access to the production environment resulting in the potential exposure of confidential data.	High
Not configured to comply with the documented requirements.	Medium	The environment is not working as designed and may cause issues when introducing new equipment.	Low
Configuration not applied at all sites concurrently	High	The high availability requirements of the environment mean that the environments at each site must be consistent so that in event of a failover to the other site and it becoming the primary site then VLAN's can be expected to consistent and not cause issues regarding access.	High
Vulnerability in the software	Medium	Potential exposure that could be used to disrupt the network.	High
Unnecessary rules	Medium	This could allow unauthorised traffic to flow between the VLAN's. Unnecessary rules also add extra difficulty to the management of the VLAN.	Medium
Unauthorised Administrator access to router	Medium	Ability to alter the router configuration and potentially compromise the network.	High
Inability to restore VLAN rule set after failure	Medium	Network outage, which would then be considered to be a Denial of Service to staff and/or customers.	High

Table 1: Risks to GIAC Enterprises VLAN structure

What Is The Current State Of Practice?

There is what I would classify as a reasonable amount of information available on the Internet and in publications that provide recommendations on how to secure a Cisco router, as well as some information available on how to audit a Cisco router. Unfortunately there is very little information on how to audit a VLAN as implemented on a Cisco router.

Some good starting points to assist with the reviewing of a VLAN are the ISO standard on Security Management (ISO 17799) and the recently published *The Standard of Good Practice for Information Security by the Information Security Forum (ISF)*.

The ISF standard states:

> "Computer networks can handle many types of traffic from a wide variety of sources. To manage network traffic effectively, network devices have to be configured correctly and particular types of network traffic denied access."[1]

The ISF standard prime principle for configuring network devices is:

> "Network devices should be configured to function as required, and to prevent unauthorised or incorrect updates." [1]

There are some very good papers on how to securely implement a VLAN on a Cisco router and are well worthwhile reading. The following documents are a good starting point for the configuring of a VLAN:

Cisco Systems Inc

"SAFE Enterprise Layer 2 Addendum"
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f.shtml

"Cisco – Securing Networks with Private VLANS and VLAN Access Control Lists"
http://www.cisco.com/warp/public/473/90.shtml

@stake

"Secure Use of VLANs: An @stake Security Assessment"
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf

qOrbit

"Catalyst Secure Template" http://www.qorbit.net/documents/catalyst-secure-template.htm

[1] ISF, "The Standard of Good Practice for Information Security", V4.0, March 2003, http://www.isfsecuritystandard.com/pdf/standard.pdf, (7 Nov 2003)

As I was not able to locate a concise audit plan that covered VLANs I used a combination of audit plans to create my own. The audit plans I used include those of auditing a CISCO router and auditing a LAN. As a VLAN is implemented within a router, then the auditing of a router became a basis for much of the audit plan.

Assignment 2 – Create An Audit Checklist

Introduction

GIAC Enterprises requested an audit be performed on their Office VLAN to ensure that those who connect to it don't have access to resources or information that they are not meant to, in particular, the Production VLAN and that the VLAN is configured to meet best practice recommendations.

The production VLAN contains information that is highly confidential and must not be accessible from the Office VLAN, except for the documented exceptions. The audit will be conducted with the Network Services staff performing the relevant commands in front of the auditor. Due to restrictions placed on the auditors by GIAC Management the audit will only take place at one site instead of at all sites.

Conventions Used:

- Commands to be executed during the audit are shown in **bold**. The commands are listed in the sequence that they must be executed to ensure correct results for the audit.
- The term (removed) indicates a section or a portion of the output deleted for purposes of brevity and/or security reasons.

Objectives

The objective of this audit is to certify the implementation of the Office VLAN is in accordance with the documented design.

The audit will determine if:

- The Office VLAN complies with the documented design and security requirements.
- The Office VLAN complies with the security policy of the organisation.
- The Office VLAN meets current best practices.
- There are any improvements that can be applied.

Scope

This audit is to concentrate on the office VLAN to ensure it only has documented access to the Production VLAN. This audit is to be performed from the Primary site only. This is only a VLAN audit not an audit of the routers; there are other papers covering auditing of routers, such as "Auditing Cisco Perimeter Routers" by Marvin Yee[2].

[2] Yee, Marvin, "Auditing Cisco Perimeter Routers", GSNA Practical Assignment, October 2001

Section A – Documentation

Audit Step 1	Security Policy for VLAN access
Control Objective	To determine whether a Security Policy is in place and that it has been effectively communicated to the organisation as well as the existence of policy and procedures for the deployment and use of VLAN technology.
Reference	ISO 17799[3]
Risk	No or inadequate policy in place could mean inconsistent deployment of VLANs and that the business objectives may not be met.
Compliance	The policy exists. Are there formal and/or informal procedures in place to support the policy? How is the policy communicated to the organisation?
Testing	Obtain a copy of the IT Security Policy to determine if there is a policy statement covering VLAN Deployment and Access or obtain a copy of a VLAN Access Security Policy to determine if one is present. Review documented procedures to determine if it supports the use of VLAN technology. Interview network staff to determine if there are any undocumented policy and procedures. Interview selected staff to determine if the policy has been effectively communicated.
Objective / Subjective	Subjective

Audit Step 2	VLAN Functional Documentation
Control Objective	To determine whether a VLAN Functional Document has been developed.
Reference	ISF[4], Original contribution
Risk	No document describing the functional requirements of the deployment of VLANs could mean a failure to meet business objectives.
Compliance	The VLAN Functional document exists and describes the functional requirements to meet the business objectives, which should be stated in the document. There Should be procedures in place to review this

[3] ISO/IEC 17799:2000 Information technology - Code of Practice for Information Security Management
[4] ISF, "The Standard of Good Practice for Information Security", V4.0, March 2003, http://www.isfsecuritystandard.com/pdf/standard.pdf, (7 Nov 2003)

	document to ensure it is updated to reflect changes in business objectives.
Testing	Obtain a copy of the VLAN Functional document to determine whether it describes the business requirements for implementing and deploying the VLANs. Determine if there are formal procedures in place to review and update the document. If there are no formal procedures, interview appropriate staff to determine if there are informal procedures in place to review and update the document.
Objective / Subjective	Subjective

Audit Step 3	VLAN Design Document
Control Objective	To determine whether a VLAN Design Document exists and effectively implements the functional requirements of the VLAN Functional Document.
Reference	ISF[5], Original contribution
Risk	No design document means the business objectives may not have been met when implementing the VLANs. The lack of a design document could mean that servers may be located in the wrong VLAN and incorrect protocols may be permitted to be transmitted between VLANs.
Compliance	The VLAN Design document exists and accurately reflects the functional requirements as documented in the VLAN Functional Document. The document should state what services are allocated to which VLANs as well as which protocols are permitted to flow between VLANs. Procedures should be in place to continually review the document and keep in line with the functional document.
Testing	Obtain a copy of the document and determine whether the design document effectively reflects the functional document. Review the design document to determine whether servers have been allocated to the correct VLAN. Review the design document to determine whether the flow of protocols have been restricted between VLANs. Determine if there are formal procedures in place to review and update the document.

[5] ISF, "The Standard of Good Practice for Information Security", V4.0, March 2003, http://www.isfsecuritystandard.com/pdf/standard.pdf, (7 Nov 2003)

	If there are no formal procedures, interview appropriate staff to determine if there are informal procedures in place to review and update the document.
Objective / Subjective	Subjective

Audit Step 4	IP Address range document
Control Objective	To determine that all used IP Address ranges are documented as to which VLAN they are assigned to and to ensure that address ranges are not assigned to multiple VLANs.
Reference	ISF[6], Original contribution
Risk	The potential to incorrectly place a device in the wrong VLAN is greatly heightened if the in use IP Address ranges are not fully documented and adhered to.
Compliance	This document ensures that all IP addresses are appropriately assigned, which environment the addresses belong to and which VLAN the address will become part of. There must be clear documentation on the IP address ranges being used and into which VLANs the addresses fall.
Testing	Ensure that all IP addresses are implemented in the ACLS. Ensure that each VLAN has its own unique range of addresses. Determine if there are formal procedures in place to review and update the document.
Objective / Subjective	Subjective

[6] ISF, "The Standard of Good Practice for Information Security", V4.0, March 2003, http://www.isfsecuritystandard.com/pdf/standard.pdf, (7 Nov 2003)

Section B – Administration

Audit Step 5	License and Support
Control Objective	The Operating System software for the switches that provide the VLAN technology must be properly licensed and covered under a technical support and software maintenance arrangement.
Reference	ISO 17799[7]
Risk	Unlicensed or improperly software may expose the organisation to legal issues. The ability to access critical patches or software updates may not be possible without proper licensing and support arrangements exposing the organisation known vulnerabilities.
Compliance	The software is registered and both the hardware and software are covered under a support agreement, which should take into account the business requirements.
Testing	View the licensing and maintenance documentation to ensure that they are applicable and valid.
Objective / Subjective	Subjective

Audit Step 6	VLAN ACLs
Control Objective	To ensure that the ACLs accurately reflect the requirements and design as documented.
Reference	Cisco[8] Original contribution
Risk	The ACLs do not reflect the business requirements and the VLANs are not configured as required. The ACLs will determine what protocols will flow between VLANs and which IP addresses have access to devices such as routers. Incorrect ACLs could mean that IP address in the Office VLAN may have inappropriate access to devices such as routers.
Compliance	The ACLs accurately reflect the documentation and thus the business requirements. This should include which protocols are permitted between VLANs as well as which servers can be accessed from the VLAN being audited. This should be performed at each site to ensure that all sites have been correctly configured.
Testing	Obtain the ACLS for the routers that define the VLANS.

[7] ISO/IEC 17799:2000 Information technology - Code of Practice for Information Security Management
[8] SAFE Enterprise Layer 2 Addendum

	Have the Network Administrator Telnet to the router and perform the following command. **sh acc** Ensure that all IP addresses documented in the IP Address document are implemented in the ACLS. Does the ACL match the definition documentation? Review both reports to determine whether they are the same and that they comply with the documentation. Use nmap to scan the VLAN address range, from the VLAN being audited, to determine if they match the requirements and / or the ACLs **Nmap –sS –O 10.xx.yy.0/24** where xx = 20 & 70, yy = 64, 76, 48 & 88. Compare the results from each site to determine whether the same rules have been implemented.
Objective / Subjective	Objective

Audit Step 7	Procedures to update VLAN configurations
Control Objective	To ensure that appropriate procedures are in place to prevent unauthorised updates to the VLAN configurations.
Reference	ISO 17799[9], Original contribution.
Risk	Unauthorised changes could compromise the VLANs with the potential to no longer meet the business objectives. Without appropriate procedures in place the risk of not effectively tracking all changes to the VLAN configuration is greatly increased. This could then result in the VLANs being compromised by incorrect updates. Backups may not be taken prior to changes being made. The change could then cause a failure without any means of recovery.
Compliance	Appropriate documentation is in place that documents the procedure(s) to be followed to update VLAN configurations. Review a selection of the changes and follow them through the process to ensure that the process has been followed correctly.
Testing	Requested the documented procedures for implementing changes to the VLAN configurations. This would include implementing a new VLAN. If formal documented procedures are not available then check for in-formal procedures.

[9] ISO/IEC 17799:2000 Information technology - Code of Practice for Information Security Management

	Is there a change control system that is used to manage changes to the VLAN configurations? Review the change control system for changes to the VLANs and select a sample to follow through to determine if procedures where followed.
Objective / Subjective	Subjective

Audit Step 8	VLAN Logging
Control Objective	To determine if there is any VLAN logging being performed on the router.
Reference	Yee[10]
Risk	Without an appropriate level of logging any unauthorised access or attempted access to the router(s) may not be detected. By not detecting unauthorised access attempts someone attempting to break-in to a router will have as much time as they require to exploit any vulnerabilities in the router.
Compliance	Logging has been enabled on the router and the log output has been directed to a server for collection and archival. A process is in place to review the logs.
Testing	Review whether logging has been enabled on the router by issuing the following command. Check the output from this command to determine which syslog servers the logs are being directed to. The IP address of the syslog servers should be displayed as part of the output from the sh logg command. Have the Network Administrator Telnet to the router and perform the following command. **sh logg** Review the procedures to determine whether the logs are archived. The logs should be archived to a non-changeable medium for long-term storage. Determine how long the logs are retained. Determine whether the logs are reviewed and how often.
Objective / Subjective	Objective

[10] Yee, Marvin, "Auditing Cisco Perimeter Routers", 26 October 2001, URL: http://www.giac.org/practical/Marvin_Yee_GSNA.zip, (Sept 2003)

Audit Step 9	Availability and Recovery
Control Objective	A high availability and recovery must be in place to prevent loss of VLANs.
Reference	ISO 17799[11]
Risk	If one or more of the VLANs fail then the business objectives may not be met. Users may not have access to their data and there may be resultant loss in productivity.
Compliance	There are procedures in place to ensure the availability of the VLANs whilst performing updates to the configuration. The procedures must fully document the processes in place to ensure the availability of the VLANs whilst changes are being made.
Testing	Copies of the VLAN configuration files must be kept as a backup prior to changes being made. Previous copies of the configuration files should be kept for the purpose of tracking the change history. Determine if there are other means of restoring or re-creating the configuration files, such as: • Can the VLAN configuration files be recreated by means other than a backup? • Can they be taken from another site with nil or minimal changes? Follow a change though the process to determine whether backups are actually performed etc. You may have to create a 'test' change to follow.
Objective / Subjective	Subjective

Audit Step 10	Operating System and Patch levels
Control Objective	The Operating System for the switches should be at the latest level and all appropriate patches should have been applied.
Reference	ISO 17799[11], Cisco
Risk	Unpatched or outdated software are classic areas of attack by those wanting to break into or disrupt a network. There is a high risk of exploitation of unpatched routers.
Compliance	Check the Operating System level and patches available for the devices to determine if it is at the latest level available.

[11] ISO/IEC 17799:2000 Information technology - Code of Practice for Information Security Management

	Procedure should be in place to ensure that the Operating System software is kept up to date.
Testing	Review the Operating System and patch levels to determine if it is at the latest level. Have the Network Administrator Telnet to the router and perform the following command. **sh ver** The following command should be performed from a VLAN that has access to the management ports on the router. **Nmap –sS –PT –PI –O –v –T IP-address** Determine whether there is a designated person who is responsible for receiving and/or reviewing patches from the vendor. Determine whether there is a procedure in place to test patches prior to being placed into production.
Objective / Subjective	Objective

Audit Step 11	Accountability
Control Objective	All devices connecting to the VLANs must be identified by their MAC address.
Reference	ISO 17799[12], Gill[13]
Risk	Devices must not be permitted to be connected to the network (VLAN) without the proper authorisation. A potential attacker could gain access to the network by physically connecting a PC to the network.
Compliance	A MAC address register must be maintained for authorised MAC addresses and non-registered MAC address must be prevented from gaining access to the network.
Testing	MAC addresses should be kept in a register with the details of the "owner" clearly identified. Unregistered MAC addresses must be prevented from connecting to the network (VLAN) Connect a PC that contains an unregistered MAC address, to the network and determine, by issuing the IPCONFIG command, whether an IP address has been assigned. **Ipconfig /all** Review the syslog to determine if the unidentified MAC address has been logged when attempting to connect to a

[12] ISO/IEC 17799:2000 Information technology - Code of Practice for Information Security Management
[13] Gill, Stephen, "Catalyst Secure Template", qOrbit Technologies, version 1.21, 14 November 2002

	VLAN. Obtain a copy of any reports for review to determine if they address the unidentified MAC addresses connecting to the network.
Objective / Subjective	Objective

Audit Step 12	VLAN Administration
Control Objective	A designated person(s) should be totally responsible for administrating the VLANs.
Reference	ISO 17799[14] , ISF[15]
Risk	Multiple people administering the VLANs could result in changes being made that are not consistent with the business objectives. When more than one individual is responsible for making changes to the VLAN, there is an increase in the potential for changes to be inadvertently backed out or overridden.
Compliance	Documented procedures on how to update and manage VMPS. Documented procedures on who is responsible for administering the VLANs.
Testing	Review the procedures relating to administering and updating VMPS. Review the procedures for applying changes across multiple sites and determine if they are applied in the same manner. Determine whether there an individual responsible for VLAN administration or multiple individuals. If there is more than one person responsible, determine how they manage the processes. Determine whether there is a backup person in case the primary person is unavailable. Determine if the procedure is being followed: • Using a 'test' case, create a change to add a MAC address to the VLAN. • Use this to determine if the MAC address was added into the correct VLAN.
Objective / Subjective	Subjective

[14] ISO/IEC 17799:2000 Information technology - Code of Practice for Information Security Management
[15] ISF, "The Standard of Good Practice for Information Security", V4.0, March 2003, http://www.isfsecuritystandard.com/pdf/standard.pdf, (7 Nov 2003)

Section C - Configuration

Audit Step 13	VLAN Configuration
Control Objective	The VLANs need to be configured to basic recommendations to ensure they comply with a minimal level of security.
Reference	Cisco[16] @stake[17], Wagner[18], Gill[19]
Risk	Basic security configuration of the VLANs and the routers need to be implemented to prevent the circumvention of the VLANs.
Compliance	The basic configuration should comply with the recommendations of Cisco and @stake: • Use a dedicated VLAN for trunk ports. • Only use VLAN 1 for trusted networks and necessary management traffic. • Set user ports to non-trunking mode. • Use spanning tree and other dynamic protocols to prevent denial of service attacks.
Testing	Is a dedicated VLAN ID used for all trunk ports? Have the Network Administrator Telnet to the router and perform the following command. **Show config** Is VLAN 1 being used for network management? VLAN 1 should only be used for trusted networks and necessary management traffic. Have all user ports been set to non-trunking mode? To prevent potential denial of service attacks and other exploitation has the switch been locked down by using spanning tree and other dynamic protocols. **Show run**
Objective / Subjective	Objective

Audit Step 14	IP permit lists for management ports
Control Objective	To reduce the exposure of the router to exploitation of the management ports by allowing only specific IP addresses to access these ports

[16] SAFE Enterprise Layer 2 Addendum
[17] Secure Use of VLANS: An @stake Security Assessment
[18] Wagner, Richard, "Securing Network Infrastructure and Switched Networks", SANS Reading Room, 21 August 2001
[19] Gill, Stephen, "Catalyst Secure Template", qOrbit Technologies, version 1.21, 14 November 2002

Reference	Cisco[16] @stake[17], Wagner[18], Gill[19]
Risk	By allowing any IP address to have access to any of the management ports an attacker can use these management ports to gain access to the router configuration.
Compliance	Inability to gain access to management ports from the VLAN being audited. There should be no access to SNMP from the VLAN being audited.
Testing	Check the router configuration to determine if there are access lists for the management ports being used for the VLAN being audited. Have the Network Administrator Telnet to the router and perform the following command. **show access-lists <vlan>** To check that the management ports are not accessible from the office VLAN. **Use Getif to scan for SNMP from the Office VLAN.**
Objective / Subjective	Objective

Audit Step 15	SNMP version and treatment of community strings
Control Objective	To determine whether SNMP is being used to manage the routers, the version of SNMP being used and to ensure that the community strings are treated as if they are root or administrator passwords.
Reference	Cisco[20] @stake[21], Wagner[22], Gill[23]
Risk	The use of SNMP as a management tool could potentially reveal information to an attacker that should be kept private. Note that even if the community strings are treated as root or administrator passwords the community strings are transmitted in plain text format across the network.
Testing	Is SNMPv3 being used and are the community strings treated like root or administrator passwords? Have the Network Administrator Telnet to the router and perform the following command. **Show SNMP group** The following should be performed from a VLAN that has

[20] SAFE Enterprise Layer 2 Addendum
[21] Secure Use of VLANS: An @stake Security Assessment
[22] Wagner, Richard, "Securing Network Infrastructure and Switched Networks", SANS Reading Room, 21 August 2001
[23] Gill, Stephen, "Catalyst Secure Template", qOrbit Technologies, version 1.21, 14 November 2002

	access to the management ports on the router. **Use Getif to scan for SNMP: Read community string of public and Write community string of private** **Use Getif to scan for SNMP: Read community string as defined.**
Objective / Subjective	Objective

Audit Step 16	Cisco Discovery Protocol
Control Objective	The use of CDP should only be used where appropriate for network management.
Reference	Cisco[24] @stake[25], Wagner[26], Gill[27]
Risk	Cisco Discovery Protocol allows Cisco devices to identify themselves to other Cisco devices. This information is transmitted in clear text format and is unauthenticated. An attacker could potentially map the environment and identify the Cisco devices on the network. This could then enable the attacker to determine what potential vulnerabilities exist within the network.
Testing	Is the Cisco Discovery Protocol (CDP) being used on the VLAN being audited? Have the Network Administrator Telnet to the router and perform the following command. **Show CDP** The following should be performed from a VLAN that has access to the management ports on the router. **Use Getif to show if CDP active**
Objective / Subjective	Objective

Audit Step 17	Port security
Control Objective	Ports should be configured to associate a limited number of MAC addresses to each port.
Reference	Cisco[24] @stake[25], Gill[27]
Risk	Without port security and the limiting of the number of MAC addresses that can connect to a port there is the potential

[24] SAFE Enterprise Layer 2 Addendum
[25] Secure Use of VLANS: An @stake Security Assessment
[26] Wagner, Richard, "Securing Network Infrastructure and Switched Networks", SANS Reading Room, 21 August 2001
[27] Gill, Stephen, "Catalyst Secure Template", qOrbit Technologies, version 1.21, 14 November 2002

	for MAC address flooding and other associated network attacks.
Testing	Determine if port security has been configured for user ports? Are ports configured to associate a limited number of MAC addresses that can connect to them? **Show config** Connect a pc using a registered MAC address to a port and perform an **ipconfig /all** Connect another pc or the same pc with a different NIC and hence different registered MAC address to the same port and perform an **ipconfig /all**
Objective / Subjective	Objective

Audit Step 18	Disable unused ports
Control Objective	To prevent a network intruder from physically being able to use an unused port to gain access to the network.
Reference	Cisco[28] @stake[29], Gill[30]
Risk	Allowing unused ports to be left available could enable a network intruder to physically plug into the unused port and to start to communicate with the rest of the network.
Testing	Determine if unused ports are disabled and put in an unused VLAN. Connect a PC with a registered MAC address to an unused port. Perform an ipconfig to determine if a valid IP address has been assigned. **Ipconfig /all**
Objective / Subjective	Objective

Audit Step 19	Physical access to switches
Control Objective	To prevent unauthorised physical access to the switches.
Reference	ISO 17799[31]
Risk	By gaining physical access to the switches a person could gain access to the network by re-cabling and directly connecting to the console port of the router.

[28] SAFE Enterprise Layer 2 Addendum
[29] Secure Use of VLANS: An @stake Security Assessment
[30] Gill, Stephen, "Catalyst Secure Template", qOrbit Technologies, version 1.21, 14 November 2002
[31] ISO/IEC 17799:2000 Information technology - Code of Practice for Information Security Management

Compliance	The switches should be located in areas of high security that prevents unauthorised physical access to the switches.
Testing	Determine whether the routers locked in appropriate cabling cabinets. Obtain a list of who has access to the switches. Review the list to determine whether all those on the list have the appropriate authorisation to have access to the routers or cabling cabinets.
Objective / Subjective	Objective

Audit Step 20	Logical access to the routers
Control Objective	To prevent unauthorised logical access to the routers.
Reference	ISO 17799[32]
Risk	If unauthorised access to a router is gained then the router could be reconfigured such that the VLANs no longer comply with the business objectives. Router traffic could be re-directed to other locations. The configuration could be altered to allow access to other parts of the network.
Compliance	Only authorised staff should be able to gain access to the routers and all services that are not required should be disabled.
Testing	Determine the protocols that are used to access the routers. Interview staff and get them to demonstrate how they gain access to the routers. Determine who has access to the routers. Have the Network Administrator Telnet to the router and perform the following command. **Show config** How is access to the routers controlled? Determine if cleartext management protocols, such as TELNET and SNMP are used. The following should be performed from a VLAN that has access to the management ports on the router. **telnet IP-address** Determine if unnecessary services have been disabled. Have the Network Administrator Telnet to the router and perform the following command to list the running process.

[32] ISO/IEC 17799:2000 Information technology - Code of Practice for Information Security Management

	Show proc cpu The following should be performed from a VLAN that has access to the management ports on the router. Check for TCP services: **Nmap –sS –PT –Pl –T 3 ipaddress** Check for UDP services: **Nmap –sU –PT –Pl –T 3 ipaddress**
Objective / Subjective	Objective

Assignment 3 – Audit Evidence

Conduct The Audit

Audit Step 1	Security Policy for VLAN access
Control Objective	To determine whether a Security Policy is in place and that it has been effectively communicated to the organisation as well as the existence of policy and procedures for the deployment and use of VLAN technology.
Testing	Obtain a copy of the IT Security Policy to determine if there is a policy statement covering VLAN Deployment and Access or obtain a copy of a VLAN Access Security Policy to determine if one is present. Review documented procedures to determine if it supports the use of VLAN technology. Interview network staff to determine if there are any undocumented policy and procedures. Interview selected staff to determine if the policy has been effectively communicated.
Findings Fail	Even though the Security Policy was being written in accordance with ISO 17799 and covered many areas of IT security, including network access, it did not cover VLAN deployment and access. This does not provide a clear direction for network staff on who can authorise connection to high privilege VLANs and under what circumstances. There is an informal policy in place that the Network Section uses to determine who and what is placed in each VLAN. To gain access to other than the Office VLAN an email from a Head of Department is required for authorisation. Documented procedures used by the Network Section support the use of VLAN technology. • VLAN Trunk Changes • Adding A New VLAN And Routing To The VLAN • Changing Dynamic VLAN Database-v05 • Implementing Access Lists For VLANs • Changing A VLAN Name

Audit Step 6	VLAN ACLs
Control Objective	To ensure that the ACLs accurately reflect the requirements and design as documented.
Testing	Obtain the ACLS for the routers that define the VLANS from the Administrator.

	Have the Network Administrator Telnet to the router and perform the following command. **sh acc** Ensure that all IP addresses documented in the IP Address document are implemented in the ACLS. Does the ACL match the definition documentation? Review both reports to determine whether they are the same and that they comply with the documentation. Use nmap to scan the VLAN address range, from the VLAN being audited, to determine if they match the requirements and / or the ACLs. **Nmap -sS -PT -PI -O -T 3 10.xx.yy.0/24** where xx = 20 & 70, yy = 64, 76, 48 & 88. Compare the results from each site to determine whether the same rules have been implemented.
Findings Pass	Source code for VLAN definition: ! ! 8 - Common ! ~~~~~~~~~~~~~~~~ ! Last change ! - who User ! - what Change control number ! ! Remove access-group from RSM interface int vlan 8 no ip access-group Common in exit ! ! delete old access-list no ip access-list extended Common !add new access-list ip access-list extended Common ! ! ** VERSION - yyyymmdd.ver ** ! ~~~~~~~~~~~~~~~~~~~~ remark Common Version:- 20031002.1 ! ** Admin Zone ** ! ~~~~~~~~~~ ! - Servers & Printers permit ip 10.0.8.0 0.127.1.255 10.0.28.0 0.127.0.255 ! - Workstations (limit back connections) permit tcp any 10.0.28.0 0.127.0.255 gt 1023

```
 permit udp any range netbios-ns netbios-dgm 10.0.28.0 0.127.0.255 range
netbios-ns netbios-dgm
 permit icmp any 10.0.28.0 0.127.0.255 echo-reply
 !  - Internal NAT
 permit ip 10.0.11.0 0.127.0.255 10.0.28.0 0.127.0.255
 !  - PCAnywhere from Admin
 permit udp any eq 5632 10.0.28.0 0.127.0.255 gt 1023
 permit tcp any eq 5631 10.0.28.0 0.127.0.255 gt 1023

 ! ** ALLOW DHCP (before deny's below) **
 !    ~~~~~~~~~~
 permit udp 10.0.8.100 0.127.0.0 eq bootps any eq bootps

 ! ** General Zone **
 !    ~~~~~~~~~~~~
 !  - Deny TCP & UDP Access to Routers
 !    - VLANs 1 - 7
 !deny ip 10.0.8.0 0.127.3.255 10.0.0.0 0.127.7.3
 !    - VLANs 8
 !deny ip 10.0.8.0 0.127.3.255 10.0.8.0 0.127.0.3
 !    - VLANs 16 - 31
 !deny ip 10.0.8.0 0.127.3.255 10.0.16.0 0.127.15.3
 !    - VLANs 32 - 63
 deny ip 10.0.8.0 0.127.3.255 10.0.32.0 0.127.31.3
 !    - VLANs 64 - 127
 deny ip 10.0.8.0 0.127.3.255 10.0.64.0 0.127.63.3
 !    - VLANs 128 - 255
 deny ip 10.0.8.0 0.127.3.255 10.0.128.0 0.127.127.3
 !    - VLANs 500 - 501
 deny ip 10.0.8.0 0.127.3.255 10.254.0.0 0.0.255.255
 !    - VLANs 602 & 701
 deny ip 10.0.8.0 0.127.3.255 xxx.xxx.0.0 0.0.255.3
 !    - VLAN 900
 deny ip 10.0.8.0 0.127.3.255 xxx.xxx.211.0 0.0.0.3
 deny ip 10.0.8.0 0.127.3.255 xxx.xxx.212.0 0.0.0.3
 deny ip 10.0.8.0 0.127.3.255 xxx.xxx.213.0 0.0.0.3
 !
 !    - NTP for RSM
 permit udp 10.0.8.20 0.127.0.0 eq ntp 10.0.8.0 0.127.0.3 eq ntp
 !
 ! - other Commom VLANs
 permit ip any 10.0.8.0 0.127.3.255

 ! ** Power User Zone **
 !    ~~~~~~~~~~~~~~~
 !  - Servers & Printers
 permit ip 10.0.8.0 0.127.0.255 10.0.16.0 0.127.0.255
 !  - Workstations (limit back connections)
```

```
 permit tcp any 10.0.16.0 0.127.0.255 gt 1023
 permit udp any range netbios-ns netbios-dgm 10.0.16.0 0.127.0.255 range
netbios-ns netbios-dgm
 permit icmp any 10.0.16.0 0.127.0.255 echo-reply
 !  - Internal NAT
 permit ip 10.0.11.0 0.127.0.255 10.0.16.0 0.127.0.255
 !  - PCAnywhere from Power User
 permit udp any eq 5632 10.0.16.0 0.127.0.255 gt 1023
 permit tcp any eq 5631 10.0.16.0 0.127.0.255 gt 1023

 ! ** Test Zone **
 !   ~~~~~~~~~
 !  - VLAN A
 permit ip any 10.0.108.0 0.127.0.255
 !  - VLAN B
 permit ip any 10.0.104.0 0.127.0.255
 !  - VLAN C
 permit ip any 10.0.96.0 0.127.0.255
 !  - VLAN D
 permit ip any 10.0.253.0 0.127.0.255

 ! ** Management Module Zone plus other Management  **
 !   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
 !  - Management Module VLAN
 permit ip any 10.0.4.0 0.127.0.255
 !  -
 permit ip any xxx.xxx.213.0 0.0.0.255
 !  -
 permit ip xxx.xxx.213.0 0.0.0.255 10.0.254.0 0.127.0.3
 !  -
 permit ip any 10.0.1.0 0.127.0.255

 ! ** DMZ Zone **
 !   ~~~~~~~~~~~~~~~
 permit ip any xxx.xxx.121.0 0.0.0.255
 permit ip any xxx.xxx.131.0 0.0.0.255
 permit ip any xxx.xxx.171.0 0.0.0.255

 ! ** Internet DMZ Zone **
 !   ~~~~~~~~~~~~~~~~~
 !  - Internet Proxy & Mail server
 permit ip any 10.0.3.64 0.127.0.63
 !
 !  - Proxy on Internet Inside DMZ
 permit ip any xxx.xxx.124.0 0.0.0.255
 permit ip any xxx.xxx.134.0 0.0.0.255
 permit ip any xxx.xxx.174.0 0.0.0.255
(removed)
```

!

! ** The following lines are manually entered after you have confirmed the ACL loaded correctly **

int vlan 8

ip access-group Common in

exit

!

end

Output from the switch:

sh access-lists Common

Extended IP access list Common

permit ip 10.0.8.0 0.127.1.255 10.0.28.0 0.127.0.255 (23862 matches)

permit tcp any 10.0.28.0 0.127.0.255 gt 1023 (24965 matches)

permit udp any range netbios-ns netbios-dgm 10.0.28.0 0.127.0.255 range netbios-ns netbios-dgm

permit icmp any 10.0.28.0 0.127.0.255 echo-reply (3 matches)

permit ip 10.0.11.0 0.127.0.255 10.0.28.0 0.127.0.255 (47 matches)

permit udp any eq 5632 10.0.28.0 0.127.0.255 gt 1023 (3 matches)

permit tcp any eq 5631 10.0.28.0 0.127.0.255 gt 1023

permit udp 10.0.8.100 0.127.0.0 eq bootps any eq bootps (152 matches)

deny ip 10.0.8.0 0.127.3.255 10.0.32.0 0.127.31.3

deny ip 10.0.8.0 0.127.3.255 10.0.64.0 0.127.63.3

deny ip 10.0.8.0 0.127.3.255 10.0.128.0 0.127.127.3

deny ip 10.0.8.0 0.127.3.255 10.254.0.0 0.0.255.255

deny ip 10.0.8.0 0.127.3.255 xxx.xxx.0.0 0.0.255.3 (196 matches)

deny ip 10.0.8.0 0.127.3.255 xxx.xxx.211.0 0.0.0.3

deny ip 10.0.8.0 0.127.3.255 xxx.xxx.212.0 0.0.0.3

deny ip 10.0.8.0 0.127.3.255 xxx.xxx.213.0 0.0.0.3

permit udp 10.0.8.20 0.127.0.0 eq ntp 10.0.8.0 0.127.0.3 eq ntp

permit ip any 10.0.8.0 0.127.3.255 (33359 matches)

permit ip 10.0.8.0 0.127.0.255 10.0.16.0 0.127.0.255 (19476 matches)

permit tcp any 10.0.16.0 0.127.0.255 gt 1023 (74 matches)

permit udp any range netbios-ns netbios-dgm 10.0.16.0 0.127.0.255 range netbios-ns netbios-dgm (2 matches)

permit icmp any 10.0.16.0 0.127.0.255 echo-reply

permit ip 10.0.11.0 0.127.0.255 10.0.16.0 0.127.0.255

permit udp any eq 5632 10.0.16.0 0.127.0.255 gt 1023

permit tcp any eq 5631 10.0.16.0 0.127.0.255 gt 1023

permit ip any 10.0.108.0 0.127.0.255 (588 matches)

permit ip any 10.0.104.0 0.127.0.255 (9019 matches)

permit ip any 10.0.96.0 0.127.0.255 (972 matches)

permit ip any 10.0.253.0 0.127.0.255 (40 matches)

permit ip any 10.0.4.0 0.127.0.255 (504 matches)

permit ip any xxx.xxx.213.0 0.0.0.255 (893 matches)

permit ip xxx.xxx.213.0 0.0.0.255 10.0.254.0 0.127.0.3

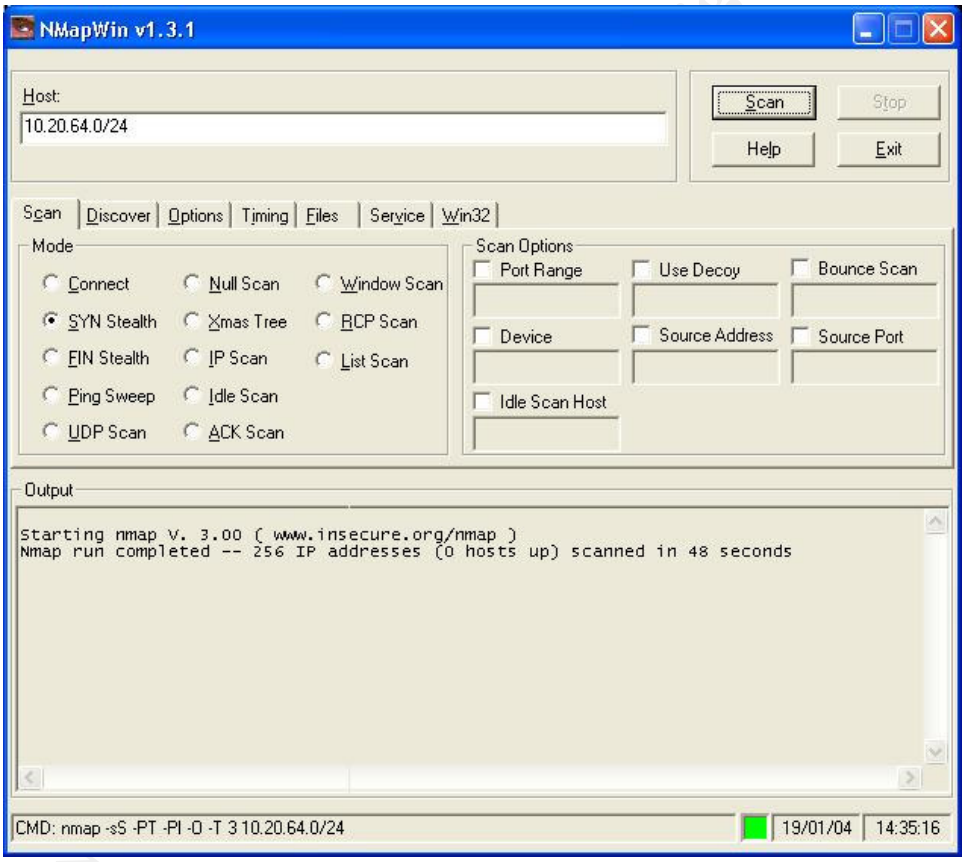
permit ip any 10.0.1.0 0.127.0.255 (245 matches)

permit ip any xxx.xxx.121.0 0.0.0.255 (582 matches)

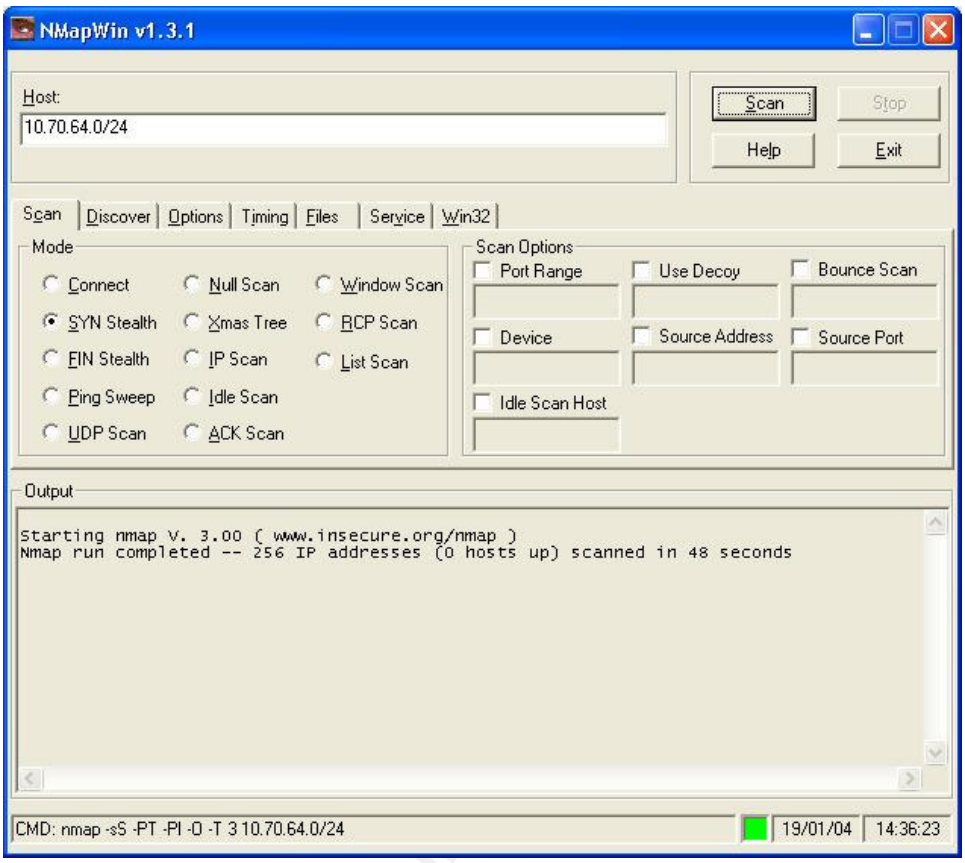
permit ip any xxx.xxx.131.0 0.0.0.255
permit ip any xxx.xxx.171.0 0.0.0.255 (93 matches)
permit ip any 10.0.3.64 0.127.0.63 (271 matches)
permit ip any xxx.xxx.124.0 0.0.0.255 (1323 matches)
permit ip any xxx.xxx.134.0 0.0.0.255
permit ip any xxx.xxx.174.0 0.0.0.255 (114 matches)
(removed)
#

Scan results from Office VLAN against Production VLAN (according to the documentation the Office VLAN should have no access to the Production VLAN):

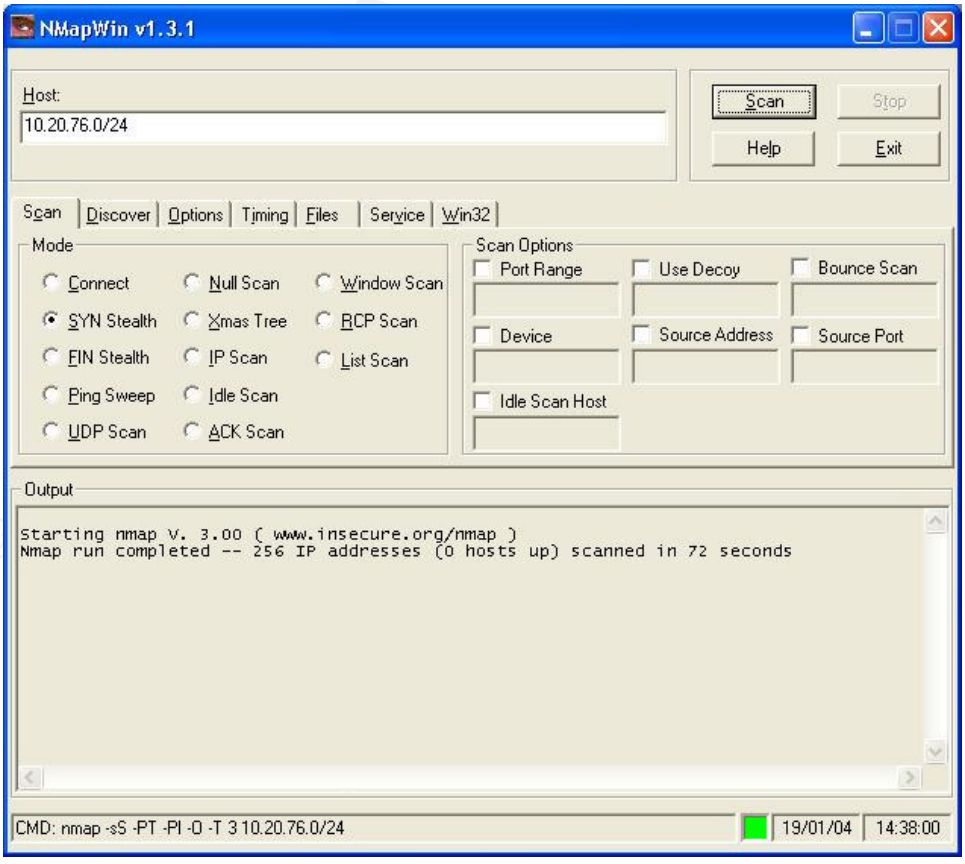
Nmap -sS -PT -PI -O -T 3 10.20.64.0/24



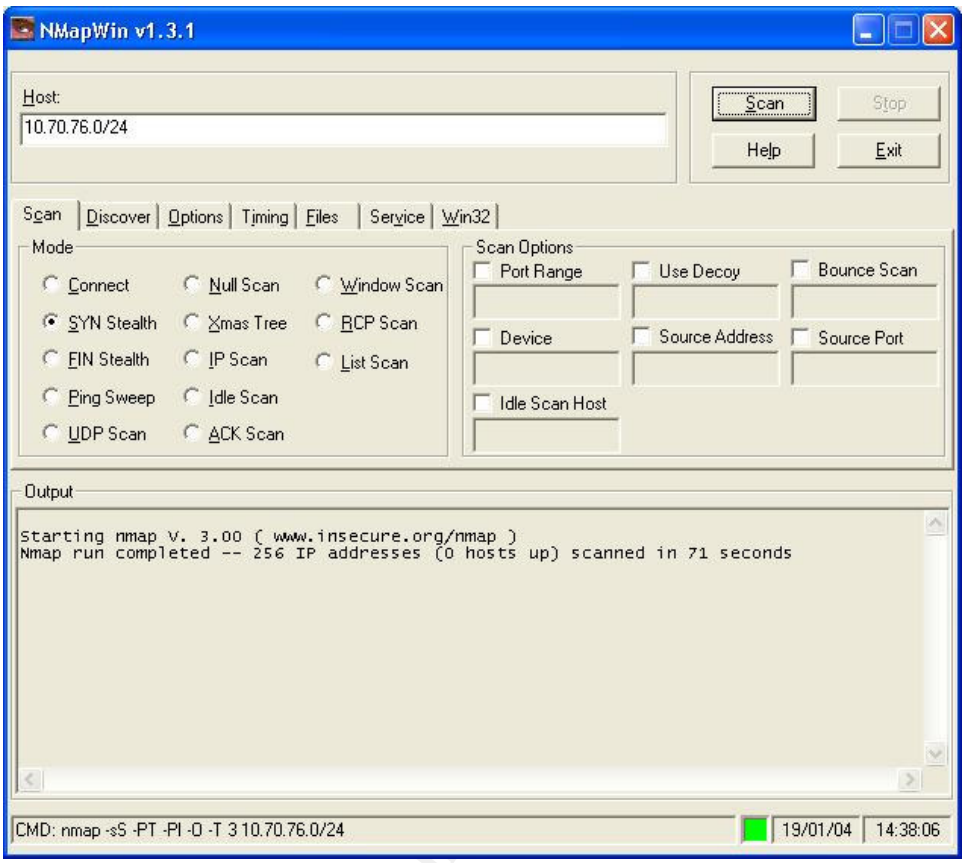
Nmap -sS -PT -PI -O -T 3 10.70.64.0/24



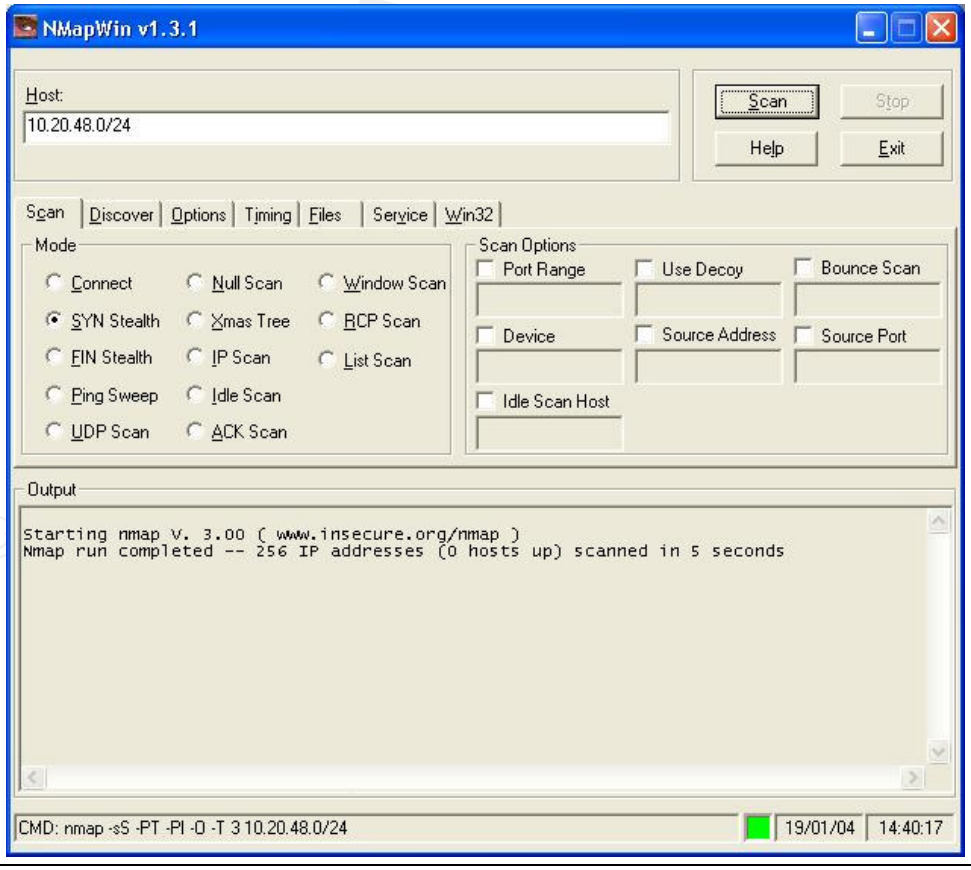
Nmap -sS -PT -PI -O -T 3 10.20.76.0/24



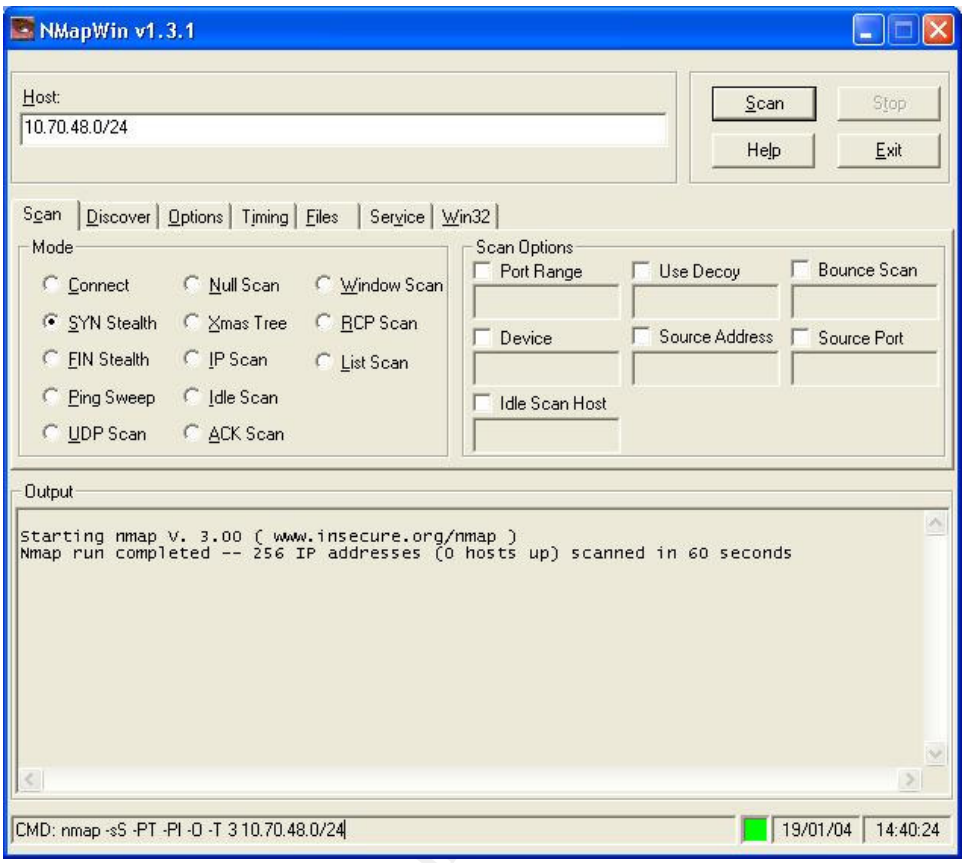
Nmap -sS -PT -PI -O -T 3 10.70.76.0/24



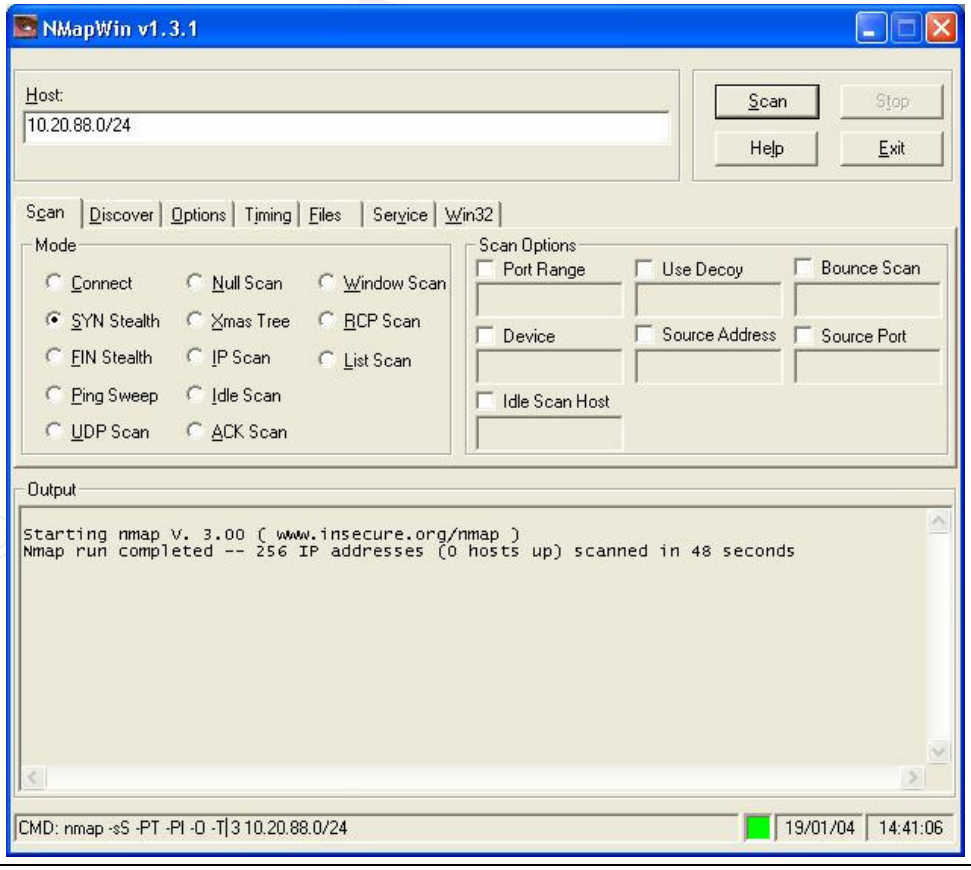
Nmap -sS -PT -PI -O -T 3 10.20.48.0/24

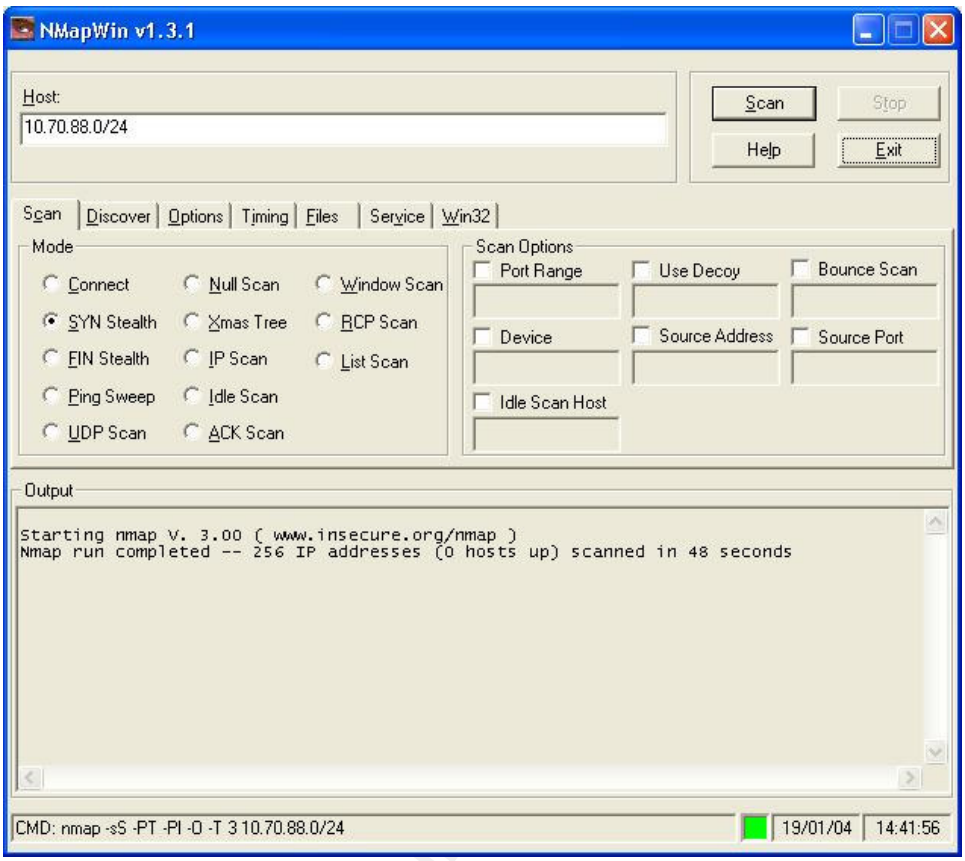


Nmap -sS -PT -PI -O -T 3 10.70.48.0/24



Nmap -sS -PT -PI -O -T 3 10.20.88.0/24



	Nmap -sS -PT -PI -O -T 3 10.70.88.0/24  Ideally the scanning should be performed at each site to ensure that all sites comply. Due to constraints on travel the scanning was performed at the Primary site only.

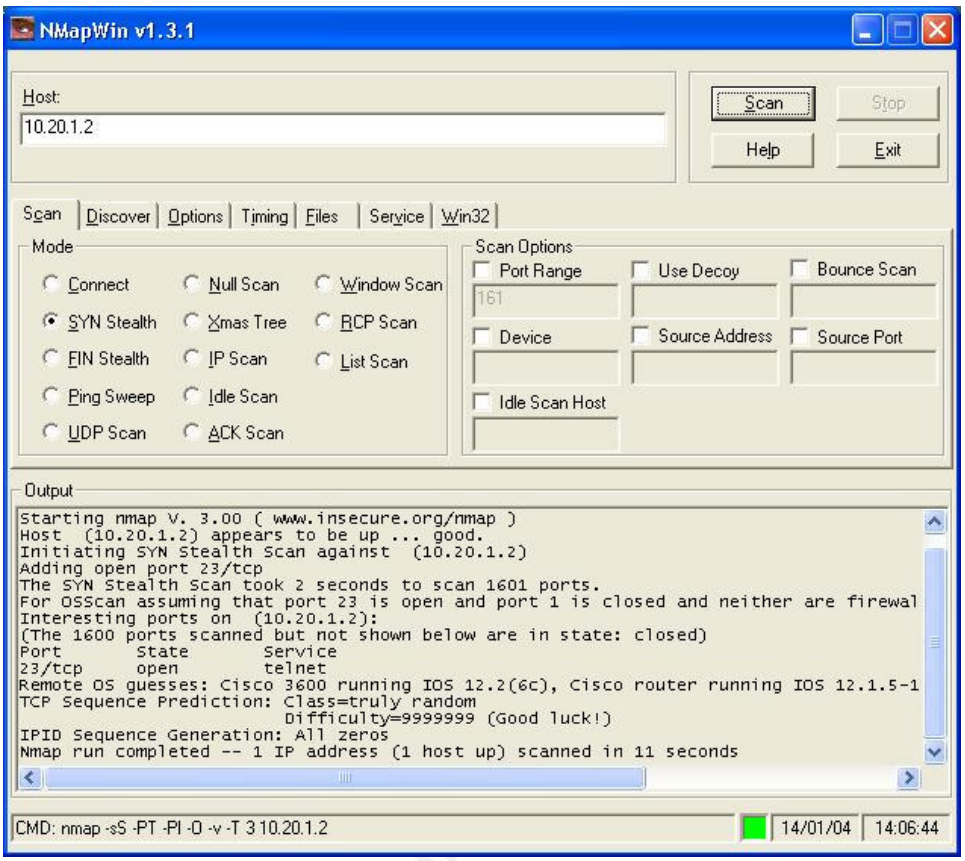
Audit Step 7	Procedures to update VLAN configurations
Control Objective	To ensure that appropriate procedures are in place to prevent unauthorised updates to the VLAN configurations.
Testing	Requested the documented procedures for implementing changes to the VLAN configurations. This would include implementing a new VLAN. If formal documented procedures is not available then check for non-formal procedures. Is there a change control system that is used to manage changes to the VLAN configurations? Review the change control system for changes to the VLANs and select a sample to follow through to determine if procedures where followed.
Findings	Formal documented procedures are available and are used to implement changes to VLAN configurations. The documented

Pass	procedures that cover the configuration of VLANs are: • VLAN Trunk Changes • Adding A New VLAN And Routing To The VLAN • Changing Dynamic VLAN Database-v05 • Implementing Access Lists For VLANs • Changing A VLAN Name The changes being made to the VLANs are documented in the change management system. Reviewed change numbers 6008, 6126, and 6679 for compliance with the procedures. These changes included adding a new VLAN and modifying an access list. Following the process it was determined that the changes were made in accordance with the documented procedures.

Audit Step 10	Operating System and Patch levels
Control Objective	The Operating System for the switches should be at the latest level and all appropriate patches should have been applied.
Testing	Review the Operating System and patch levels to determine if it is at the latest level. Have the Network Administrator Telnet to the router and perform the following. **sh ver** The following command should be performed from a VLAN that has access to the management ports on the router. **Nmap –sS –PT –PI –O –v –T IP-address** Determine whether there is a designated person who is responsible for receiving and/or reviewing patches from the vendor. Determine whether there is a procedure in place to test patches prior to being placed into production.
Findings Pass	OS and patch level: >**sh ver** Cisco Internetwork Operating System Software IOS (tm) C5RSM Software (C5RSM-ISV-M), Version 12.1(12), RELEASE SOFTWARE (fc1) Copyright (c) 1986-2001 by cisco Systems, Inc. Compiled Tue 27-Nov-01 03:17 by kellythw Image text-base: 0x60010958, data-base: 0x60E92000 ROM: System Bootstrap, Version 11.2(17523) [mohsen 102], INTERIM SOFTWARE BOOTLDR: C5RSM Software (C5RSM-BOOT-M), Version 11.2(18)P, RELEASE

	SOFTWARE (fc1) xxxxxxxx uptime is 5 weeks, 2 days, 4 minutes System returned to ROM by reload at 09:55:51 AEST Fri Sep 12 2003 System restarted at 14:01:32 AEST Mon Sep 15 2003 System image file is "slot0:c5rsm-isv-mz.121-12.bin" cisco RSP2 (R4700) processor with 32768K/2072K bytes of memory. R4700 CPU at 100Mhz, Implementation 33, Rev 1.0 Last reset from power-on G.703/E1 software, Version 1.0. G.703/JT2 software, Version 1.0. X.25 software, Version 3.0.0. Bridging software. 1 C5IP controller (26 Vlan). 26 Virtual Ethernet/IEEE 802.3 interface(s) 123K bytes of non-volatile configuration memory. 16384K bytes of Flash PCMCIA card at slot 0 (Sector size 128K). 8192K bytes of Flash internal SIMM (Sector size 256K). Configuration register is 0x2102

Nmap –sS –PT –PI –O –v –T 10.20.1.2

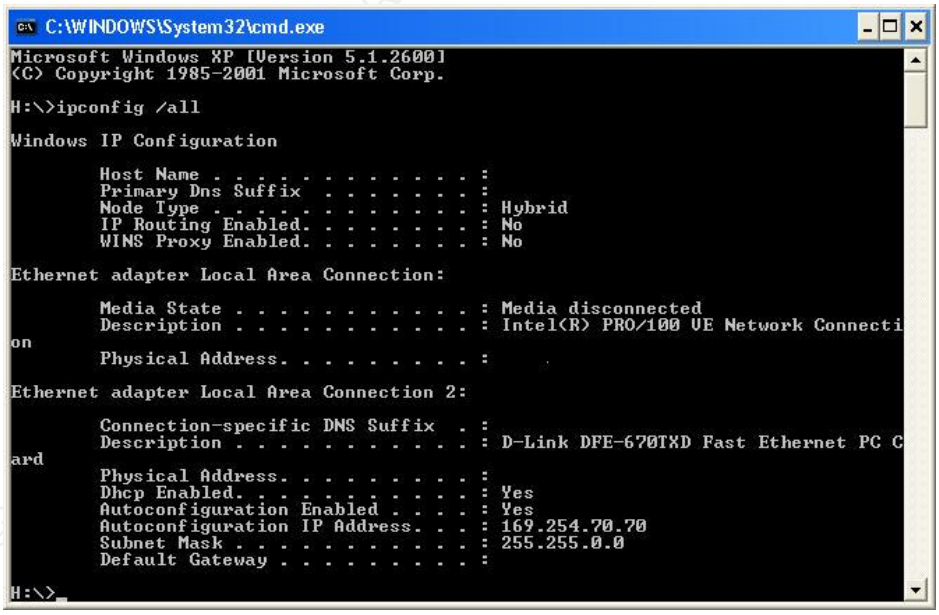


An individual is assigned the task of receiving and/or reviewing patches from the vendor. The individual responsible for this task is changed on a regular basis to enable all members of the team to perform the task and be capable of providing a backup for one another.

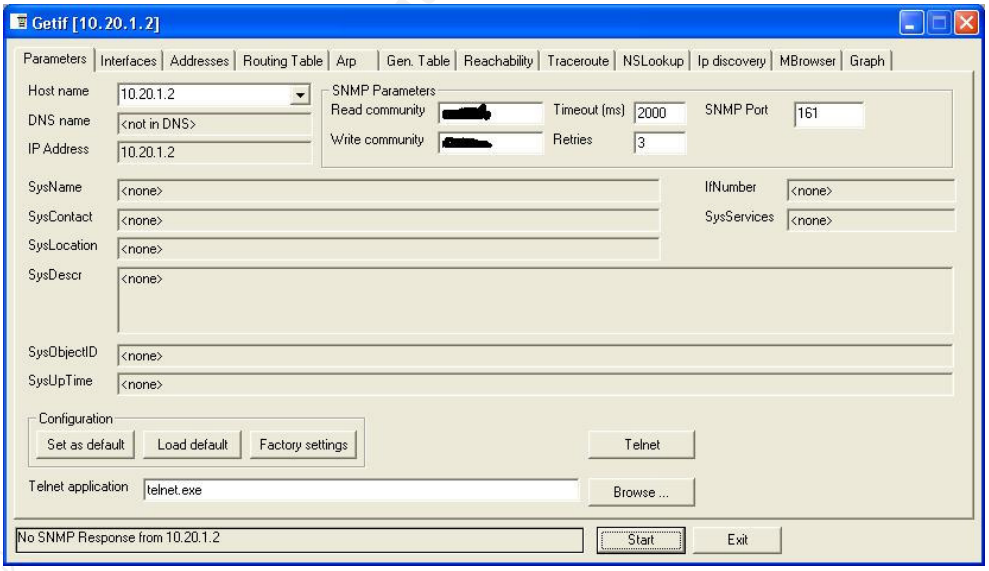
The OS upgrades are kept to a minimum so that it is easier to manage the devices. Later OS versions may and often do introduce or re-introduce issues and thus cause more patching problems. Due to the high availability nature of the network all OS upgrades are tested as fully as possible before being rolled out to all switches.

Security patches are reviewed immediately on notification and applied as soon as possible after testing.

The current versions on the routers are not at the latest version. A project is underway to upgrade all the routers to the latest tested version. There are later versions of software than what is being deployed but they haven't as yet been tested in the environment. The normal process for upgrading of the OS is to wait for the software to become General Deployment and then test and deploy into the environment.

Audit Step 11	Accountability
Control Objective	All devices connecting to the VLANs must be identified by their MAC address.
Testing	MAC addresses should be kept in a register with the details of the "owner" clearly identified? Unregistered MAC addresses should be prevented from connecting to the network (VLAN). Connect a PC to the network and determine by issuing the IPCONFIG command whether an IP address has been assigned. **Ipconfig /all** Review the syslog to determine if the unidentified MAC address has been logged when attempting to connect to a VLAN. Obtain a copy of any reports for review to determine if they address the unidentified MAC addresses connecting to the network.
Findings Pass	The MAC addresses are kept in a register with all details of who is the "owner" and contact details. This information is stored in the VLAN Management Protocol System. Unregistered MAC addresses are prevented from connecting to the network and obtaining an IP address. **Ipconfig /all**  Unregistered MAC addresses are logged to syslog and a daily report is sent to the network staff They investigate any anomalies and report to the Network Manager, who then reports any security concerns to the IT Manager for action. Syslog entry for the unauthorised MAC address: 13/11/03,9:46:14,10.20.1.191,xxxNos1nw1,LOCAL7,CRITICAL,2766: Nov 13

	09:45:05.35 0: %VQPCLIENT-2-DENY: Host xxxx.xxxx.xxxx denied on interface Fa0/18

Audit Step 14	IP permit lists for management ports
Control Objective	To reduce the exposure of the router to exploitation of the management ports by allowing only specific address to access these ports.
Testing	Check the router configuration to determine if there are access lists for the management ports being used for the VLAN being audited. Have the Network Administrator Telnet to the router and perform the following command. **show access-lists <vlan>** To check that the management ports are not accessible from the Office VLAN. **Use Getif to scan for SNMP from the Office VLAN.**
Findings Fail	No access list exists for blocking access to ports 2001, 4001 and 6001. **show access-lists Common** no access list for ports 2001, 4001 and 6001 **Getif connecting to router using the public community string.**  Getif could not connect to the router via SNMP, which demonstrates that this port is prevented from being accessed from this VLAN.

Audit Step 15	SNMP version and treatment of community strings
Control Objective	To determine whether SNMP is being used to manage the routers, the version of SNMP being used and to ensure that the community strings are treated as if they are root or administrator passwords.
Testing	Is SNMPv3 being used and are the community strings treated like root or administrator passwords? Have the Network Administrator Telnet to the router and perform the following command. **Show SNMP group** The following should be performed from a VLAN that has access to the management ports on the router. **Use Getif to scan for SNMP: Read community string of public and Write community string of private** **Use Getif to scan for SNMP: Read community string as defined.**
Findings Pass	SNMPv2 is used as not all Cisco equipment being employed across the sites support v3 yet. Some of the network management software being used does not yet support SNMP v3. All community strings are treated in the same manner as a root or administrator password. The default public and private SNMP community strings are deleted as part of the network device build procedures. **show snmp group** groupname: ILMI security model:v1 readview :*ilmi writeview: *ilmi notifyview: <no notifyview specified> row status: active groupname: ILMI security model:v2c readview :*ilmi writeview: *ilmi notifyview: <no notifyview specified> row status: active groupname: xxxxxx security model:v1 readview :v1default writeview: <no writeview specified> notifyview: *tv.FFFFFFFF.FFFFFFFF row status: active

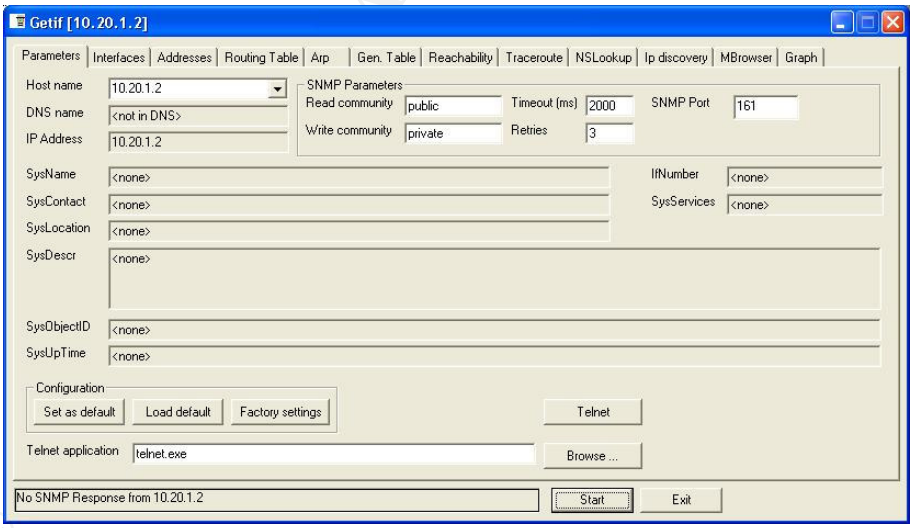
groupname: xxxxxx security model:v2c
readview :v1default writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active

groupname: yyyyyy security model:v1
readview :v1default writeview: v1default
notifyview: <no notifyview specified>
row status: active

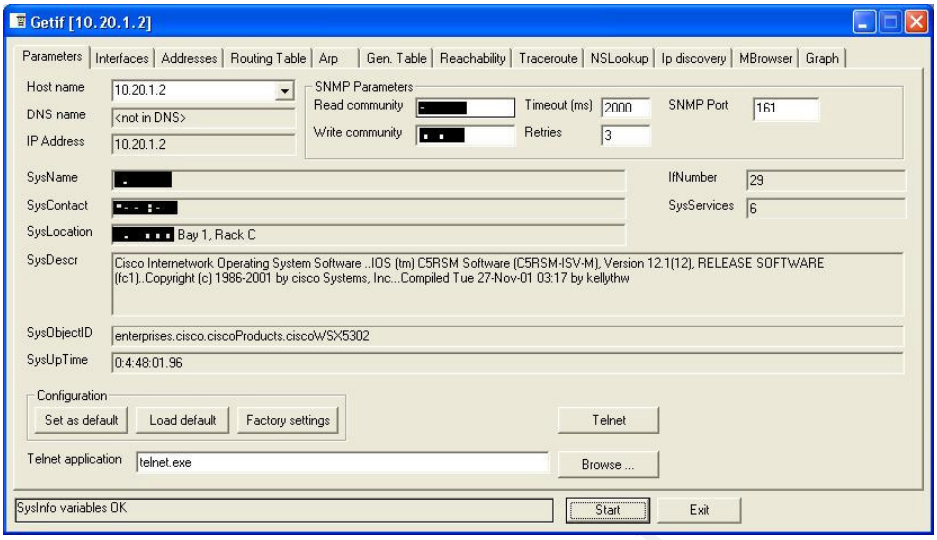
groupname: yyyyyy security model:v2c
readview :v1default writeview: v1default
notifyview: <no notifyview specified>
row status: active

The version of SNMP being used is shown as version 2.

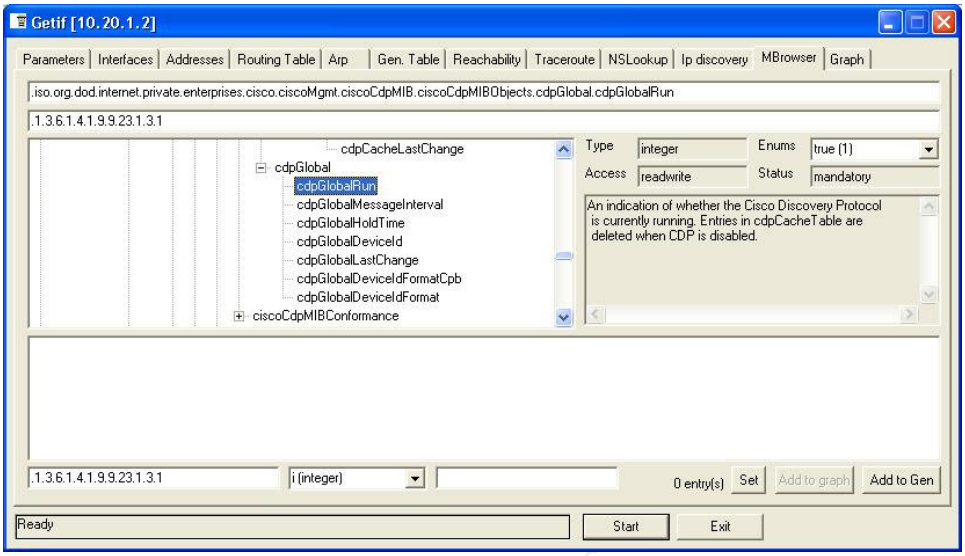
Getif with Read community string of Public and Write community string of private.



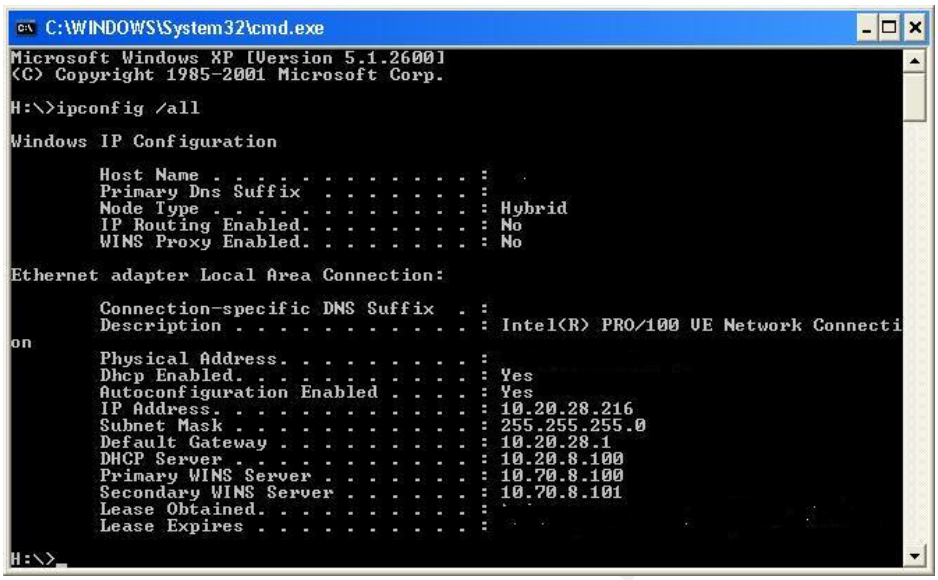
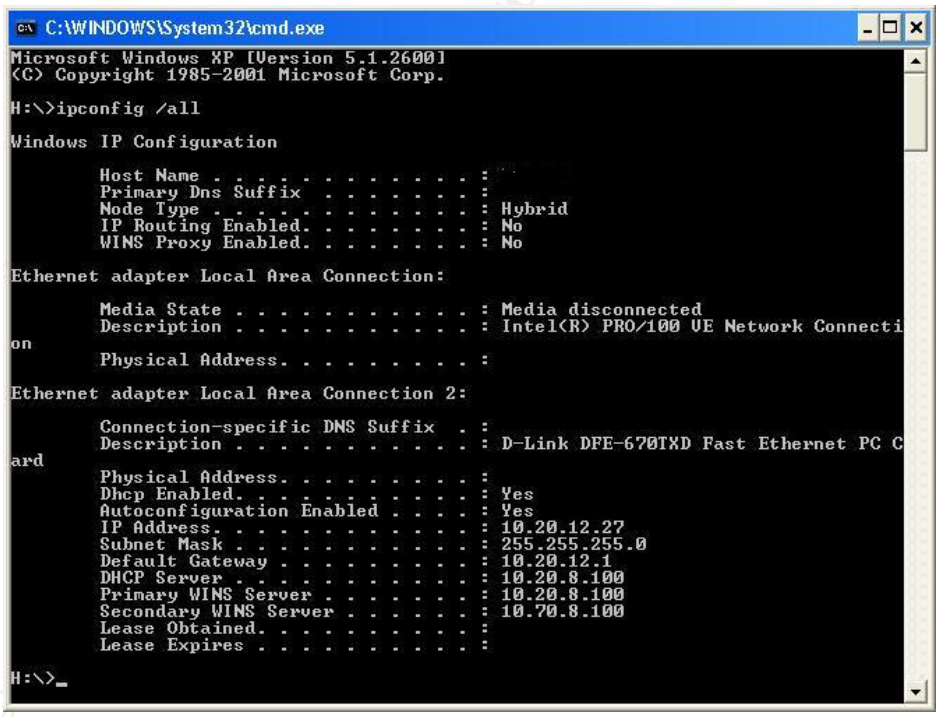
No access to SNMP via the default community strings public and private.

	Getif using the defined Read and Write Community strings  By using the appropriate community strings the router can be accessed.

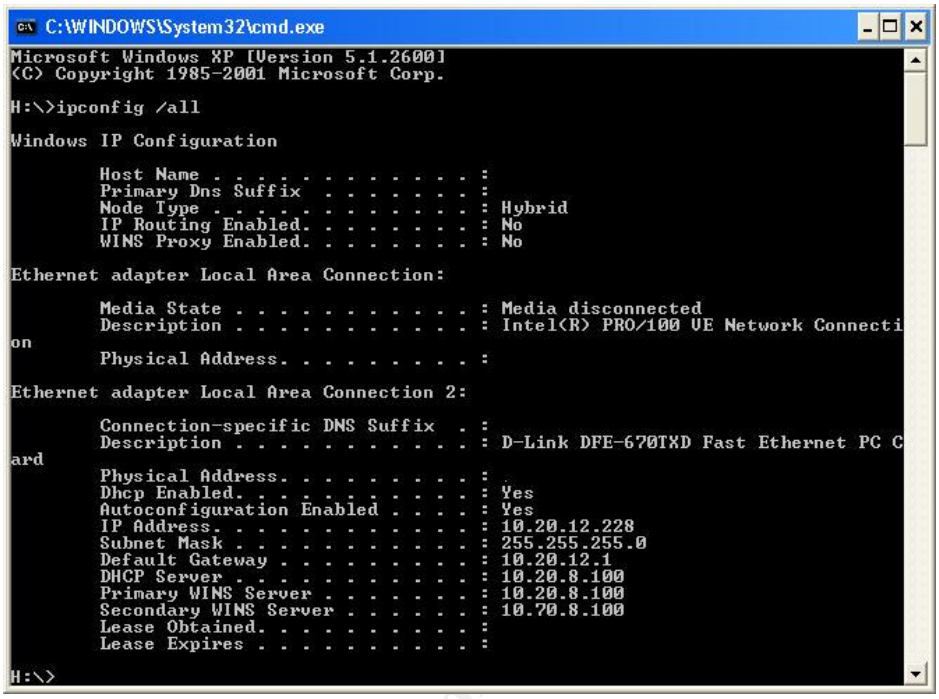
Audit Step 16	Cisco Discovery Protocol
Control Objective	The use of CDP should only be used where appropriate for network management.
Testing	Is the Cisco Discovery Protocol (CDP) being used on the VLAN being audited? Have the Network Administrator Telnet to the router and perform the following command. **Show CDP** The following should be performed from a VLAN that has access to the management ports on the router. **Use Getif to show if CDP active**
Findings Pass	Cisco Discovery Protocol has only been enabled for the core devices and disabled on all the edge devices. This router is not an edge device and has CDP enabled. **Show cdp** Global CDP information: Sending CDP packets every 60 seconds Sending a holdtime value of 180 seconds Sending CDPv2 advertisements is enabled

	Use Getif and browse through to MIB .1.3.6.1.4.1.9.9.23.1.3.1 to determine if CDP is on. 

Audit Step 17	Port security
Control Objective	Ports should be configured to associate a limited number of MAC addresses to each port.
Testing	Determine if port security has been configured for user ports. Are ports configured to associate a limited number of MAC addresses that can connect to them? **Show config** Connect a pc using a registered MAC address to a port and perform an **ipconfig /all** Connect another pc or the same pc with a different NIC and hence different registered MAC address to the same port and perform an **ipconfig /all**
Findings Fail	No. This was considered to be an unnecessary management overhead as the network is classed as trusted. **Show config** No mac port security defined in the configuration.

	Ipconfig /all (first MAC address)  **ipconfig /all** (second MAC address on the same port) 

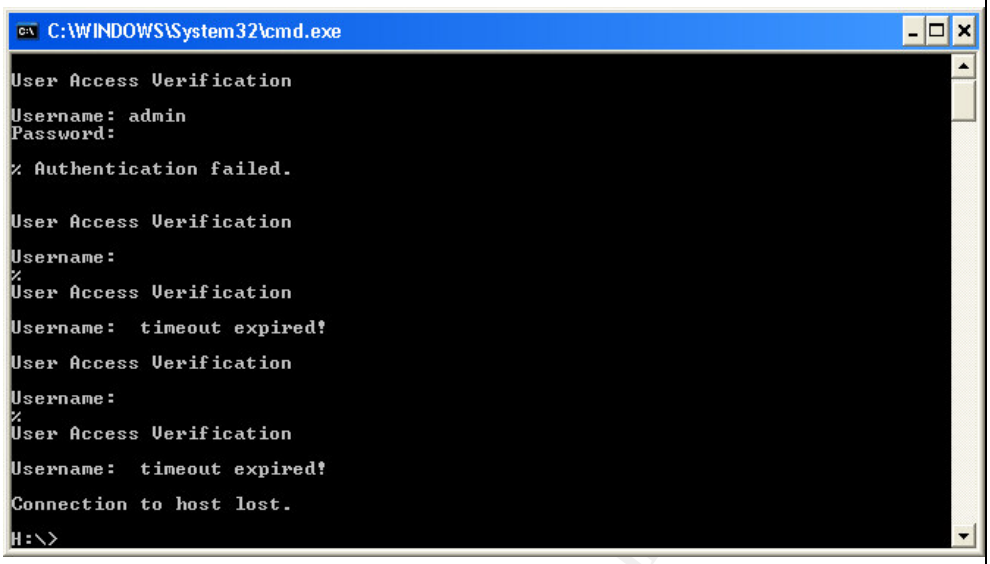
Audit Step 18	Disable unused ports
Control Objective	To prevent a network intruder from physically being able to use an unused port to gain access to the network.
Testing	Determine if unused ports are disabled and put in an unused VLAN.

	Connect a PC with a registered MAC address to an unused port. Perform an ipconfig to determine if a valid IP address has been assigned. **Ipconfig /all** 
Findings Fail	On core routers the unused ports are disabled. On the access routers they are enabled. This was considered to be an unnecessary management overhead such that in cases of failure other ports needed to be easily accessible to get alternative servers and workstations back on-line.

Audit Step 20	Logical access to the routers
Control Objective	To prevent unauthorised logical access to the routers.
Testing	Determine the protocols that are used to access the routers. Interview staff and get them to demonstrate how they gain access to the routers. Determine who has access to the routers. Have the Network Administrator Telnet to the router and perform the following command. **Show config** How is access to the routers controlled? Determine if cleartext management protocols, such as TELNET and SNMP are used.

	The following should be performed from a VLAN that has access to the management ports on the router. **telnet IP-address** Determine if unnecessary services have been disabled. Have the Network Administrator Telnet to the router and perform the following command to list the running process. **Show proc cpu** The following should be performed from a VLAN that has access to the management ports on the router. Check for TCP services: **Nmap –sS –PT –Pl –T 3 ipaddress** Check for UDP services: **Nmap –sU –PT –Pl –T 3 ipaddress**
Findings Pass	TELNET is the main protocol used for communicating with the switches. **show config** line vty 0 4 access-class 1 in exec-timeout 15 0 password 7 (removed) transport input telnet Only those who have access to the Administration VLAN and are a member of the tacacs group on the RADIUS server (TACACS at one site) and have an account on the router. **Show config** aaa new-model aaa authentication login default group tacacs+ line aaa authentication enable default group tacacs+ enable enable secret 5 (removed) The network is not considered to be hostile by management and as such both TELNET and SNMP v2c are used.

Telnet ipaddress



Telnet is being used, with a timeout active.

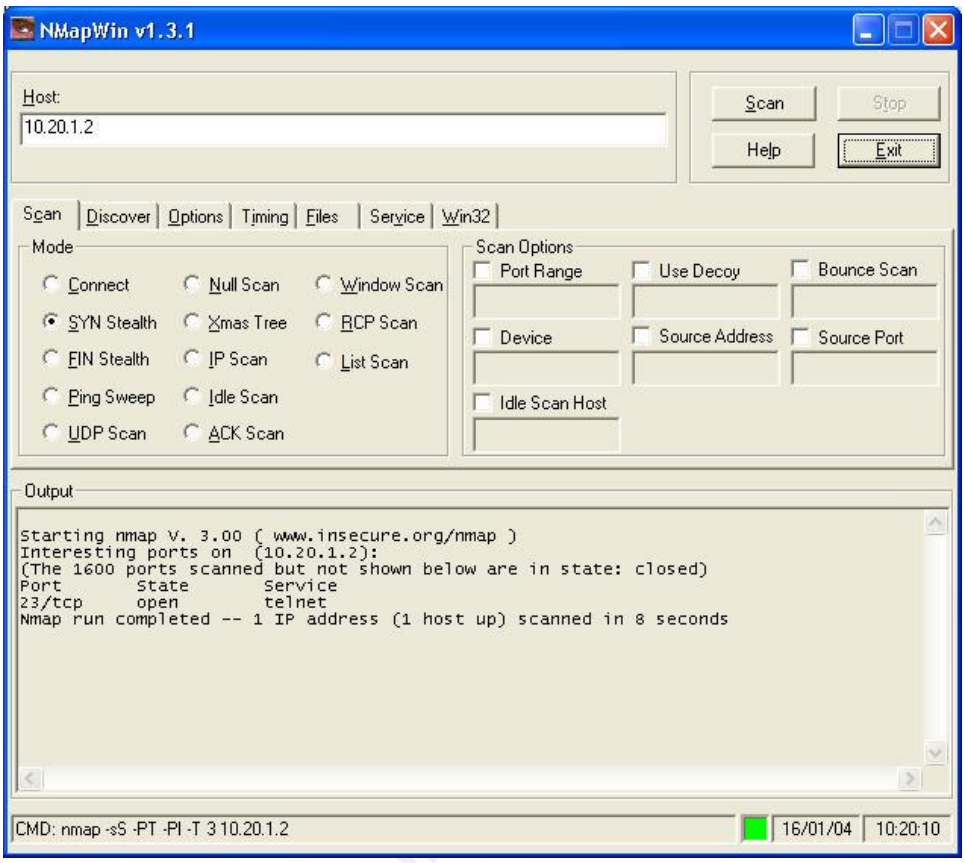
Show proc cpu

CPU utilization for five seconds: 21%/16%; one minute: 19%; five minutes: 17%

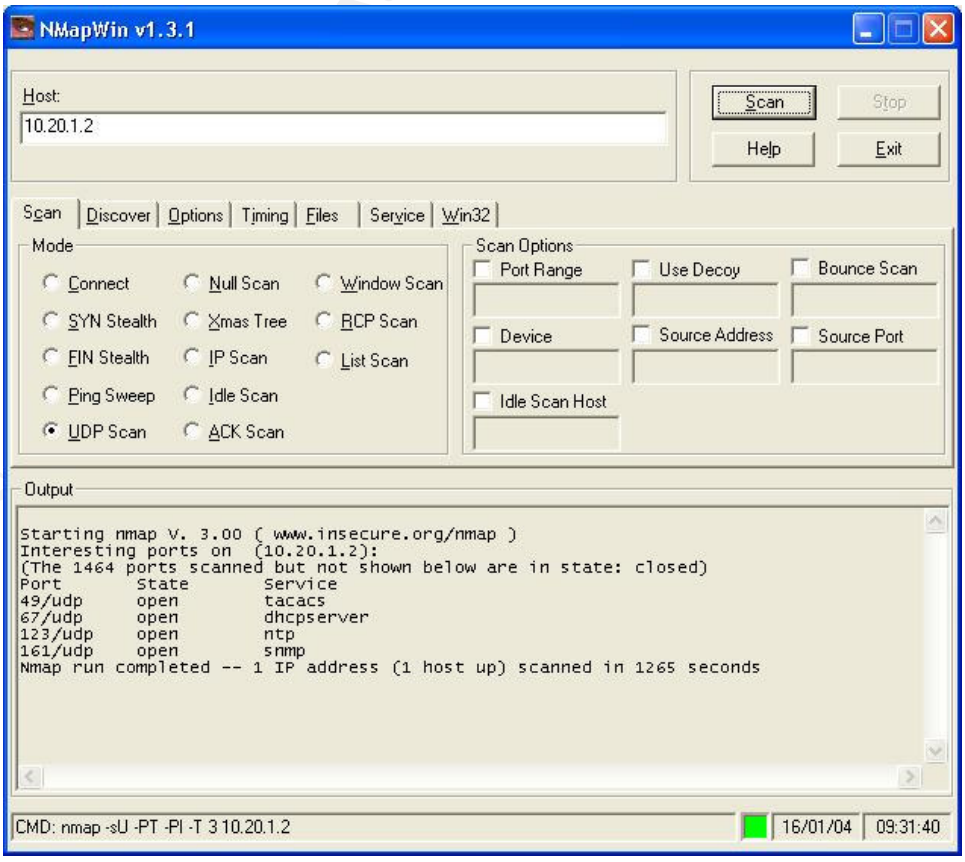
PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
1	1952	741291	2	0.00%	0.00%	0.00%	0	Load Meter
2	1866548	12084228	154	0.00%	0.02%	0.00%	0	OSPF Hello
3	3052560	439249	6949	0.00%	0.08%	0.06%	0	Check heaps
4	0	1	0	0.00%	0.00%	0.00%	0	Chunk Manager
5	1088	1535	708	0.00%	0.00%	0.00%	0	Pool Manager
6	0	2	0	0.00%	0.00%	0.00%	0	Timers
7	0	2	0	0.00%	0.00%	0.00%	0	Serial Backgroun
8	0	1	0	0.00%	0.00%	0.00%	0	OIR Handler
9	0	1	0	0.00%	0.00%	0.00%	0	IPC Zone Manager
10	38572	3705755	10	0.00%	0.00%	0.00%	0	IPC Periodic Tim
11	28312	3705755	7	0.00%	0.00%	0.00%	0	IPC Deferred Por
12	0	1	0	0.00%	0.00%	0.00%	0	IPC Seat Manager
13	16989064	19387971	876	0.98%	0.31%	0.28%	0	ARP Input
14	69444	741158	93	0.00%	0.00%	0.00%	0	HC Counter Timer
15	0	2	0	0.00%	0.00%	0.00%	0	DDR Timers
16	0	2	0	0.00%	0.00%	0.00%	0	Dialer event
17	0	1	0	0.00%	0.00%	0.00%	0	Entity MIB API
18	0	1	0	0.00%	0.00%	0.00%	0	SERIAL A'detect
19	0	1	0	0.00%	0.00%	0.00%	0	Microcode Loader
20	0	1	0	0.00%	0.00%	0.00%	0	Critical Bkgnd
21	168432	606476	277	0.00%	0.00%	0.00%	0	Net Background
22	152	236	644	0.00%	0.00%	0.00%	0	Logger
23	51316	3705742	13	0.00%	0.00%	0.00%	0	TTY Background
24	391876	3705755	105	0.00%	0.00%	0.00%	0	Per-Second Jobs
25	0	1	0	0.00%	0.00%	0.00%	0	Inode Table Dest
26	0	1	0	0.00%	0.00%	0.00%	0	Inode Table Refr
27	0	1	0	0.00%	0.00%	0.00%	0	IP Crashinfo Inp
28	0	1	0	0.00%	0.00%	0.00%	0	DSX3MIB ll handl

29	146824	3705755	39	0.00%	0.00%	0.00%	0	RSP Background
30	8	62	129	0.00%	0.00%	0.00%	0	IPC Cat5k Inband
31	0	1	0	0.00%	0.00%	0.00%	0	MIP Mailbox
32	0	1	0	0.00%	0.00%	0.00%	0	vcq_proc
33	0	1	0	0.00%	0.00%	0.00%	0	CT3 Mailbox
34	0	1	0	0.00%	0.00%	0.00%	0	CE3 Mailbox
35	0	1	0	0.00%	0.00%	0.00%	0	IPC CBus process
36	67131844	98849485	679	2.94%	1.34%	0.83%	0	IP Input
37	64504	434358	148	0.00%	0.00%	0.00%	0	CDP Protocol
38	0	1	0	0.00%	0.00%	0.00%	0	X.25 Encaps Mana
39	191640	63064	3038	0.00%	0.00%	0.00%	0	IP Background
40	0	1	0	0.00%	0.00%	0.00%	0	SNMP Timers
41	0	1	0	0.00%	0.00%	0.00%	0	PPP IP Add Route
42	304264	69800	4359	0.00%	0.00%	0.00%	0	Adj Manager
43	14522108	6233547	2329	0.24%	0.25%	0.25%	0	CEF process
44	612	61366	9	0.00%	0.00%	0.00%	0	TCP Timer
45	336	368	913	0.00%	0.00%	0.00%	0	TCP Protocols
46	4	1	4000	0.00%	0.00%	0.00%	0	Probe Input
47	0	1	0	0.00%	0.00%	0.00%	0	RARP Input
48	0	1	0	0.00%	0.00%	0.00%	0	HTTP Timer
49	0	1	0	0.00%	0.00%	0.00%	0	Socket Timers
50	56204	60394	930	0.00%	0.00%	0.00%	0	DHCPD Receive
51	109092	61764	1766	0.00%	0.00%	0.00%	0	IP Cache Ager
52	0	1	0	0.00%	0.00%	0.00%	0	PAD InCall
53	0	2	0	0.00%	0.00%	0.00%	0	X.25 Background
54	328	149	2201	0.00%	0.20%	0.05%	2	Virtual Exec
55	4152	7412167	0	0.00%	0.00%	0.00%	0	cbus utilization
56	10142176	100894173	100	0.08%	0.10%	0.09%	0	Net Input
57	9052	741291	12	0.00%	0.00%	0.00%	0	Compute load avg
58	719848	61764	11654	0.00%	0.00%	0.00%	0	Per-minute Jobs
59	4764284	635236	7500	0.00%	0.07%	0.08%	0	IP SNMP
60	4372	114	38350	0.00%	0.00%	0.00%	0	SNMP ConfCopyPro
61	0	1	0	0.00%	0.00%	0.00%	0	SNMP Traps
62	6232	195316	31	0.00%	0.00%	0.00%	0	CEF Scanner
63	183176	775211	236	0.00%	0.00%	0.00%	0	FCP Router
64	0	2	0	0.00%	0.00%	0.00%	0	IP Flow Backgrou
65	5185600	59438265	87	0.08%	0.00%	0.00%	0	Standby (HSRP)
66	24	1800	13	0.00%	0.00%	0.00%	0	TACACS+
67	0	3	0	0.00%	0.00%	0.00%	0	TCP Listener
68	644872	4669664	138	0.00%	0.00%	0.00%	0	NTP
70	48	30888	1	0.00%	0.00%	0.00%	0	DHCPD Timer
71	24996	1049973	23	0.00%	0.00%	0.00%	0	DHCPD Database
72	2485320	4332312	573	0.00%	0.00%	0.00%	0	OSPF Router
73	36832	8778767	4	0.00%	0.00%	0.00%	0	BGP Router
74	55920	123079	454	0.00%	0.00%	0.00%	0	BGP I/O
75	3315484	339105	9777	0.00%	0.06%	0.05%	0	BGP Scanner

Nmap –sS -PT –PI –T 3 ipaddress



nmap –sU –PT –PI –T 3 ipaddress



	The active services: • Telnet, • TACACS, • DHCP, • NTP and • SNMP.

Measure Residual Risk

Five control points failed their audit tests. The residual risk is discussed in the following tables:

Audit Step 1	Security Policy for VLAN access
Discussion	One of the basic building blocks for effective IT Security is policy. Policy is there to provide clear guidance in all areas of the business in the aspect of security and security related issues. Without this guidance then security may not be implemented according to what the business requires and can then increase the risk level to the business. Employees often end up making up what rules they think are correct for the organisation and this can be very different to what the business thinks is correct for the business.
Risk Mitigation	A policy needs to be written to cover the use of VLAN technology. This policy should cover: • Who can authorise changes to the VLAN environment, in respect to the configuration of the VLANs. • Who can authorise the movement of MAC addresses between VLANs and under what circumstances a movement can take place. • Who authorises the creation of a new VLAN.
Residual Risk	High. Without clear direction in the form of a policy then staff are required to make decisions that may conflict with the business requirements. These decisions may be made on technical or technology grounds instead of on business grounds.
Estimated Costs	Creation of policy, including the management review and endorsement of the policy: 20 hours.

Audit Step 2, 3 & 4	VLAN Functional Documentation, VLAN Design Documentation & IP Address Range Document
Discussion	The documentation that is required to take the business requirements and translate them into the VLAN design was provided. The IP Address range document that fully documents the IP address used by the organisation was provided. The VLAN Functional documentation had undergone a minor revision in July 2003 as stated in the release notes minor clarifications and was at v1.1a1. The other documentation have no release notes or change history associated with them. For the VLAN implementation to be capable of supporting the business requirements these documents must be kept up to date. To

	effectively keep these documents in a state that represents the business requirements there needs to be a regular review of them performed. Any changes in business direction could then be quickly implemented and thus have minimal impact on the business.
Risk Mitigation	As business requirements can change quickly to respond to the changing market place, the technology that supports the business needs to be able to respond as quickly. To reduce the risk of the technology of VLANs not supporting the business a six monthly review should be performed to ensure that the documents reflect the current business needs.
Residual Risk	Low. The business requirement document had been revised in the last six months whilst the other documents have no indication of having been reviewed. With a constant changing market place and the lack of updated documentation could mean that the VLANs do not meet the business needs and can actually hinder the business. Business requirements change over time and the technology supporting these requirements must be capable of supporting these changes. Without regular reviews of the business requirements and whether these business requirements are being met by the technology a situation can occur that can cause disruption to the business. An example may be that the business now requires some of those in the general office environment to have access to a particular server in the production environment. The VLAN configuration is updated without the VLAN design documentation being updated to reflect this change. A further updated required by the business is actioned according to the documentation, this change inadvertently grants access to more of the production environment than necessary because the VLAN design document did not reflect the actual VLAN environment. By performing a review of the documentation the undocumented changes would have been highlighted and any subsequent changes would not have granted incorrect access.
Estimated Costs	Review and maintenance of the documents. This would include the time spent on reviewing the business requirements, re-interviewing appropriate staff, updating the documents and submitting the documents for approval: 30 hours per year.

Audit Steps 13, 14, 15, 17,18	VLAN Configuration
Discussion	Even though VLANs are not implemented for security purposes there are certain security exposures that should be reduced to ensure that as another layer in security in-depth the best possible environment is created. Cisco does provide recommendations on how to best implement a VLAN and these recommendations should be followed where

	appropriate for the environment. It is good practice to use recommendations from other than the vendor to implement the environment as these recommendations are often developed with independence in mind and should provide clearer recommendations for both security and performance.
Risk Mitigation	The routers defining the VLAN environment should be configured to what can be considered as best practice to reduce both security exposures and performance issues.
Residual Risk	High. Most of the issues raised in this audit have been based on not following best practice. The following of best practice ensures that an adequate level of security has been complied with. As well as the resultant reduction in exposure of the organisation to exploits that take advantage of system defaults. Following best practice usually ensures that most of the potential exposures have been addressed and future exploits may not be able to take advantage of these exposures. "The results of @stake's test sequences clearly demonstrate that VLANs on Cisco Catalyst switches, when configured according to best-practice guidelines, can be effectively deployed as security mechanisms."[33] Using MAC address limiting on network device ports can prevent a malicious network user from using MAC address spoofing to gain access to other network devices. The use of clear text protocols, such as TELNET, enables a malicious user on the network to set up a sniffer to capture a userid and password. Once captured it is then easy for the user to gain access to the router and to reconfigure it for their own purposes.
Estimated Costs	This will take a reasonable amount of time and resources in reviewing the configuration to bring it up to best practices. I estimate that it would take a network specialist in the order of 60 - 80 hours to complete the work.

Is The System Auditable?

The VLAN system is auditable and the following objectives were met, determine if:

- The Office VLAN complies with the documented design and security requirements.
- The Office VLAN complies with the security policy of the organisation.
- The Office VLAN configuration meets current best practices.
- There are any improvements that can be applied.

[33] Secure Use of VLANS: An @stake Security Assessment

There were no issues raised in the auditing of the VLAN environment from performing the tests, therefore the VLAN environment is auditable. The documentation is auditable in a way that it shows that the design has been thought about and that the actual implementation has been based upon documented requirements of the business.

The actual design and functional specifications of the VLAN is not in question. The audit is to determine the accuracy of the implementation of the VLAN and whether the documents exist and are being properly maintained.

Assignment 4 – Audit Report

Executive Summary

This audit was commissioned to audit a subset of the VLAN implementation at GIAC Enterprises. This subset was specifically that the Office VLAN does not have un-documented access to the production VLAN and the configuration met with best practice recommendations.

The objectives of the audit have been met. These objectives were to determine if:

- The Office VLAN complies with the documented design and security requirements.
- The Office VLAN implementation complies with the security policy of the organisation.
- The Office VLAN configuration meets current best practices.
- There are any improvements that can be applied.

It should be noted that even though there are some audit issues that need to be addressed, the audit has demonstrated that the Office VLAN does not have any undocumented access to the Production VLAN.

Audit Findings

The audit has shown that the Office VLAN has been configured according to the documentation such that it does not have any undocumented access to the Production VLAN. However there are a number of areas that have failed the audit, these being:

Audit step 1 of the checklist: Fail. The Security Policy version 1.00 dated 26 June 2003 was reviewed to determine if there was any part of the policy that related to the implementation of VLANs. Even though the Security Policy covered many areas of network management and controls it does not have a policy directly relating to VLANs.

Audit step 2, 3 and 4 of the checklist: Fail. The documents: VLAN Functional Document, VLAN Design Document and IP Address Range Document, were reviewed and found to have adequately described the functional requirements of the business, the design was in line with the functional requirements and the IP Address range document covered the complete address range of the organisation. When questioned about the review cycle of all these documents it was determined that there is no formal procedure in place to conduct a review. These documents had been reviewed within the previous nine months in an informal process.

Audit steps 13, 14, 15, 17 & 18 of the checklist: Fail. The version of SNMP being used on the routers is v2c and not the recommended v3. The reason being given is that not all the equipment being used supports version 3 and to stay consistent across all the equipment the organisation has stayed with version 2. It has been considered by the organisation that the risk associated with staying at version 2 and being consistent across all the routers out ways the risk associated with being at a lower level of SNMP.

When ports are not required best practice states that they should be explicitly disabled instead of leaving them in such that they are neither disabled nor enabled. By leaving ports in an undefined state it can be possible for a hacker to force the port to enabled and use the port to gain access to the network. Future updates to the router software may change the state of ports from undefined state to one that conflict with the requirements of the organisation. By explicitly defining the state of the port means there is no misunderstanding regarding the state of the port.

Port security for the management ports 2001, 4001 and 6001 has not been configured. To prevent authorised access to the router management ports access control lists should be defined to restrict what IP addresses may have access to these ports.

Port security has not been configured for user ports. This could mean that a malicious user could use MAC address spoofing once connected to the network to redirect traffic and capture data from these packets in an effort to circumvent security measures. Spoofing is when a machine, in this case, pretends to be another machine. By using MAC address limiting then it is possible to prevent any user from pretending to be any other machine by using its MAC address, as only one MAC address may be used on a port in under say a 5 minute time period.

Unused ports on the access routers have not been disabled. This was considered to be an unnecessary management overhead, especially in the case of an equipment failure. Due to the high availability requirements it was considered that the risk of having the unused ports enabled for immediate access was lower than the risk of changing the configuration by moving the port from an unused VLAN to the correct VLAN whenever a port needed to be activated. Best practice is that unused ports should be disabled. This adds another layer of security to the network by making it more difficult for a malicious user from just connecting to the network and attempting to access network resources.

Allowing clear text information in the form of user account name and password to be transmitted across the network increases the risk of someone on the network using a sniffer to catch the account and password. Once captured the account can then be used to connect to a router and change the configuration to one that suits the attacker. This could be by enabling traffic to flow between VLANs that normally would not have this traffic flow or by preventing traffic to flow and cause a Denial of Service.

Best practice states that logon banners should be displayed to users when logging on to systems and/or resources so that in a case of being hacked there is some legal defence in that the person was notified that the system and/or resource was only for authorised personnel.

Background / Risk

A discussion of the risks associated with the issues raised as a result of the audit.

Audit step 1: Security Policy for VLAN access. This is a high-risk issue, without clear direction in the form of a policy then staff are required to make decisions that may conflict with the business requirements or top management's directions. The decisions that technical staff make are often made purely on technical or technology grounds instead of on business grounds. Two of the main objectives of a Security Policy are

> "To document top management's direction on and commitment to information security, and communicate it to all relevant individuals."[34] And
>
> "The information security policy should define information security, associated responsibilities and the information security principles to be followed by all staff."[34]

Audit Step 2, 3 & 4: VLAN Functional Documentation, VLAN Design Documentation & IP Address Range Document. Low. With a constant changing market place and the lack of updated documentation could mean that the VLAN design does not meet the business needs and could eventually hinder the business processes.

Business requirements change over time and the technology supporting these requirements must be capable of supporting the changes. Without a regular review of the business requirements and whether these business requirements are being met by the technology then a situation may occur whereby the business processes are disrupted. This disruption then causes a loss in business and a resulting loss of confidence with the IT systems.

An example may be that the business now requires some of those in the general office environment to have access to a particular server in the production environment. By not reviewing all the documentation and updating it accordingly all users in the general office VLAN may end up being granted access to the complete production environment instead of the individual server, which is not what the business wants.

Audit Step 13, 14, 15, 17 & 18: VLAN Configuration. High. The following of best practice ensures that an adequate level of security has been complied with and this should reduce the exposure of the organisation to exploits that take advantage of system defaults.

Following best practice usually ensures that most of the potential exposures have been address and future exploits may not be able to take advantage of these exposures.

> "The results of @stake's test sequences clearly demonstrate that VLANs on Cisco Catalyst switches, when configured according to best-practice guidelines, can be effectively deployed as security mechanisms."[35]

[34] Information Security Forum (ISF), "The Standard of Good Practice for Information Security", V4.0, March 2003, http://www.isfsecuritystandard.com/pdf/standard.pdf, (7 Nov 2003)
[35] Secure Use of VLANS: An @stake Security Assessment

Audit Recommendations

To mitigate the risks associated with the areas found to be deficient in the audit I have the following recommendations:

- Update the Security Policy to include a policy on VLANs and who can authorise a connection to the high privilege VLANs such as the production VLAN.
- The documents that define the VLANs need to be scheduled for regular review and update to correctly reflect the business requirements. These documents should be reviewed at least six monthly to determine whether they still meet the needs of the business.
- An access list should be defined to prevent unauthorised access to ports 2001, 4001 and 6001.
- The organisation should look at ensuring that it progresses upgrading all the network equipment to support SNMP v3.
- Investigate the potential to use MAC Limiting on network device ports to reduce the possibility of MAC address spoofing. An example would be to limit one MAC address to be on a port at one time. If this number is exceeded before the previous MAC address is aged out (default of 5 minutes), then the port will be automatically shutdown awaiting manual intervention.
- A review should be conducted on the possibility of disabling unused ports and allocating them to an unused VLAN. Best practice states that ports should be explicitly disabled when not required instead of leaving them in an undefined state.
- Even though the network is considered to be trusted it is best practice to use a secure protocol to communicate with devices such as routers than to use plain text protocols like TELNET. I recommend changing to Secure Shell Protocol (SSH) instead of TELNET for communicating with the routers.
- Whilst performing the audit it was noted that no banners are displayed on connecting to the routers by TELNET. It is best practice to display a banner notifying anyone connecting to the router that it is for authorised user only. I recommend creating a banner along the lines of “This system is for authorised network administrators only. All activity will be recorded and monitored.”

Costs

The costs have been estimated in the form of hours of work required to complete the task. This gives a better estimate of the cost than actual dollars because the cost will vary depending upon the costs associated with those who will actually perform the work.

Item	Cost
Security Policy for VLAN access	Creation of policy, including the management review and endorsement of the policy: 20 hours.
VLAN Functional Documentation, VLAN Design Documentation & IP Address Range Document	Review and maintenance of the documents. This would include the time spent on reviewing the business requirements, re-interviewing appropriate staff, updating the documents and submitting the documents for approval: 30 hours per year.
VLAN Configuration	This will take a reasonable amount of time and resources in reviewing the configuration to bring it up to best practices. I estimate that it would take a network specialist in the order of 60 - 80 hours to complete the work.

Table 2: Estimated costs

Compensating Controls

Even though the Security Policy does not completely cover the security issues relating the VLANs, the current procedures in place in the Network Services Department do compensate for this inadequacy. These procedures would suffice until the Security Policy has been updated.

Using SNMP v2 as the standard SNMP for the network devices is adequate considering that the public strings have been treated as a root password. Using SNMP v2 will suffice whilst the project to update all the routers to the same level of IOS. As an outcome of this project there is a follow up project to investigate the upgrading of SNMP to v3.

In an ideal world, the disabling of all unused ports is the goal. Knowing that in the real world, this is not always possible then the goal should be to reduce the exposure of leaving unused ports enabled. To achieve this goal then the logs need to be continually monitored for unusual activity. Any unusual activity should then be investigated thoroughly to alleviate any concerns of unauthorised access attempts.

Glossary

Term	Definition
ACL	Access Control List
BPDU	Bridge Protocol Data Unit
DMZ	De-Militarised Zone
IOS	Cisco's Internetwork Operating System
IP	Internet Protocol
ISF	Information Security Forum
ISO	International Standards Organisation
MAC	Media Access Control
NIC	Network Interface Card
POP	Point of Presence
RADIUS	Remote Authentication Dial-in User Service
RSM	Route Switch Module
SNMP	Simple Network Management Protocol
SSH	Secure Shell protocol
TACACS	Terminal Access Controller Access Control System
UDLD	UniDirectional Link Detection
VLAN	Virtual Local Area Network
VMPS	Cisco's VLAN Membership Policy Server

Table 3: Glossary of terms

References

"Webopedia: Online Dictionary for Computer and Internet Terms." 5 April 2003, URL: http://www.webopedia.com/TERM/V/VLAN.html (4 Sept. 2003).

Blanco, Ramon Luis Perez, "Whatis?com", 15 June 1999, URL: http://iroi.seu.edu.cn/books/ee_dic/whatis/vlan.htm (4 Sept. 2003).

Information Security Forum (ISF), "The Standard of Good Practice for Information Security", V4.0, March 2003, http://www.isfsecuritystandard.com/pdf/standard.pdf, (7 Nov 2003)

Cisco Systems Inc, "SAFE Enterprise Layer 2 Addendum", 2003, URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfblu_wp.pdf, (4 Sept 2003)

Pollino, David, Schiffman, Mike "Secure Use of VLANs: An @stake Security Assessment", August 2002 , URL: http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf, (8 Sept 2003)

Cisco Systems Inc, "Cisco – Securing Networks with Private VLANS and VLAN Access Control Lists", 15 July 2003, URL: http://www.cisco.com/warp/public/473/90.shtml, (Sept 2003)

Dietrich, John "Auditing A Checkpoint VPN-1 Mobile User Virtual Private Network (VPN) From An Independent Auditor's Point Of View", 11 February 2003, URL: http://www.giac.org/practical/GSNA/John_Dietrich.pdf, (Sept 2003)

Goudie, Mark, "Auditing a Cisco PIX Firewall An Auditor's Perspective", 21 August 2003, URL: http://www.giac.org/practical/Darrin_Wassom_GSNA.doc, (Sept 2003)

Yee, Marvin, "Auditing Cisco Perimeter Routers", 26 October 2001, URL: http://www.giac.org/practical/Marvin_Yee_GSNA.zip, (Sept 2003)

Gill, Stephen, "Catalyst Secure Template", Version 1.21, 14 November 2002, URL: http://www.qorbit.net/documents/catalyst-secure-template.htm, (Sept 2003)

Wagner, Richard, "Securing Network Infrastructure and Switched Networks", SANS Reading Room, 21 August 2001, URL: http://www.sans.org/rr/papers/index.php?id=451, (Sept 2003)

Ratliff, Richard L. "Internal Auditing: Principles and Techniques. Altamonte Springs: The Institute of Internal Auditors", 1996. 187-193.

Viitamaki, Oliver, "An Audit of a Wireless Demonstration Network Implementing Cisco Aironet 1200 An Auditor's Perspective, GSNA Practical V2.1 - San Francisco - December 2002"

International Organization for Standardisation (ISO 17799), URL: http://www.iso.ch/iso/en/prods-services/popstds/informationsecurity.html