Summer 7-2012

Implementing network security at Layer 2 and Layer 3 OSI model

Luan Gashi

University for Business and Technology

Faculty of Computer Science and Engineering

Implementing network security at Layer 2 and Layer 3 OSI model

Student: Luan Gashi

July 2012

Prishtinë

Faculty of Computer Sciences and Engineering

Academic year 2011-2012

Student: Luan Gashi

Bachelor Thesis

Implementing network security at Layer 2 and Layer 3 OSI model

Mentor: Dr.Sc. Petrit Shala

July / 2012

Abstract

This thesis investigated the features of security devices that would be suitable for implementations in medium to large enterprise networks at the global scale. In the thesis are covered open standard and proprietary security features. The open standard security features that are discussed in the report are the one that are developed by Internet Engineering Task Force – IETF and described in their Request For Comments – RFC. The proprietary features discussed in this report are from Cisco Systems and these features are always implemented in the Cisco Systems equipment.

The author at the beginning describes common vulnerabilities, threats and attacks and then used comparative and quantities methodology to analyze the security features and its mitigation. Then in details were analyzed features of Cisco security devices, which operate at layer two and three of the OSI model, as the most commonly used equipment worldwide for securing entire computer networks.

Based on their features and technical specifications it is shown that Cisco IOS Firewall feature set and Cisco Adaptive Security Appliance features are suitable for medium to big networks and with a staff that has advanced knowledge of risk security at computer networks.

Network security is the process by which digital information assets are protected. The goals of security are to protect confidentiality, maintain integrity, and assure availability. With this in mind, it is imperative that all networks be protected from threats and vulnerabilities in order for a business to achieve its fullest potential. Typically, these threats are persistent due to vulnerabilities, which can arise from misconfigured hardware or software, poor network design, inherent technology weaknesses, or end-user carelessness.

With the help of the Packet Tracer simulation software, different features and implementations of security features are tested. Using Packet Tracer software the author has created configuration script for every case used in a designed topology.

At the end of the thesis under the Appendixes section is introduced operation of the Packet Tracer and configuration topology that is used throughout this report for the testing purposes.

Acknowledgements

This thesis would have been incomplete without the contributions of the following people.

First and foremost, I would like to express my sincere gratitude to my mentor Dr.Sc. Petrit Shala, who despite his busy schedule devoted a great deal of time in supervising me. Thank you very much for your constant confidence and encouraging support throughout the process of writing this thesis.

I would also like to express my gratitude to the management of the department of Computer Science for my three years of studies here at University of Business and Technology – UBT in Prishtina.

Lastly, I am very grateful to my wife, my parents, brothers and sisters and my friends, who always expressed full hope and encouragement toward me. Without their support, this thesis would prove unsuccessful.

Prishtina, 16th May 2012

Luan Gashi

Table of Contents

List of figures

Acronyms

ACL	- Access Control List
AFI	- Address Family Identifier
ARP	- Address Resolution Protocol
BGPv4	- Border Gateway Protocol version 4
CAM	- Content Addressable Memory
CIDR	- Classless Inter-domain Routing
DHCP	- Dynamic Host Configuration Protocol
DNS	- Domain Name System
DUAL	- Diffusing Update Algorithm
EIGRP	- Enhanced Interior Gateway Routing Protocol
ICMP	- Internet Control Message Protocol
IETF	- Internet Engineering Task Force
IGRP	- Interior Gateway Routing Protocol
ISP	- Internet Service Provider
MAC	- Media Access Control
MD5	- Message Digest 5
NTP	- Network Time Protocol
OSI	- Open System Interconnection
OSPF	- Open Shortest Path First
PDM	- Protocol-dependent modules
RFC	- Request for Comments
RIPng	- Routing Information Protocol Next Generation
RTP	- Reliable Transport Protocol
SNMP	- Simple Network Management Protocol
SSH	- Secure Shell
VLAN	-Virtual Local Area Network
VLSM	- Variable Length Subnet Mask

1. Introduction

1.1. Introduction to Vulnerabilities, Threats, and Attacks

The Internet continues to grow exponentially. As personal, government and business-critical applications become more prevalent on the Internet, there are many immediate benefits. However, these network-based applications and services can pose security risks to individuals as well as to the information resources of companies and government. In many cases, the rush to get connected comes at the expense of adequate network security. Information is an asset that must be protected. Without adequate protection or network security, many individuals, businesses, and governments are at risk of losing that asset. [7]

Network security is the process by which digital information assets are protected. The goals of security are to protect confidentiality, maintain integrity, and assure availability. With this in mind, it is imperative that all networks be protected from threats and vulnerabilities in order for a business to achieve its fullest potential. Typically, these threats are persistent due to vulnerabilities, which can arise from misconfigured hardware or software, poor network design, inherent technology weaknesses, or end-user carelessness. [7]

This topic provides an overview of essential network security concepts, common vulnerabilities, threats, attacks, and vulnerability analysis.

1.2. Overview of Network Security

Security has one purpose, to protect assets. For most of history, this meant building strong walls to stop the bad guys, and establishing small, well-guarded doors to provide secure access for the good guys. This strategy worked well for the centralized, fortress-like world of mainframe computers and closed networks. The closed network typically consists of a network designed and implemented in a corporate environment, and provides connectivity only to known parties and sites without connecting to public networks. Networks were designed this way in the past and thought to be reasonably secure because of no outside connectivity. [1]

With the advent of personal computers, LANs, and the wide-open world of the Internet, the networks of today are more open. As e-business and Internet applications continue to grow, finding the balance between being isolated and being open will be critical, along with the ability to distinguish the good guys from the bad guys. Furthermore, the rise of mobile commerce and wireless networks will be as the cannon was to the castle walls, exploding the old model and demanding that security solutions become seamlessly integrated, more transparent, and more flexible. [3]

With the increased number of LANs and personal computers, the Internet began to create untold numbers of security risks. Firewall devices, which are software or hardware that enforce an access control policy between two or more networks, were introduced. This technology gave businesses a balance between security and simple outbound access to the Internet which was mostly used for e-mail and Web surfing.This balance was short lived however as the use of extranets began to grow, which connected internal and external business processes. Businesses were soon realizing tremendous cost savings by connecting supply-chain management and enterprise resource planning systems to their business partners, and by connecting sales-force automation systems to mobile employees, and by providing electronic commerce connections to business customers and consumers. The firewall began to include intrusion detection, authentication, authorization, and vulnerability assessment systems. Today, successful companies have once again struck a balance by keeping the bad guys out with increasingly complex ways of letting the good guys in. [1]

Most people expect security measures to ensure the following:

- Users can perform only authorized tasks.
- Users can obtain only authorized information.
- Users cannot cause damage to the data, applications, or operating environment of a system.

The word security means protection against malicious attack by outsiders, and involves controlling the effects of errors and equipment failures. Anything that can protect against an attack will probably prevent random misfortune as well. Throughout this course many definitions, acronyms and logical device symbols dealing with security will be introduced. Refer to the glossary for further explanation when encountering unknown terms and acronyms. A risk analysis should identify the risks to the network, network resources, and data. The intent of a risk analysis is to identify the components of the network, evaluate the importance of each component, and then apply an appropriate level of security. This helps to maintain a workable balance between security and required network access. Before the network can be secured, the individual components that make up the network must be identified. An asset inventory needs to be created. All of the network devices and endpoints, such as hosts and servers, should be included in the asset inventory. Once the inventory is complete, the components can be prioritized and assessed for vulnerabilities. [1]

Once the network components have been identified, they can be assessed for vulnerabilities. These vulnerabilities could be weaknesses in the technology, configuration, or security policy. Any vulnerability that is discovered will need to be addressed to mitigate any threat that could take advantage of the vulnerability. Vulnerabilities can be fixed by various methods, including applying software patches, reconfiguring devices, or deploying countermeasures, such as firewalls and anti-virus software. A threat is an event that can take advantage of vulnerability and cause a negative impact on the network. Potential threats to the network need to be identified, and the related vulnerabilities need to be addressed to minimize the risk of the threat. The goal of any security design is to provide maximum security with minimum impact on user access and productivity. Some security measures, such as network data encryption, do not restrict access and productivity. On the other hand, cumbersome or unnecessarily redundant verification and authorization systems can frustrate users and prevent access to critical network resources. [3]

Like security models, many devices can be classified as open, restrictive, or closed. For example, routers and switches are typically open devices, allowing high functionality and services by default. On the other hand, a firewall is typically a closed system that does not allow any services until they are switched on. Server operating systems can fall into any of the three categories, depending on the vendor. It is important to understand these principles when deploying these devices. An open security model is the easiest to implement. Very few security measures are implemented in this design. Administrators configure existing hardware and software basic security capabilities. Firewall, Virtual Private Networks (VPN), Intrusion Detection Systems (IDS) and other measures that incur additional costs are typically not implemented. Simple passwords and server security become the foundation of this model. If encryption is used, it is implemented by individual users or on servers. This model assumes that the protected assets are minimal, users are trusted and threats are minimal. However, this does not exclude the need for data backup systems in most open security policy scenarios. LANs, which are not connected to the Internet or public WANs, are more likely to implement this type of model. [7]

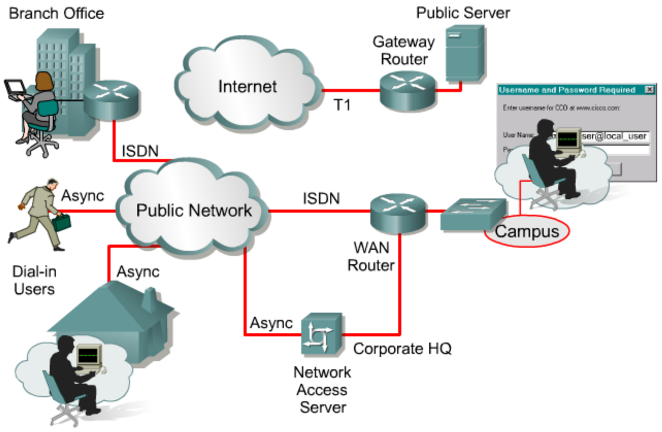


Figure 1. An open security model [7]

This type of network design gives users free access to all areas. When security breaches occur, they are likely to result in great damage and loss. Network administrators are usually not held responsible for network breaches or abuse. A restrictive security model is more difficult to implement. Many security measures are implemented in this design. Administrators configure existing hardware and software for security capabilities in addition to deploying more costly hardware and software solutions such as firewalls, VPN, IDS, and identity servers. Firewalls and identity servers become the foundation of this model. This model assumes that the protected assets are substantial, some users are not trustworthy, and that threats are likely. LANs, which are connected to the Internet or public WANs, are more likely to implement this type of model. Ease of use for users is diminished as security is tightened. [7]

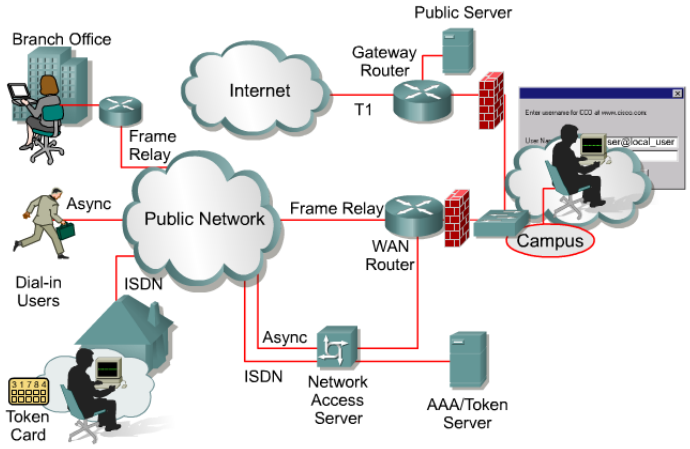


Figure 2. A restrictive security model [7]

A closed security model is most difficult to implement. All available security measures are implemented in this design. Administrators configure existing hardware and software for maximum-security capabilities in addition to deploying more costly hardware and software solutions such as firewalls, VPN, IDS, and identity servers.This model assumes that the protected assets are premium, all users are not trustworthy, and that threats are frequent. User access is very difficult and cumbersome. Network administrators require greater skills and more time to administer the network. Furthermore, companies require a higher number of network administrators to maintain this tight security. [7]

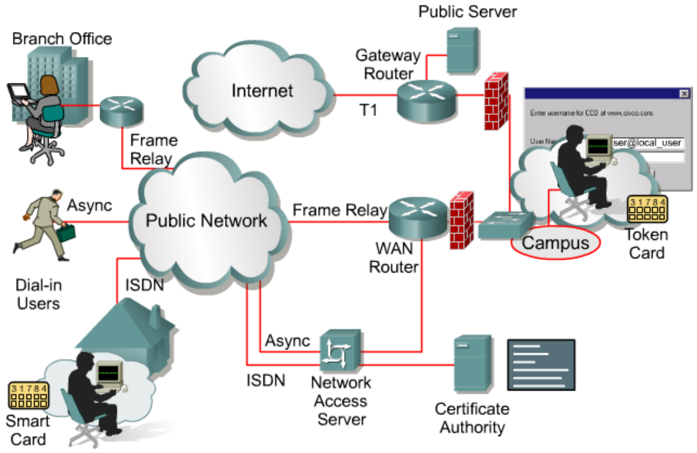


Figure 3. A closed security model [7]

In many corporations and organizations, these administrators are likely to be very unpopular while implementing and maintaining security. Network security departments must clarify that they only implement the policy, which is designed, written, and approved by the corporation. Politics behind the closed security model can be monumental. In the event of a security breach or network outage, network administrators may be held more accountable for problems. As in any fast-growing industry, changes are to be expected. The types of potential threats to network security are always evolving. If the security of the network is compromised, there could be serious consequences, such as loss of privacy, theft of information, and even legal liability. For many businesses today, one of the biggest reasons to create and follow a security policy is compliance with the law. Any business is potentially liable should a hacker or a virus take down the operation. Similarly, if a business is running a publicly held e-business and a catastrophic attack seriously impairs the business, a lawsuit is possible. The increasing use of wireless local area network (WLAN) connections and the rapid rise of Internet access from cell phones in Europe and Asia are requiring entirely whole new approaches to security. RF connections do not respect firewalls the way wired connections do. Moreover, the slow processors, small screens, and nonexistent keyboards on cell phones and personal digital assistants (PDAs) break many of the standard approaches to access, authentication, and authorization. The number of broadband connections to the Internet from homes is exceeding projections. Many businesses are finding that multiple T1 or E1 connections to the Internet are no longer sufficient. Current software-based security approaches have problems scaling to OC-1 and higher rates. [7]

1.3. Overview of Vulnerabilities, Threats, and Attacks

When discussing network security, three common terms used are vulnerability, threat, and attack. Vulnerability is a weakness which is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves. Threats are the people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses. Finally, the threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints such as servers and desktops. [1]

There are three primary vulnerabilities or weaknesses:

Technological Weaknesses - Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses.

Configuration Weaknesses - Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate.

Security Policy Weaknesses - Security policy weaknesses can create unforeseen security threats. The network may pose security risks to the network if users do not follow the security policy.

There are four primary classes of threats to network security:

Unstructured threats - Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker’s skills can still do serious damage to a company. For example, if an external company Web site is hacked, the integrity of the company is damaged. Even if the external Web site is separate from the internal information that sits behind a protective firewall, the public does not know that. All the public knows is that the site is not a safe environment to conduct business. [2]

Structured threats - Structured threats come from hackers that are more highly motivated and technically competent. These people know system vulnerabilities, and can understand and develop exploit-code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies. [2]

External threats - External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers. [2]

Internal threats - Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. According to the FBI, internal access and misuse account for 60 to 80 percent of reported incidents .[2]

As the types of threats, attacks, and exploits have evolved, various terms have been coined to describe different groups of individuals. Some of the most common terms are as follows: Hacker, Cracker, Phreaker, Spammer, Phisher, White hat and Black hat.

There are 3 primary classes of attacks [7] :

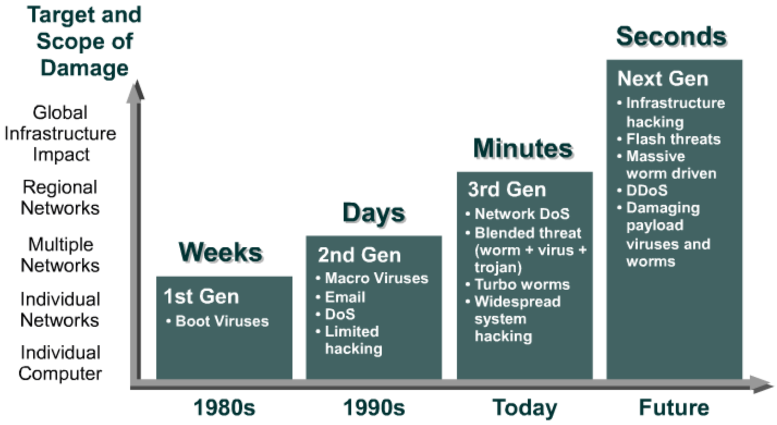


Figure 4. Classes of attacks [7]

Reconnaissance - Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering and, in most cases, it precedes an actual access or Denial of Service (DoS) attack. Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, easy-to-open doors, or open windows. [2]

Access - System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems to which one does not have access usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked. [2]

Denial of Service (DoS) - Denial of service (DoS) implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack simply involves running a hack or script. The attacker does not need prior access to the target because a way to access it is all that is usually required. For these reasons, DoS attacks are the most feared. [2]

1.4. Attack Examples

Reconnaissance attacks can consist of the following:

- Packet sniffers
- Port scans
- Ping sweeps
- Internet information queries

A malicious intruder typically ping sweeps the target network to determine which IP addresses are alive . After this, the intruder uses a port scanner to determine what network services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the application type and version, as well as the type and version of operating system running on the target host. Based on this information, the intruder can determine if a possible vulnerability exists that can be exploited. Using, for example, the *nslookup* and *whois* utilities, an attacker can easily determine the IP address space assigned to a given corporation or entity . The **ping** command tells the attacker what IP addresses are alive. Network snooping and packet sniffing are common terms for eavesdropping. Eavesdropping is listening in to a conversation, spying, prying, or snooping. The information gathered by eavesdropping can be used to pose other attacks to the network. [3]

An example of data susceptible to eavesdropping is SNMP version 1 community strings, which are sent in clear text. An intruder could eavesdrop on SNMP queries and gather valuable data on network equipment configuration. Another example is the capture of usernames and passwords as they cross a network.

Types of Eavesdropping - A common method for eavesdropping on communications is to capture TCP/IP or other protocol packets and decode the contents using a protocol analyzer or similar utility. Two common uses of eavesdropping are as follows [7]:

- **Information gathering** – Network intruders can identify usernames, passwords, or information carried in the packet such as credit card numbers or sensitive personal information.
- **Information theft** – Network eavesdropping can lead to information theft. The theft can occur as data is transmitted over the internal or external network. The network intruder can also steal data from networked computers by gaining unauthorized access. Examples include breaking into or eavesdropping on financial institutions and obtaining credit card numbers. Another example is using a computer to crack a password file.

Tools Used to Perform Eavesdropping- The following tools are used for eavesdropping:

- Network or protocol analyzers
- Packet capturing utilities on networked computers

Methods to Counteract Attacks - Three of the most effective methods for counteracting eavesdropping are as follows:

- Implementing and enforcing a policy directive that forbids the use of protocols with known susceptibilities to eavesdropping
- Using encryption that meets the data security needs of the organization without imposing an excessive burden on the system resources or the users
- Using switched networks

Access attacks - Access attacks exploit known vulnerabilities in authentication services, FTP services, and Web services to gain entry to Web accounts, confidential databases, and other sensitive information. Access attacks can consist of password attacks which can be implemented using several methods, including brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both. These repeated attempts are called brute force attacks.

Often a brute-force attack is performed using a program that runs across the network and attempts to log in to a shared resource, such as a server. When an attacker gains access to a resource, he or she has the same access rights as the user whose account has been compromised. If this account has sufficient privileges, the attacker can create a back door for future access, without concern for any status and password changes to the compromised user account. [2]

Trust Exploitation - Although it is more of a technique than a hack itself, trust exploitation refers to an attack in which an individual takes advantage of a trust relationship within a network. The classic example is a perimeter network connection from a corporation. These network segments often house Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), and Hypertext Transfer Protocol (HTTP) servers. Because all these servers reside on the same segment, the compromise of one system can lead to the compromise of other systems because these systems usually trust other systems attached to the same network. Another example is a system on the outside of a firewall that has a trust relationship with a system on the inside of a firewall. When the outside system is compromised, it can take advantage of that trust relationship to attack the inside network. Another form of an access attack involves privilege escalation. Privilege escalation occurs when a user obtains privileges or rights to objects that were not assigned to the user by an administrator. Objects can be files, commands, or other components on a network device. The intent is to gain access to information or execute unauthorized procedures. This information will be used to gain administrative privileges to a system or device. They use these privileges to install sniffers, create backdoor accounts, or delete log files. Trust exploitation-based attacks can be mitigated through tight constraints on trust levels within a network. Systems on the outside of a firewall should never be absolutely trusted by systems on the inside of a firewall. Such trust should be limited to specific protocols and should be authenticated by something other than an IP address where possible. [2]

Port Redirection - Port redirection attacks are a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. Consider a firewall with three interfaces and a host on each interface. The host on the outside can reach the host on the public services segment, but not the host on the inside. This publicly accessible segment is commonly referred to as a Demilitarized Zone (DMZ). The host on the public services segment can reach the host on both the outside and the inside. If hackers were able to compromise the public services segment host, they could install software to redirect traffic from the outside host directly to the inside host. Though neither communication violates the rules implemented in the firewall, the outside host has now achieved connectivity to the inside host through the port redirection process on the public services host. An example of an application that can provide this type of access is netcat. Port redirection can be mitigated primarily through the use of proper trust models, which are network specific (as mentioned earlier). Assuming a system under attack, a host-based IDS can help detect a hacker and prevent installation of such utilities on a host. [2]

Man-in-the-middle Attack - A man-in-the-middle attack requires that the hacker have access to network packets that come across a network. An example could be someone who is working for an Internet service provider (ISP) and has access to all network packets transferred between the ISP network and any other network.

Such attacks are often implemented using network packet sniffers and routing and transport protocols. The possible uses of such attacks are theft of information, hijacking of an ongoing session to gain access to private network resources, traffic analysis to derive information about a network and its users, Denial of Service (DoS), corruption of transmitted data, and introduction of new information into network sessions. Man-in-the-middle attack mitigation is achieved by encrypting traffic in an IPSec tunnel, which would allow the hacker to see only cipher text [10].

Denial of service attacks - Certainly the most publicized form of attack, DoS attacks are also among the most difficult to completely eliminate. Even within the hacker community, DoS attacks are regarded as trivial and considered bad form because they require so little effort to execute. Still, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators. If you are interested in learning more about DoS attacks, researching the methods employed by some of the better-known attacks can be useful. DoS attacks take many forms. Ultimately, they prevent authorized people from using a service by using up system resources. The following are some examples of common DoS threats [6]:

- **Ping of death** – This attack modifies the IP portion of the header, indicating that there is more data in the packet than there actually is, causing the receiving system to crash.
- **SYN flood attack** – This attack randomly opens up many TCP ports, tying up the network equipment or computer with so many bogus requests that sessions are thereby denied to others. This attack is accomplished with protocol analyzers or other programs.

- **Packet fragmentation and reassembly** – This attack exploits a buffer–overrun bug in hosts or internetworking equipment.
- **E-mail bombs** – Programs can send bulk e-mails to individuals, lists, or domains, monopolizing e-mail services.
- **CPU hogging** – These attacks constitute programs such as Trojan horses or viruses that tie up CPU cycles, memory, or other resources.
- **Malicious applets** – These attacks are Java, JavaScript, or ActiveX programs that act as Trojan horses or viruses to cause destruction or tie up computer resources.
- **Misconfiguring routers** – Misconfiguring routers to reroute traffic disables web traffic.
- **The chargen attack** – This attack establishes a connection between UDP services, producing a high character output. The host chargen service is connected to the echo service on the same or different systems, causing congestion on the network with echoed chargen traffic.
- **Out-of-band attacks such as WinNuke** – These attacks send out-of-band data to port 139 on Windows 95 or Windows NT machines. The attacker needs the victim’s IP address to launch this attack.
- **Denial of Service** – DoS can occur accidentally because of misconfigurations or misuse by legitimate users or system administrators.
- **Land.c** – This program sends a TCP SYN packet that specifies the target host address as both source and destination. The program also uses the same port (such as 113 or 139) on the target host as both source and destination, causing the target system to stop functioning.
- **Teardrop.c** – In this attack, the fragmentation process of the IP is implemented in such a way that reassembly problems can cause machines to crash.
- **Targa.c** – This attack is a multi-platform DoS attack that integrates bonk, jolt, land, nestea, netear, syndrop, teardrop, and winnuke all into one exploit.

Masquerade/IP Spoofing - With a masquerade attack, the network intruder can manipulate TCP/IP packets by IP spoofing, falsifying the source IP address, and thereby appearing to be another user. The intruder assumes the identity of a valid user and gains that user’s access privileges by IP spoofing. IP spoofing occurs when intruders create IP data packets with falsified source addresses. During an IP spoofing attack, an attacker outside the network pretends to be a trusted computer. The attacker may either use an IP address that is within the range of IP addresses for the network or use an authorized external IP address that is trusted and provides access to specified resources on the network. Normally, an IP spoofing attack is limited to the injection of data or commands into an existing stream of data passed between a client and server application or a peer-to-peer network connection. The attacker simply does not worry about receiving any response from the applications. To enable bi-directional communication, the attacker must change all routing tables to point to the spoofed IP address. Another approach the attacker could take is to simply not worry about receiving any response from the applications. If an attacker manages to change the routing tables they can receive all of the network packets that are addressed to the spoofed address, and reply just as any trusted user can. Like packet sniffers, IP spoofing is not restricted to people who are external to the network. [2]

Some tools used to perform IP spoofing attacks are as follows [6]:

- Protocol analyzers, also called password sniffers
- Sequence number modification
- Scanning tools that probe TCP ports for specific services, network or system architecture, and the OS

After obtaining information through scanning tools, the intruder looks for vulnerabilities associated with those entities.

2. Literature review

2.1. Fundamental security on routers and switches

Routers can support a large number of network services that allow users and host processes to connect to the network. Some of these services can be restricted or disabled, improving security without affecting the operational use of the network. For security purposes, it should be a common practice for network devices to only support the traffic and protocols the network needs.
In addition to a general overview of security issues, this study also provides hands-on labs for essential skills such as configuring router privileges and accounts, disabling and controlling TCP/IP services, configuring routing protocol authentication, and Secure Shell (SSH). [7]

This study will also discuss access control lists (ACLs) and how they are handled by the Router IOS with firewall enhanced features or PIX Security Appliance. The first part of this chapter will focus on configuring ACLs and knowing how and when to use ACLs in different network environments. The reader will learn when to use this technology and why it is necessary.

2.2. Control access to network devices

Secure configurations are necessary to protect access to routers and switches. Anyone who can log in to a router or switch can display information that should not be made available to the general public. It is important to realize that any router or switch, by default, is an open system. A user who can log in may be able to use the device as a relay for further network attacks. Anyone who can obtain privileged access to the router or switch can reconfigure it. To prevent inappropriate access, administrators need to control logins. Although most access is disabled by default, there are exceptions. They are sessions from directly connected, asynchronous terminals, such as the console terminal, and sessions from integrated modem lines. [7]

Console Ports - The console port of an IOS device has special privileges. In particular, if a **Break** or **Ctrl-Break** signal is sent to the console port during the first few seconds after a reboot, the password recovery procedure can easily be used to take control of the system. Attackers who can interrupt power or induce a system crash, and who have access to the console port via a hardwired terminal, a modem, a terminal server, or some other network device, can take control of the system, even if they do not have physical access to it or the ability to log in to it normally. It follows that any modem or network device that gives access to the console port must be secured to the same degree as the router. At a bare minimum, any console modem should require the dialup user to supply a password for access, and the modem password should be carefully managed. [7]

General Access - There are more ways of connecting to routers than users may realize. Cisco IOS software, depending on the configuration and software version, may support connections through Telnet, rlogin, SSH, non-IP-based network protocols like LAT, MOP, X.29, and V.120. Connections may also be supported by way of local asynchronous connections or modem dial-ins. Additional protocols for access are always being added. Telnet access occurs not only on the standard TCP port 23, but on a variety of higher-numbered ports as well. The best way to protect a system is to make certain that appropriate controls are applied on all lines, including *vty* lines and *tty* lines. Administrators should usually make sure that logins on all lines are controlled using some sort of authentication mechanism, even on machines that are supposed to be inaccessible from untrusted networks. This is especially important for vty lines and for lines connected to modems or other remote access devices. Logins may be completely prevented on any line by configuring the router with the ***login*** and ***no password*** commands. This is the default configuration for vtys, but not for ttys. There are many ways to configure passwords and other forms of user authentication for tty and vty lines. Controlling TTYs and AUX Local asynchronous terminals are less common than they once were, but they still exist in some installations. Even if the terminals are physically secured, the router should be configured to require users on local asynchronous terminals to log in before using the system. Most tty ports in modern routers are either connected to external modems, or are implemented by integrated modems. Securing these ports is even more important than securing local terminal ports.

Controlling VTYs - Any vty should be configured to accept connections only with the protocols actually needed. This is done with the ***transport input*** command. For example, a vty that was expected to receive only Telnet sessions would be configured with ***transport input telnet***, while a vty permitting both Telnet and SSH sessions would have ***transport input telnet ssh***. If the software supports an encrypted access protocol such as SSH, it may be wise to enable only that protocol, and to disable Telnet. It is also a good idea to use the ***ip access-class*** command to restrict the IP addresses from which the vty will accept connections. A Cisco IOS device has a limited number of vty lines, usually five. When all of the vtys are in use, no more additional remote connections can be established. This creates the opportunity for a DoS attack. If an attacker can open remote sessions to all the vtys on the system, the legitimate administrator may not be able to log in. The attacker does not have to log in to do this. The sessions can simply be left at the login prompt. One way of reducing this exposure is to configure a more restrictive ***ip access-class*** command on the last vty line in the system. The last vty might be restricted to accept connections only from a single, specific administrative workstation, whereas the other vtys might accept connections from any address in a corporate network. Another useful tactic is to configure vty timeouts using the ***exec-timeout*** command. This prevents an idle session from consuming the vty line indefinitely. Although its effectiveness against deliberate attacks is relatively limited, it also provides some protection against sessions accidentally left idle. Similarly, enabling Transmission Control Protocol (TCP) keepalives on incoming connections, using the ***service tcp-keepalives-in*** command, can help guard against both malicious attacks and orphaned sessions caused by remote system crashes. Disabling all non-IP-based remote access protocols, and using SSH, SSL, or IP Security (IPSec) encryption for all remote connections to the router can provide complete vty protection. [1]

2.3. Remote configuration using SSH

Having remote access to network devices is critical for effectively managing a network. Traditionally, Cisco IOS supports Telnet, which allows users to connect to a remote router using TCP port 23. However, this method provides no security because all Telnet traffic goes over the network in clear text. Secure Shell (SSH) replaces Telnet to provide remote router administration with connections that support strong privacy and session integrity. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, SSH allows for secure communications over an insecure network.

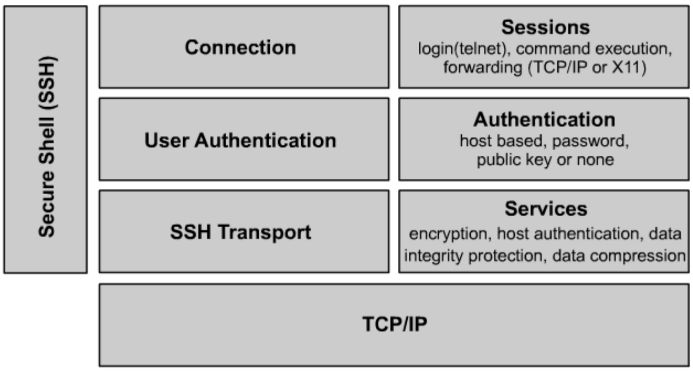

Secure Shell (SSH)
Connection
Sessions
login(telnet), command execution, forwarding (TCP/IP or X11)
User Authentication
Authentication
host based, password, public key or none
SSH Transport
Services
encryption, host authentication, data integrity protection, data compression
TCP/IP

Figure 5. Components that make up SSH [4]

There are currently two versions of SSH available, SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2). SSH was introduced into IOS platforms/images in the following sequence [4]:

- SSHv1 server was introduced in some IOS platforms/images starting in 12.1.(1)T.
- SSHv1 client was introduced in some IOS platforms/images starting in 12.1.(3).T.
- SSHv1 terminal-line access, also known as reverse-Telnet, was introduced in some IOS platforms/images starting in 12.2.(2).T.
- SSHv2 was introduced into 12.3(4)T.

The SSH terminal-line access feature enables users to configure their router with secure access and perform the following tasks [7]:

- Connect to a router that has multiple terminal lines connected to consoles or serial ports of other routers, switches, or devices
- Simplify connectivity to a router from anywhere by securely connecting to the terminal server on a specific line
- Allow modems attached to routers to be used for dial-out securely
- Require authentication to each of the lines through a locally defined username and password, TACACS+, or RADIUS

Cisco routers are capable of acting as the SSH client and server. By default, both of these functions are enabled on the router when SSH is enabled. These two functions are detailed in the following sections.

SSH Client - The SSHv1 Integrated Client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco router or other SSH client to make a secure, encrypted connection to another Cisco router or to any other device running the SSHv1 server. The SSH client in Cisco IOS software works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), Triple DES (3DES), and password authentication. User authentication is performed like that in the telnet session to the router. The user authentication mechanisms supported for SSH are RADIUS, TACACS+, and the use of locally stored user names and passwords. [7]

SSH Server - When the SSH server function is enabled on a Cisco router or other device, an SSH client is able to make a secure, encrypted connection to that router or device. The SSH server in Cisco IOS will work with publicly and commercially available SSH clients as well as other Cisco routers that have SSH enabled. When SSH is enabled on a Cisco Router, it acts as both a client and a server by default. The Secure Copy Protocol (SCP) feature that is provided with SSH also allows for the secure transfer of configuration and image files. [7]

2.4. Password administration

Passwords are the most critical tools in controlling access to a router. There are two password protection schemes in Cisco IOS [4]:

1. Type 7 uses the Cisco-defined encryption algorithm, which is not as strong as Type 5 encryption.
2. Type 5 uses an MD5 hash, which is much stronger. Cisco recommends that Type 5 encryption be used instead of Type 7 where possible. Type 7 encryption is used by the ***enable password***, ***username***, and ***line password*** commands.

To protect the privileged EXEC level as much as possible, do not use the enable password command. Use the ***enable secret*** command. Even if the ***enable secret*** is set, do not set the ***enable*** password because it will not be used and may give away a system password. No user account should be created above privilege level 1 since it is not possible to use Type 5 encryption on the default EXEC login or the ***username*** command. User accounts should be created for auditing purposes. The ***username*** command should be used to create individual user accounts at the EXEC level and then the higher privilege levels should be protected with the ***enable secret*** password. Users with a need to work at higher levels would be given the higher privilege level password. If the ***login*** command is used to protect a line, then the ***password*** command is the only way to set a password on a line. But if the ***login*** **local** command is used to protect a line then the specified user name and password pair is used. For access and logging reasons use the ***login local*** command. The privileged EXEC secret password should not match any other user password. Do not set any user or line password to the same value as any ***enable secret*** password. The ***service password-encryption*** command will keep passersby from reading passwords that are displayed on the screen. Be aware that there are some secret values that ***service password-encryption*** does not protect. Never set any of these secret values to the same string as any other password. [7]

Cisco IOS Software Release 12.3(1) and greater allow administrators to set the minimum character length for all router passwords using the ***security passwords*** global configuration command, as shown in the figure. This command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as "lab" and "cisco." This command affects user passwords, enable passwords and secrets, and line passwords created after the command was executed (existing router passwords remain unaffected). [7]

By default, Cisco IOS routers allow a break sequence during power up, forcing the router into ROMMON mode. Once the router is in ROMMON mode, anyone can choose to enter a new enable secret password using the well-known Cisco password recovery procedure. This procedure, if performed correctly, leaves the router configuration intact. This scenario presents a potential security breach in that anyone who gains physical access to the router console port can enter ROMMON, reset the enable secret password, and discover the router configuration. [3]

This potential security breach can be mitigated using the **no *service password-recovery*** global configuration command

2.5. IOS network services

Cisco routers support a large number of network services at layers 2, 3, 4, and 7. Some of these services are application layer protocols that allow users and host processes to connect to the router. Others are automatic processes and settings intended to support legacy or specialized configurations, which are detrimental to security. Some of these services can be restricted or disabled to improve security without degrading the operational use of the router. General security practice for routers should be to support only traffic and protocols a network needs. Most of the services listed in this section are not needed. Turning off a network service on the router itself does not prevent it from supporting a network where that protocol is employed. For example, a router may support a network where the bootp protocol is employed, but some other host is acting as the bootp server. Bootp is a user datagram protocol (UDP) that can be used by Cisco routers to access copies of IOS on another Cisco router running the Bootp service. In this case, the bootp server on the router should be disabled. In many cases, Cisco IOS supports turning a service off entirely, or restricting access to particular network segments or sets of hosts. If a particular portion of a network needs a service but the rest does not, then the restriction features should be employed to limit the scope of the service. Turning off an automatic network feature usually prevents a certain kind of network traffic from being processed by the router or prevents it from traversing the router. For example, IP source routing is a little-used feature of IP that can be utilized in network attacks. Unless it is required for the network to operate, IP source routing should be disabled. [6]

Start by running the ***show proc*** command on the router. Next, turn off clearly unneeded facilities and services. Some services that should almost always be turned off and the corresponding commands to disable them are as follows: [6]

- Small services such as echo, discard, and chargen – ***no service tcp-small-servers*** or ***no service udp-small-servers***
- BOOTP – ***no ip bootp server***
- Finger – ***no service finger***
- Hypertext Transfer Protocol (HTTP) – ***no ip http server***
- Simple Network Management Protocol (SNMP) – ***no snmp-server***

It is also important to shut down services that allow certain packets to pass through the router, send special packets, or are used for remote router configuration. The corresponding commands to disable them are as follows: [6]

- Cisco Discovery Protocol (CDP) – ***no cdp run***
- Remote configuration. – ***no service config***
- Source routing – ***no ip source-route***
- Classless routing – ***no ip classless***

The interfaces on the router can be made more secure by using certain commands in the Configure Interface mode. These commands should be applied to every interface: [6]

- Unused interfaces – ***shutdown***
- No SMURF attacks – ***no ip directed-broadcast***
- Ad-hoc routing – ***no ip proxy-arp***

2.6. Routing, proxy ARP and ICMP

IP Source Routing- Source routing is a feature of IP whereby individual packets can specify routes. This feature is used in several kinds of attacks. Cisco routers normally accept and process source routes. Unless a network depends on source routing, it should be disabled on all network routers in the network [8].

Proxy ARP - Network hosts use the Address Resolution Protocol (ARP) to translate network addresses into MAC addresses. Normally, ARP transactions are confined to a particular LAN segment. A Cisco router can act as an intermediary for ARP, responding to ARP queries on selected interfaces and thus enabling transparent access between multiple LAN segments. This service is called proxy ARP. Proxy ARP should be used only between two LAN segments at the same trust level, and only when absolutely necessary to support legacy network architectures. Cisco routers perform proxy ARP by default on all IP interfaces. Disable it on each interface where it is not needed, even on interfaces that are currently idle, using the interface configuration command ***no ip proxy-arp***. [8]

IP Directed Broadcast - Directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment. This technique was used in some old DoS attacks, and the default Cisco IOS configuration is to reject directed broadcasts. Explicitly disable directed broadcasts on each interface using the interface configuration command **no *ip directed-broadcast***. [8]

IP Classless Routing - By default, a Cisco router will make an attempt to route almost any IP packet. If a packet arrives addressed to a subnet of a network with no default network route, then IOS will use IP classless routing to forward the packet along the best available route. This feature is often not needed. On routers where IP classless routing is not needed, disable it. [8]

IP Unreachables, Redirects and Mask Replies - The Internet Control Message Protocol (ICMP) supports IP traffic by relaying information about paths, routes, and network conditions. Cisco routers automatically send ICMP messages under a wide variety of conditions. Attackers for network mapping and diagnosis commonly use three ICMP messages: [3]

1. Host unreachable
2. Redirect
3. Mask Reply

2.7. CAM table overflow attack

Let's say the machine that belongs to the attacker is on VLAN 10. The attacker floods MAC addresses to port 3/25 on the switch. When the content addressable memory (CAM) table threshold is reached, the switch operates as a hub and simply floods traffic out all ports. This flooding also occurs on adjacent switches configured with VLAN 10, however flooding is limited to only the source VLAN and does not affect other VLANs.

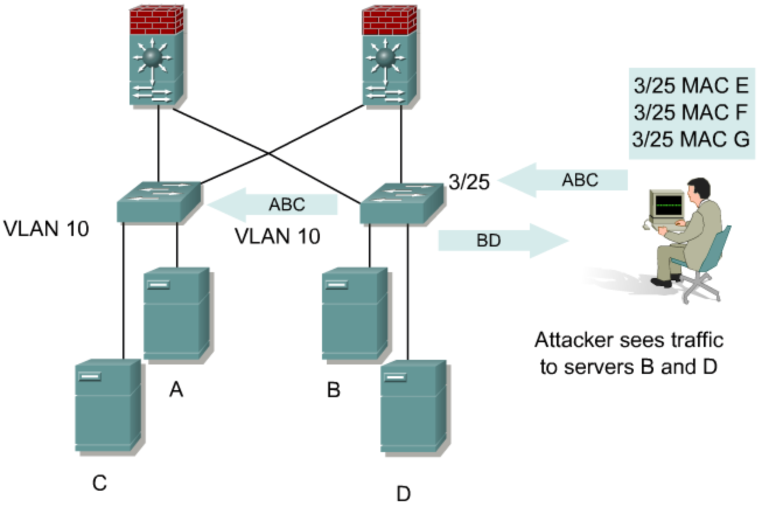


Figure 6. CAM table overflow attack[7]

MAC Flooding - MAC flooding is the attempt to exploit the fixed hardware limitations of the CAM table of a switch. The Catalyst switch CAM table stores the source MAC address and the associated port of each device connected to the switch. The CAM table on the Catalyst 6000 can contain 128,000 entries. These 128,000 entries are organized as 8 pages that can store approximately 16,000 entries. A 17 bit hash algorithm is used to place each entry in the CAM table. If the hash results in the same value, each entry is stored on separate pages. Once these eight locations are full, the traffic is flooded out all ports on the same VLAN on which the source traffic is being received.

CAM tables are limited in size. If enough entries are entered into the CAM table before other entries are expired, the CAM table fills up to the point that no new entries can be accepted. Typically a network intruder will flood the switch with a large number of invalid-source MAC addresses until the CAM table fills up. When that occurs, the switch will flood all ports with incoming traffic because it cannot find the port number for a particular MAC address in the CAM table. The switch, in essence, acts like a hub. If the intruder does not maintain the flood of invalid-source MAC addresses, the switch will eventually time out older MAC address entries from the CAM table and begin to act like a switch again. CAM table overflow only floods traffic within the local VLAN so the intruder will see only traffic within the local VLAN to which he or she is connected [6].

2.8. Routing protocol authentication and update filtering

An unprotected router or routing domain is an easy target for any network-savvy adversary. For example, an attacker who sends false routing update packets to an unprotected router can easily corrupt its routing table. This enables the attacker to re-route network traffic as desired. The key to preventing this type of an attack is to protect the routing tables from unauthorized and malicious changes.

There are two basic approaches available for protecting routing table integrity:

- Use only static routes: This may work in small networks, but is unsuitable for large networks.
- Authenticate route table updates: By using routing protocols with authentication, network administrators can deter attacks based on unauthorized routing changes. Authenticated router updates ensure that the update messages come from legitimate sources. Bogus messages are automatically discarded.

Another attack involves preventing router update messages from being sent or received, which will result in bringing down parts of a network. To resist such attacks and recover from them quickly, routers need rapid convergence and backup routes. Routing protocol authentication is vulnerable to eavesdropping and spoofing of routing updates. Message Digest 5 (MD5) authentication of routing protocol updates prevents the introduction of unauthorized or false routing messages from unknown sources. [8]

Cisco IOS software supports the use of MD5 authentication of routing protocol updates for the following protocols:

- OSPF
- RIPv2
- Enhanced IGRP
- BGP

The ***key-string*** command defines the MD5 key that is used to create the message digest, or hash, that is exchanged with the opposite router. It is possible to specify the time period during which the key can be received and sent with the ***accept-lifetime*** and ***send-***

lifetime commands. Static routes are manually configured on the router as the sole path to a given destination. In one sense, static routes are very secure. They are not vulnerable to spoofing attacks because they do not deal with router update packets. However, exclusively using static routes will make network administration extremely difficult. Also, configuring a large network to use only static routes can make the availability of large segments of the network subject to single points of failure. Static routes cannot handle events such as router failures. However, a dynamic routing protocol, such as OSPF, can correctly reroute traffic in the case of a router failure. [1]

Passive Interfaces - The ***passive-interface*** command is used to prevent other routers on the network from learning about routes dynamically. It can also be used to keep any unnecessary parties from learning about the existence of certain routes or routing protocols used. It is typically used when the wildcard specification on the network router configuration command configures more interfaces than desirable. [1]

2.9. MAC spoofing – man in the middle attacks

MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the targeted host to the network attacker. By sending a single frame with the source MAC address of the targeted host, the network attacker overwrites the CAM table entry so that the switch forwards packets destined for the targeted host to the network attacker. The targeted host will not receive any traffic until it sends traffic. When the targeted host sends out traffic, the CAM table entry is rewritten once more so that it associates the MAC address back to the original port.

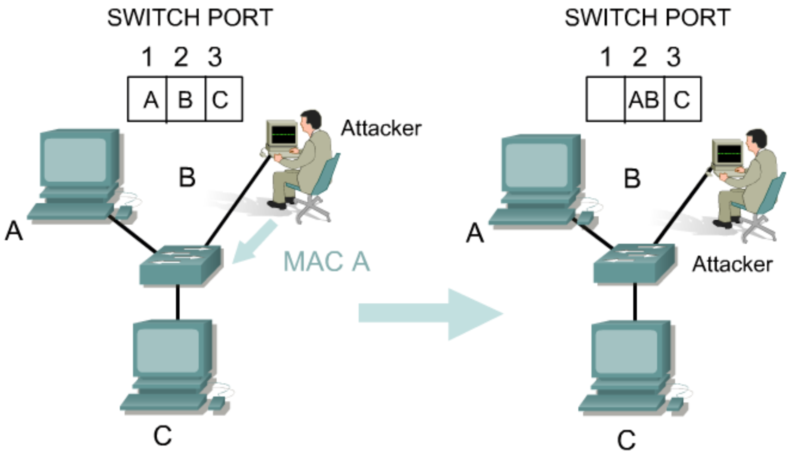


Figure 7. Man in the middle attacks [1]

2.10. NTP, SNMP, router name, DNS

NTP Service - Cisco routers and other hosts use the Network Time Protocol (NTP) to keep their time-of-day clocks accurate and in synchrony. If possible, configure all routers as part of an NTP hierarchy. If an NTP hierarchy is not available on the network, then disable NTP . Disabling NTP on an interface will not prevent NTP messages from traversing the router. To reject all NTP messages at a particular interface, use an access list.[7]

SNMP Services - The Simple Network Management Protocol (SNMP) is the standard Internet protocol for automated remote monitoring and administration. There are several different versions of SNMP with different security properties. If a network has an SNMP infrastructure in place for administration, then all routers on that network should be configured to securely participate in it. In the absence of a deployed SNMP scheme, all SNMP facilities on all routers should be disabled using the following steps: [7]

- Erase existing community strings, and set a hard-to-guess, read-only community string.
- Apply a simple IP access list to SNMP denying all traffic.
- Disable SNMP system shutdown and trap features.

Disable SNMP - It starts with listing the current configuration to find the SNMP community strings. The configuration listing is often quite long, but there is no other mechanism in Cisco IOS for viewing the configured SNMP community strings. The command ***no snmp-server*** shuts down all SNMP processing on the router. When SNMP processing is shut down, SNMP configuration will not appear in any listing of the running configuration, but it may still be there. [7]

Router Name and DNS Name Resolution - Cisco IOS supports looking up host names with the Domain Name System (DNS). DNS provides the mapping between names, such as central.mydomain.com to IP addresses, such as 14.2.9.250. Unfortunately, the basic DNS protocol offers no authentication or integrity assurance. By default, name queries are sent to the broadcast address 255.255.255.255. If one or more name servers are available on the network, and it is desirable to use names in IOS commands, then explicitly set the name server addresses using the global configuration command ***ip name-server*** addresses. Otherwise, turn off DNS name resolution with the command ***no ip domain-lookup*** . It is also a good idea to give the router a name, using the command ***hostname***. The name given to the router will appear in the prompt. [7]

3. Implementing fundamental security on routers and switches

3.1. Configuring privileges and accounts

Cisco IOS provides for 16 different privilege levels ranging from zero to 15. The Cisco IOS comes with two predefined user levels. User EXEC mode runs at privilege level 1, and the privileged EXEC mode runs at level 15. Every IOS command is pre-assigned to either level 1 or level 15. By default, Cisco provides user EXEC level 1 with a few commands that may, in terms of security, belong at a higher privilege level.

There are several considerations to keep in mind when customizing privilege levels [8]:

- Do not use the ***username*** command to set up accounts above level one. Instead, use the ***enable secret*** command to set a level password.
- Be very careful about moving too much access down from level 15, as this could cause unexpected security holes in the system.
- Be very careful about moving any part of the ***configure*** command down from level 15. Once a user has write access, they could leverage this to acquire greater access.

Configuration example:

```
Router# config t
Router (config)#  privilege exec level 15 connect
Router (config)#  privilege exec level 15 telnet
Router (config)#  privilege exec level 15 rlogin
Router (config)#  privilege exec level 15 show ip access-lists
Router (config)#  privilege exec level 15 show access-lists
Router (config)#  privilege exec level 15 show logging
Router (config)#  privilege exec level 1 show ip
Router (config)# username ffisteku password ciscopass
Router (config)# username ffisteku privilege 1
Router (config)# username ffisteku password 2B-or-3B
Router (config)# no username embiemri
Router (config)# end
Router #
```

3.2. Configuring ACLs

The actual configuration of the ACL on a Cisco IOS is relatively simple. An ACL is implemented using the ***access-list*** command and the ***access-group*** command. The ***access-list*** command is used to create an ACL, and the ***access-group*** command applies the ACL to the specific interface on the device. Keep in mind that only one ACL can be bound to an interface at a time using the ***access-group*** command. PIX ACLs differ from ACLs on Cisco IOS routers in that the PIX does not use a wildcard mask like Cisco IOS. It uses a regular subnet mask in the ACL definition. As with Cisco IOS routers, the PIX ACL has an implicit deny all at the end of the ACL. [7]

ACL Guidelines - Use the following guidelines for specifying a source, local or destination address [7]:

- Use a 32-bit address in four-part, dotted-decimal format
- Use the keyword *any* as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0
  This keyword is normally not recommended for use with IPSec
- Use the *host* keyword as an abbreviation for a mask of 255.255.255.0

Use the following guidelines for specifying a network mask:

- Do not specify a mask if the address is for a host/if the destination is for a host, use the host keyword before the address as shown in the following example:

  ```
  Router(config)# access-list acl_grp permit tcp any host 192.168.1.1
  ```

- If the address is a network address, specify the mask in 32-bit, four-part, dotted-decimal format. Place zeros in the bit positions that should be ignored
- Remember that the network mask is different than the mask used in the Cisco IOS software access-list command. With the PIX Security Appliance , 255.255.0.0 for a class B address, and 255.255.255.0 for a Class C address. If using a subnetted network address, use the appropriate network mask, as shown in the following example:

  ```
  access-list acl_grp permit tcp any 209.165.201.0 255.255.255.224
  ```

3.3. Using ACLs

In Figure 8. the ACL ***acl_inside*** is applied to the inside interface. The ACL ***acl_inside*** denies HTTP connections from an internal network, but let's all other IP traffic through. Applying an ACL to the inside interface restricts internal users from establishing outside web connections.

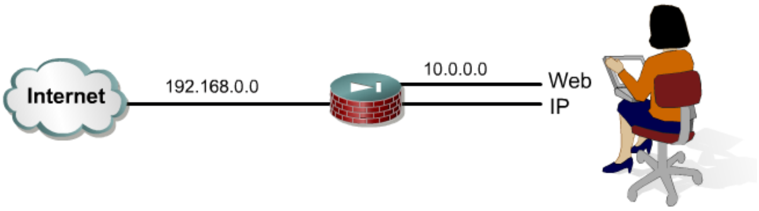


Figure 8. Using Inside ACL [7]

Show configuration example:

```
pixfirewall # write terminal
…..
access-list acl_inside deny tcp any any eq www
access-list acl_inside permit ip any any
access-group acl_inside in interface inside
nat (inside) 1 10.0.0.0 255.255.255.0
global (outside) 1 192.168.0.20-192.168.0.254 netmask 255.255.255.0
…..
```

NOTE: The internal network addresses, 10.0.0.0, are dynamically translated to the range 192.168.0.20 through 192.168.0.254 to allow outbound connections.

In Figure 10., the IP address of the web server is translated to an outside IP address of 192.168.0.11. The ACL acl_outside is applied to traffic inbound to the outside interface. The ACL acl_outside permits HTTP connections from the Internet to a public Internet web server, 192.168.0.11. All other IP traffic is denied access to the DMZ or inside networks.

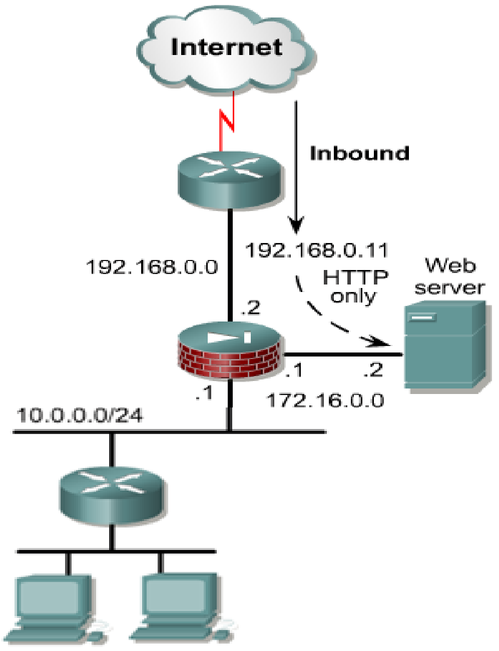


Figure 9. Using Outside ACL [8]

In Figure 9, the web server is statically translated from 172.16.0.2 to 172.18.0.17. The ACL acl_partner is applied to traffic inbound to the partnernet interface. The ACL acl_partner permits Web connections from the hosts on network 172.18.0.0/24 to the DMZ web server via its statically mapped address, 172.18.0.17. All other traffic from the Partner network is denied.

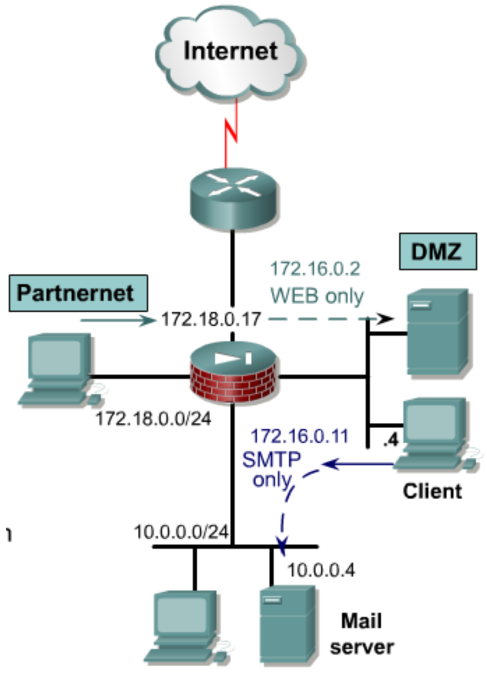


Figure 10. ACL denying selected traffic [8]

In the second scenario in Figure 10. the client on the DMZ is trying to connect to the mail server on the inside network. The mail server IP address is statically translated to 172.16.0.11 by the PIX Security Appliance. The ACL acl_dmz is applied to traffic inbound to the DMZ interface. The ACL acl_dmz permits the host 172.16.0.4 mail access to the internal mail server on the inside interface via the statically mapped address of the mail server, 172.16.0.11. All other traffic originating from the DMZ network is denied.

3.4. Mitigating the CAM table overflow attack

The CAM table-overflow attack can be mitigated by configuring port security on the switch. This option provides for either the specification of the MAC addresses on a particular switch port or the specification of the number of MAC addresses that can be learned by a switch port. When an invalid MAC address is detected on the port, the switch can either block the offending MAC address or shut down the port.

Specifying MAC addresses on switch ports is far too unmanageable a solution for a production environment. Limiting the number of MAC addresses on a switch port is manageable. A more administratively scalable solution would be the implementation of dynamic port security at the switch. To implement dynamic port security, specify a maximum number of MAC addresses that will be learned.

Port Security - Port security allows administrators to specify MAC addresses for each port or to permit a limited number of MAC addresses. When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or learned on the port. If a MAC address of a device attached to the port differs from the list of secure addresses, the port shuts down permanently, shuts down for a specified period of time, or drops incoming packets from the insecure host. The behavior of the port depends on how it is configured to respond to a security violator. The default behavior is to shut down permanently.

Cisco recommends to configure the port security feature to issue a ***shutdown*** instead of dropping packets from insecure hosts through the ***restrict*** option. The ***restrict*** option may fail under the load of an attack and the port is disabled anyway [4].

Configuration example:

```
Switch (config)# interface interface_id
Switch (config-if)# switchport mode access
Switch (config-if)# switchport port-security
Switch (config-if)# switchport port-security mac-addrss mac_address
Switch (config-if)# end
```

Verify the Port Security Configuration - There are two ways to check the port security configuration:

```
switch# show port-security interface interface_id
```

This command displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode.

```
switch# show port-security address
```

This command displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode.

To restrict traffic through a port by limiting and identifying MAC addresses of the stations allowed to access the port, perform the tasks shown below:

```
Switch (config) # interface interface_id
Switch (config-if) # switchport mode access
Switch (config-if) # switchport port-security
Switch (config-if) # switchport port-security violation {protect | restrict | shutdown}
Switch (config-if) # switchport port-security mac-address mac_address
Switch (config-if) # end
```

3.5. Mitigating MAC spoofing attacks

Use the ***port security*** interface configuration command to mitigate MAC spoofing attacks. The ***port security*** command provides the capability to specify the MAC address of the system connected to a particular port. The command also provides the ability to specify an action to take if a port security violation occurs. However, as with the CAM table overflow attack mitigation, specifying a MAC address on every port is an unmanageable solution. Hold-down timers in the interface configuration menu can be used to mitigate ARP spoofing attacks by setting the length of time an entry will stay in the ARP cache.

Configuration example posibilities:

```
Switch (config-if)#
port security max-mac-count {1-32}
```

```
Switch (config-if)#
port security action {shutdown|trap}
```

```
Switch (config-if)#
arp timeout seconds
```

3.6. Using dynamic ARP inspection to mitigate MAC spoofing attacks

Address Resolution Protocol (ARP) is used to map IP addressing to MAC addresses in a local area network segment where hosts of the same subnet reside. Normally, a host will send out a broadcast ARP request to find the MAC address of another host with a particular IP address and an ARP response will come from the host whose address matches the request. The requesting host will then cache this ARP response [1].

ARP Spoofing - Within the ARP protocol a provision is made for hosts to perform unsolicited ARP replies. The unsolicited ARP replies are called gratuitous ARPs (GARP). GARP can be exploited maliciously by an attacker to spoof the identity of an IP address on a LAN segment. Typically, this is used to spoof the identity between two hosts or all traffic to and from a default gateway in a Man in the Middle attack.

By crafting an ARP reply, a network attacker can make their system appear to be the destination host sought by the sender. The ARP reply causes the sender to store the MAC address of the attacking system in the ARP cache. This MAC address is also stored by the switch in its CAM table. In this way the network attacker has inserted the MAC address of his or her system into both the CAM table of the switch and the ARP cache of the sender. This allows the network attacker to intercept frames destined for the host that is being spoofed.

DHCP Snooping - A solution that can be used to mitigate various ARP-based network exploits is the use of DHCP snooping. DHCP Snooping provides security by filtering trusted DHCP messages and then using these messages to build and maintain a DHCP snooping binding table. DHCP Snooping considers DHCP messages originating from any user facing port that is not a DHCP server port or an uplink to a DHCP server as untrusted. From a DHCP Snooping perspective these untrusted, user-facing ports should not send DHCP server type responses such as DHCPOffer, DHCPAck, or DHCPNak.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives the adminstrator a way to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

DHCP Snooping Configuration Guidelines - These are the configuration guidelines for DHCP snooping.

- DHCP snooping must be enabled globally on the switch.
- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.
- Before configuring the DHCP information option on the switch, make sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude must be specified, or DHCP options for devices must be configured.

Configuration example:

```
Switch (config)# ip dhcp snooping
Switch (config)# ip dhcp snooping vlan vlan_id
Switch (config)# interface interface_id
Switch (config-if)# ip dhcp snooping trust
Switch (config-if)# ip dhcp snooping limit rate rate
Switch (config-if)# end
Switch # show ip dhcp snooping
```

The DHCP Snooping Binding Table - The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information corresponding to the local untrusted interfaces of a switch. The table does not have information about hosts interconnected with a trusted port because each interconnected switch has its own DHCP snooping binding table.

The ***show ip dhcp snooping binding*** command displays the DHCP snooping binding entries for a switch.

Dynamic ARP Inspection - Dynamic ARP Inspection (DAI) determines the validity of an ARP packet based on the valid MAC address to IP address bindings stored in a DHCP snooping database. Additionally, DAI can validate ARP packets based on user-configurable ACLs. This allows for the inspection of ARP packets for hosts using statically configured IP addresses. DAI allows for the use of per-port and VLAN Access Control Lists (VACLs) to limit ARP packets for specific IP addresses to specific MAC addresses.

3.7. DHCP starvation attacks

A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses . This is easily achieved with attack tools such as gobbler. If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers for a period of time. This is a simple resource starvation attack, similar to how a SYN flood is a starvation attack. The network attacker can then set up a rogue DHCP server on their system and respond to new DHCP requests from clients on the network.

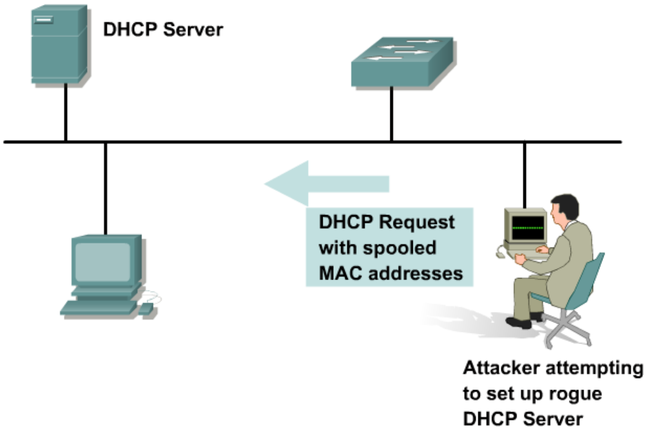

DHCP Server
DHCP Request with spooled MAC addresses
Attacker attempting to set up rogue DHCP Server

Figure 11. DHCP starvation attacks [8]

Exhausting all of the DHCP addresses is not required to introduce a rogue DHCP server. As stated in RFC 2131 [5]:

"*The client collects DHCPOFFER messages over a period of time, selects one DHCPOFFER message from the (possibly many) incoming DHCPOFFER messages (for example, the first DHCPOFFER message or the DHCPOFFER message from the previously used server) and extracts the server address from the `server identifier' option in the DHCPOFFER message. The time over which the client collects messages and the mechanism used to select one DHCPOFFER are implementation dependent.*"

By placing a rogue DHCP server on the network, a network attacker can provide clients with addresses and other network information. Since DHCP responses typically include default gateway and DNS server information, the network attacker can supply their own system as the default gateway and DNS server resulting in a man-in-the-middle attack.

3.8. Mitigating DHCP starvation attacks

The techniques that are used to mitigate CAM table flooding can also be used to mitigate DHCP starvation by limiting the number of MAC addresses on a switch port. As implementation of RFC 3118, Authentication for DHCP Messages, increases, DHCP starvation attacks will become more difficult. Additional features in the Catalyst family of switches, such as the DHCP snooping feature, can be used to help guard against a DHCP starvation attack. DHCP snooping is a security feature that filters untrusted DHCP messages and builds and maintains a DHCP snooping binding table. The binding table contains information such as the MAC address, IP address, lease time, binding type, VLAN number and the interface information corresponding to the local untrusted interfaces of a switch. Untrusted messages are those received from outside the network or firewall and untrusted switch interfaces are ones that are configured to receive such messages from outside the network or firewall. [7]

The following commands can be used to mitigate DHCP starvation attacks using DHCP snooping:

```
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan vlan_id {,vlan_id}
switch(config-if)# ip dhcp snooping trust
switch(config-if)# ip dhcp snooping limit rate rate
```

3.9. Private VLAN vulnerabilities

Private VLANs are a common mechanism to restrict communications between systems on the same logical IP subnet. Private VLANs work by limiting the ports within a VLAN that can communicate with other ports in the same VLAN. Isolated ports within a VLAN can communicate only with promiscuous ports. Community ports can communicate only with other members of the same community and promiscuous ports. Promiscuous ports can communicate with any port. One network attack capable of bypassing the network security of private VLANs involves the use of a proxy to bypass access restrictions to a private VLAN.

Private VLAN Proxy Attack - In this network attack against private VLANs, frames are forwarded to a host on the network connected to a promiscuous port, such as on a router. The network attacker sends a packet with the source IP and MAC address of their device, a destination IP address of the target system, but a destination MAC address of the router. The switch forwards the frame to the router. The router routes the traffic, rewrites the destination MAC address as that of the target, and sends the packet back out. Now the packet has the proper format and is forwarded to the target system. This network attack allows only for unidirectional traffic because any attempt by the target to send traffic back will be blocked by the private VLAN configuration. If both hosts are compromised, static ARP entries could be used to allow bidirectional traffic. This scenario is not a private VLAN vulnerability because all the rules of private VLANs were enforced. However, the network security was bypassed.

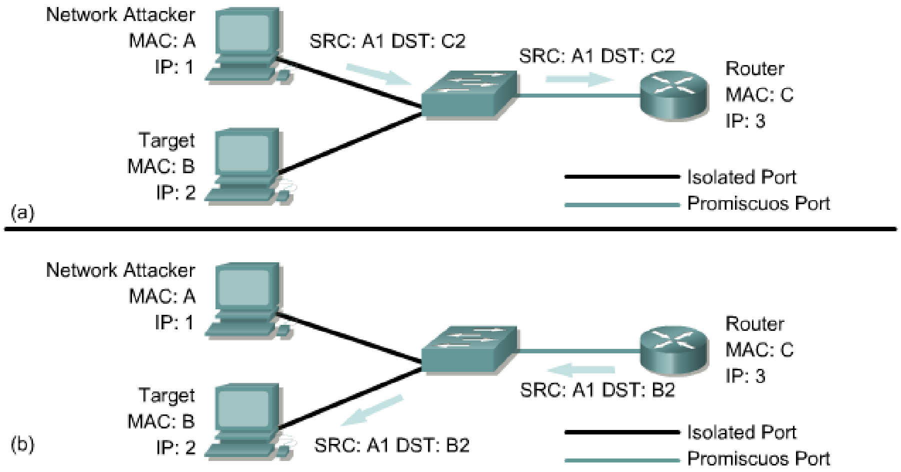


Figure 12. Private VLAN Proxy Attack [8]

3.10. Defending private VLANs

ACLs can be configured on the router port to mitigate private VLAN attacks. VLAN ACLs (VACLs) can also be used to help mitigate the effects of private VLAN attacks. An example of using ACLs on the router port is if a server farm segment were 172.16.34.0/24, then configuring the ACLs shown below on the default gateway would mitigate the private VLAN proxy attack.

```
Router (config) # access-list 101 deny 172.16.34.0 0.0.0.255 172.16.34.0 0.0.0.255 log
Router (config) # access-list 101 permit ip any any
Router (config) # interface fastethernet 0/1
Router (config-if) # ip access-group 101 in
Router (config-if) # end
```

4. Conclusion

In this report the author explained security aspects considering Layer 2 and Layer 3 of OSI model giving examples of implementation in computer networks. Earlier in the report, the author has explained the security networks determining vulnerabilities, threats and attacks on computer networks continuing with fundamental implementations at devices in order to prevent undesired activities from inside or outside the company.

The Internet continues to grow exponentially. As personal, government and business-critical applications become more prevalent on the Internet, there are many immediate benefits. However, these network-based applications and services can pose security risks to individuals as well as to the information resources of companies and government. In many cases, the rush to get connected comes at the expense of adequate network security. Information is an asset that must be protected. Without adequate protection or network security, many individuals, businesses, and governments are at risk of losing that asset.

Security risks cannot be eliminated or prevented completely. However, effective risk management and assessment can significantly minimize the existing security risks. An acceptable level of risk depends on how much risk the business is willing to assume. A security policy is an important component in deciding how this risk is managed. A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide. A security policy can be as simple as an acceptable use policy for network resources or it can be several hundred pages in length and detail every element of connectivity and associated policies.

Routers can support a large number of network services that allow users and host processes to connect to the network. Some of these services can be restricted or disabled, improving security without affecting the operational use of the network. For security purposes, it should be a common practice for network devices to only support the traffic and protocols the network needs.

Cisco Identity Based Networking Services (IBNS) is an integrated solution combining several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. The Cisco IBNS solution enables greater security while simultaneously offering cost-effective management of changes throughout the organization. Authentication proxy provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks which are not covered in this thesis.

Like routers, both Layer 2 and Layer 3 switches have their own sets of network security requirements. Unlike routers, however, there is not much public information available that discusses the network security risks in switches and what can be done to mitigate those risks.

5. References

[1]. Michael Watkins, Kevin Wallace. (July 2008). *CCNA Security Official Exam Certification Guide, Cisco Press.*

[2]. Myth or not: Most security breaches originate internally, date accessed 22 April 2012, http://www.techrepublic.com/blog/security/myth-or-not-most-security-breaches-originate-internally/1606

[3]. Classes of attacks, date accessed 13 April 2012, https://www.informit.com/articles/article.aspx?p=1151753&seqNum=2

[4]. Catherine Paquet, (September 2010). *Implementing Cisco IOS Network Security, 2nd Edition, Cisco Press.*

[5]. Internet Engineering Task Force – IETF, (March 1997). *Dynamic Host Configuration Protocol Request For Coments 2131, date accessed March 2012,* http://www.ietf.org/rfc/rfc2131.txt

[6]. Mark Ciampa, (November 2008). *Security+ Guide to Network Security Fundamentals, 3rd Edition, Course Technology.*

[7]. Antoon Rufi, (October 2006). *Network Security 1 Companion Guide, (Cisco Networking Academy Program), Cisco Press*

[8]. Antoon Rufi, (October 2006). *Network Security 2 Companion Guide, (Cisco Networking Academy Program), Cisco Press.*

[9]. Internet Engineering Task Force – IETF, (November 1998), *Security Architecture for the Internet Protocol Request For Comment 2401, date accessed April 2012.* http://www.rfc-editor.org/rfc/rfc2401.txt

[10]. Internet Engineering Task Force – IETF, (March 2004), *IPsec-Network Address Translation (NAT) Compatibility Requirements Request For Comments 3715, date accessed April 2012.* http://www.rfc-editor.org/rfc/rfc3715.txt

6. Appendixes

Packet Tracer Network Simulation Software

Packet Tracer is a medium fidelity, network-capable, simulation-based learning environment for networking novices to design, configure, and troubleshoot computer networks at a CCNA-level of complexity. Packet Tracer is an integrated simulation, visualization, collaboration, and assessment environment. Packet Tracer supports student and instructor creation of simulations, visualizations, and animations of networking phenomena. Like any simulation, Packet Tracer relies on a simplified model of networking devices and protocols. Real computer networks experienced both in-person/hands-on and remotely, remain the benchmark for understanding network behavior and developing networking skills. Packet Tracer was created to help address the Digital Divide in networking education, where many students and teachers lack access to equipment, bandwidth, and interactive modes of learning networking.

When you open Packet Tracer, by default you will be presented with the following interface as seen in the Figure 13:

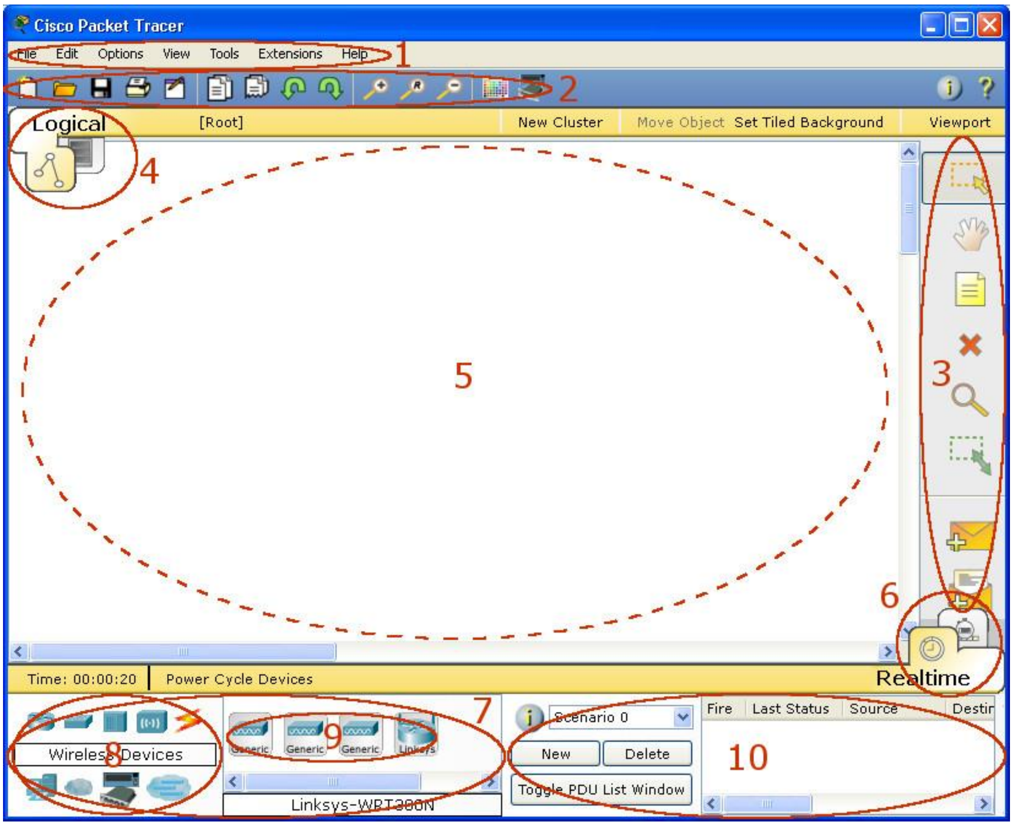


Figure 13. Packet Tracer Interface

This initial interface contains ten components. If you are unsure of what a particular interface item does, move your mouse over the item and a help balloon will explain the item. The table below explains the components of packet tracer interface.

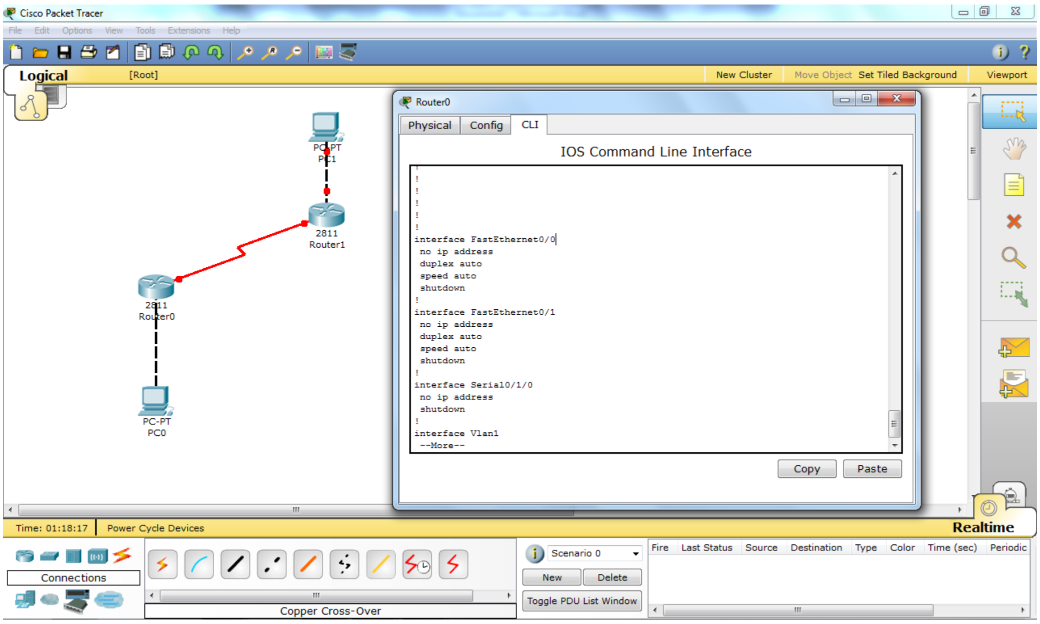
1	**Menu Bar**	This bar provides the **File**, **Edit**, **Options**, **View**, **Tools**, **Extensions**, and **Help** menus. You will find basic commands such as **Open**, **Save**, **Save as Pkz, Print**, and **Preferences** in these menus. You will also be able to access the **Activity Wizard** from the **Extensions** menu.
2	**Main Tool Bar**	This bar provides shortcut icons to the **File** and **Edit** menu commands. This bar also provides buttons for **Copy**, **Paste**, **Undo**, **Redo**, **Zoom**, the **Drawing Palette**, and the **Custom Devices Dialog**. On the right, you will also find the **Network Information** button, which you can use to enter a description for the current network (or any text you wish to include).
3	**Common Tools Bar**	This bar provides access to these commonly used workspace tools: **Select**, **Move Layout**, **Place Note**, **Delete**, **Inspect**, **Resize Shape**, **Add Simple PDU**, and **Add Complex PDU**. See "Workspace Basics" for more information.
4	**Logical/Physical Workspace and Navigation Bar**	You can toggle between the Physical Workspace and the Logical Workspace with the tabs on this bar. In Logical Workspace, this bar also allows you to go back to a previous level in a cluster, create a **New Cluster**, **Move Object**, **Set Tiled Background**, and **Viewport**. In Physical Workspace, this bar allows you to navigate through physical locations, create a **New City**, create a **New Building**, create a **New Closet**, **Move Object**, apply a **Grid** to the background, **Set Background**, and go to the **Working Closet**.
5	**Workspace**	This area is where you will create your network, watch simulations, and view many kinds of information and statistics.
6	**Realtime/Simulation Bar**	You can toggle between Realtime Mode and Simulation Mode with the tabs on this bar. This bar also provides buttons to **Power Cycle Devices** as well as the **Play Control** buttons and the **Event List** toggle button in Simulation Mode. Also, it contains a clock that displays the relative **Time** in Realtime Mode and Simulation Mode.
7	**Network Component**	This box is where you choose devices and

	Box	connections to put into the workspace. It contains the **Device-Type Selection** Box and the **Device-Specific Selection** Box.
8	**Device-Type Selection Box**	This box contains the type of devices and connections available in Packet Tracer. The **Device-Specific Selection** Box will change depending on which type of device you choose.
9	**Device-Specific Selection Box**	This box is where you choose specifically which devices you want to put in your network and which connections to make.
10	**User Created Packet Window**	This window manages the packets you put in the network during simulation scenarios. See the "Simulation Mode" section for more details.

Table 1. Components of Packet tracer interface

Packet Tracer has two workspaces (Logical and Physical) and two modes (Realtime and Simulation). Upon startup, you are in the Logical Workspace in Realtime Mode. You can build your network and see it run in real time in this configuration. You can switch to Simulation Mode to run controlled networking scenarios. You can also switch to the Physical Workspace to arrange the physical aspects (such as the location) of your devices. Note that you view a simulation while you are in the Physical Workspace. You should return to the Logical Workspace after you are done in the Physical Workspace.

All the basic configurations in this report are designed, implemented and test using Packet Tracer and the sample topology is given below.



```
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface Vlan1
 --More--
```

Figure 14. Sample topology presented with Packet Tracer Software

7. Glossary of terms

Router - is an internetworking device which operates at OSI Layer 3. A Router interconnects network segments or entire networks and passes data packets between networks based on Layer 3 information. The router, by default, is an open device. Services must be turned off or secured.

Switches – are devices which connect LAN segments, use a table of MAC addresses to determine the segment on which a datagram needs to be transmitted, and reduce traffic. Switches, which typically operate at Layer 2, can be categorized as stackable or chassis based.

Cisco Adaptive Security Appliance (ASA) 5500 Series - is a high-performance, multifunction security appliance family delivering converged firewall, IPS, network anti-virus and VPN services. As a key component of the Cisco Self-Defending Network, it provides proactive threat mitigation that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity while remaining cost-effective and easy-to-manage.

Cisco PIX Security Appliance Series – is a network device which delivers robust user and application policy enforcement, multi-vector attack protection, and secures connectivity services in cost-effective, easy-to-deploy solutions. Ranging from compact, plug-and-play desktop appliances for small and home offices to modular gigabit appliances with superior investment protection for enterprise and service-provider environments, Cisco PIX Security Appliances provide comprehensive security, performance, and reliability for network environments of all sizes.

Cisco IOS Firewall – is the Cisco IOS feature set which provides robust, integrated firewall, intrusion detection, and VPN functionality for every perimeter of the network. The Firewall feature set is available for most Cisco routers including the 1700, 1800, 2600, 2800, 3600, 3800, 7100, and 7200 series routers, however some features may not be available on low end and legacy router models.

Cisco Firewall Services Module (FWSM) - is a high-speed, integrated firewall module for Cisco Catalyst ® 6500 switches and Cisco 7600 Series routers, and provides a 5 Gbps throughput, 100,000 connections per second, and one million concurrent connections. Up to four FWSMs can be installed in a single chassis providing scalability to 20 Gbps per chassis. Based on Cisco PIX Security Appliance technology, the FWSM provides large enterprises and service providers with unmatched security, reliability, and performance within a switch chassis.

IPS Sensor - is a network appliance which monitors traffic flowing across a network segment. IPS Sensors detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse which match an attack signature.

Host based intrusion prevention software – is a software which should be installed on mission critical desktops and servers. Most of the attacks today are targeted towards public servers.

Mobile workers - can include staff within a company. Virtually every occupation and business has workers who are mobile.

End users - are workers who are connected to the network through a PC, laptop, or other mobile devices. Users are what drive the business. Without people, a business cannot survive. Unfortunately, they also can be responsible for security breaches. Some users carelessly use easy to guess passwords, write them on a note near the computer, or simple give their passwords when asked.

End User or Attacker -At one point, some end users can become the attacker. Many times, there is a fine line between network use and hacking, for example, a user in the marketing department accessing confidential data in the human resources department. Almost 75 percent of the network attacks come from inside the network.

Hacker – Hacker is a general term that has historically been used to describe a computer programming expert. More recently, this term is commonly used in a negative way to describe an individual that attempts to gain unauthorized access to network resources with malicious intent.

Cracker – Cracker is the term that is generally regarded as the more accurate word that is used to describe an individual that attempts to gain unauthorized access to network resources with malicious intent.

Phreaker – A phreaker is an individual that manipulates the phone network in order to cause it to perform a function that is normally not allowed. A common goal of phreaking is breaking into the phone network, usually through a payphone, to make free long distance calls.

Spammer – A spammer is an individual that sends large quantities of unsolicited email messages. Spammers often use viruses to take control of home computers in order to use these computers to send out their bulk messages.

Phisher – A Phisher uses email or other means in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords. The Phisher will masquerade as a trusted party that would have a legitimate need for the sensitive information.

White hat – White hat is a term used to describe individuals that use their abilities to find vulnerabilities in systems or networks, and then report these vulnerabilities to the owners of the system so that they can be fixed.

Black hat – Black hat is another term for individuals that use their knowledge of computer systems to break into systems or networks that they are not authorized to use.

- END -