Department of Electronics and Communications Engineering

SECURING A NETWORK BY USING VLAN, PORT SECURITY AND ACCESS CONTROL LIST

Prepared By

Md. Asif Raihan

ID: 2011-1-55-038

Marzia Afroze

ID: 2012-2-55-020

Dept. of ECE

East West University

Supervised By

Md. Asif Hossain

Assistant Professor, Dept. of ECE

December 2016

Letter of Transmittal

To
Md. Asif Hossain
Assistant Professor
Department of Electronics and Communication Engineering
East West University

Subject: Submission of Project Report

Dear Sir,

We are pleased to let you know that we have completed our project on **"Securing a Network by Using VLAN, Port Security and Access Control List"**. This project that has been prepared for your evaluation and consideration. Working on this project we have gained lots of practical knowledge. This knowledge is the reflection of the knowledge that we have learnt in the whole ungraduated period from you and the other honorable faculty members of EWU. This project work would be a great help for us in future.

We are very grateful to you for your guidance and supervision which helped us a lot to complete our project and acquire practical knowledge.

Thanking You.

Yours Sincerely

Md. Asif Raihan
ID: 2011-1-55-038

Marzia Afroze
ID: 2012-2-55-020

Dept. of ECE
East West University

Declaration

This is certified that the project is done by us under the course "Thesis (ETE-498)". The thesis of **"Securing a Network by Using VLAN, Port Security and Access Control List"** has not been submitted elsewhere for the requirement of any degree or any other purpose except for publication.

Md. Asif Raihan
ID: 2011-1-55-038

Marzia Afroze
ID: 2012-2-55-020

Acceptance

This thesis paper is submitted to the **Department of Electronics and Communications Engineering, East West University** is submitted in partial fulfillment of the requirements for the degree of **B.Sc.** in **Electronics & Telecommunications Engineering** under complete supervision of the undersigned.

_____

Md. Asif Hossain
Assistant Professor
Dept. of ECE
East West University

Abstract

Any communication network is vulnerable with various security threats. Among them unauthorized access is one the major examples. To mitigate such threats there are several mechanisms used in networking. In this project, virtual LAN, port security of the switches, inter VLAN routing and the access control list in router have been used. They have been simulated in packet tracer 6.3 software. It has been found that applying these techniques improve the network security significantly.

Keywords: VLAN, switch port security, ACL, network security threats, packet tracer etc.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues [1]. The evolution of networking and the Internet, the threats to information and networks have risen dramatically. Many of these threats have become cleverly exercised attacks causing damage or committing theft. Gaining the unauthorized access of the network is one the great threats on the network. 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 [2].

Without adequate protection or network security, many individuals, businesses, and governments are at risk of losing that asset. 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. A router is similar to many computers in that it has many services enabled by default. Many of these services are unnecessary and may be used by an attacker for information gathering or for exploitation. All unnecessary services should be disabled in the router configuration to prevent the attacker from using it to damage the network or to stealing the important information, or network devices configuration. In this project a review of attacks on routers, and how can prevent, or mitigating it will be described. Routers and switch are very critical parts of network operations and network security. Careful management and diligent audit of router and switch operations, can reduce network downtime, improve security, prevent the attacks and hackers, network threats decrease, and aid in the analysis of suspected security breaches. We have implemented VLAN, port security and ACL (access Control List) on the router. For the simulation purpose, we have used Cisco's Packet Tracer 6.3.

CHAPTER 2

NETWORK SECURITY ISSUES

Security has one purpose, to protect assets. 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. 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.

Network security is the most vital component in information security because it is responsible for securing all information passed through networked computers [3, 4]. Network security refers to all hardware and software functions, characteristics, features, operational procedures, accountability measures, access controls, administrative and management policy required to provide an acceptable level of protection for hardware, software, and information in a network. Network security, in order for it to be successful in preventing information loss, must follow three fundamental precepts. First, a secure network must have integrity such that all of the information stored therein is always correct and protected against fortuitous data corruption as well as willful alterations. Next, to secure a network there must be confidentiality, or the ability to share information on the network with only those people for whom the viewing is intended. Finally, network security requires availability of information to its necessary recipients at the predetermined times without exception. The three principles that network security must adhere to evolved from years of practice and experimentation that make up network history.

Real-world security includes prevention, detection, and response. If the prevention mechanisms were perfect, we wouldn't need detection and response. But no prevention mechanism is perfect. Without detection and response, the prevention mechanisms only have limited value. Detection and response are not only more cost effective but also more effective than piling on more prevention. On the Internet, this translates to monitoring. In Network Protection, there are fortunately many preventative techniques to properly secure network against threats. The first method of protection is to address the actual physical layer of the network to assure that it is

properly equipped. Next, three network administrative guidelines should be adhered to [5, 6].

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message. When developing a secure network, the following need to be considered [7]:

1. Access – authorized users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack [8]. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor.

Additionally, firewalls and encryption should be incorporated into a network to heighten its security. Finally, several other passwords, variations of capital and small letters further increase the strength of a password. Proper authentication is an integral part of the administrative step in securing a network. Firewalls are yet another measure used in increasing the level of security in a network. A firewall is in essence a portal through which information enters and exits. On one side of the portal is the internal network that must remain secure, and on the other is the information needed from the outside world combined with the undesirable threats of external networks. Three of the major types of firewalls, listed in order of increasing quality and price, are packet-filtering routers, application-level gateways, and circuit-level gateways. Although it is not the best available firewall, a positive step in increasing network security is the use of packet-

filtering routers. A packet filtering router allows the network to determine which connections can pass through the router into the local area network and which connections will be denied. The application-level gateway is designed specifically as a firewall that authenticates the user for individual applications. Its primary function is to identify and validate the user and then provide access to specific applications such as E-Mail or file browsers depending on which one the user is requesting. Finally, a circuit-level gateway performs all of the packet-filtering that a router does and a bit more. The primary enhancement is the use of identification and authentication before an insider can access our in-house network.

User Authorization: Resource Access Permission

Authorization defines users' permissions in terms of access to digital resources and extent of its usage. Authorization is granted to the successfully authenticate users according to his/her rights information available in the Access Management System (AMS) (Lynch, 2009). Authorization also addresses the issue of responsibilities assigned to different personnel involved in development of a digital repository/library and their respective authorities in terms of addition, deletion, editing and uploading of records into a digital collection. Authorization is more challenging than authentication, especially for widely distributed digital content providers.

Conventional access control architecture denotes an access control policy as a subject (user) is authorized to exercise some permission on an object. This usual model implicitly assumes that the user population is known more or less. But in a digital content environment the user population is vast, dynamic and impossible to predict all the users. Thus conventional authorization or access control mechanisms that rely on knowing the user and associating permissions with them fail significantly in digital repositories. So, this digital environment demands some further challenge for access control (Bertino, 2002). The access control policies are often based on user qualifications and characteristics. In one of the early works on access control in digital repositories or libraries, Gladney (1997) proposes a scheme called DACM (Document Access Control Methods), where the basic idea is geared toward flexible access control with some extensions to handle mandatory access control. Blaze has proposed credential-based access control (Blaze, 1996), to address the problem of unknown users. In these models a user has to produce one or more testimonials that have been certified by one or more third parties. The credential provides information about the rights, qualifications, responsibilities and other characteristics attributable to its bearer by the third parties. These third parties need to be trusted by the service provider. Winslett (1997) developed a credential based security and

privacy related system for enforcing access control in digital contents of repository or system. Access to systems containing protected information resources must be managed based on one or multiple selections of the alternative access control methods. However, different methods are based on, Users identity, Role, Policy, Content Dependency, Context, View, Time, Physical Location, Network Node, Mandatory, and Discretionary. In-addition, a risk assessment is needed to conduct to identify the data or resource risk and severity prior to establishing the level and selection of access controls or authorization to digital contents (Access control, 2009) [9].

CHAPTER 3

MITIGATION OF THE SECURITY THREATS

3.1 Overview of VLANs

VLAN is a logical partition of a layer 2 network. Multiple partitions can be created allowing for multiple VLANs to co-exist. Each VLAN is a broadcast domain, usually with its own IP network .VLAN area mutually isolated and packets can only pass between them via a router. The partitioning of the layer 2 network takes place inside a layer 2 device, usually via a switch. The hosts grouped within a VLAN area unaware the VLAN's existence.

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow us to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.

We can define one or many virtual bridges within a switch. Each virtual bridge we create in the switch defines a new broadcast domain (VLAN). Traffic cannot pass directly to another VLAN (between broadcast domains) within the switch or between two switches. To interconnect two different VLANs, we must use routers or Layer 3 switches. Figure 3.1 shows an example of three VLANs that create logically defined networks.

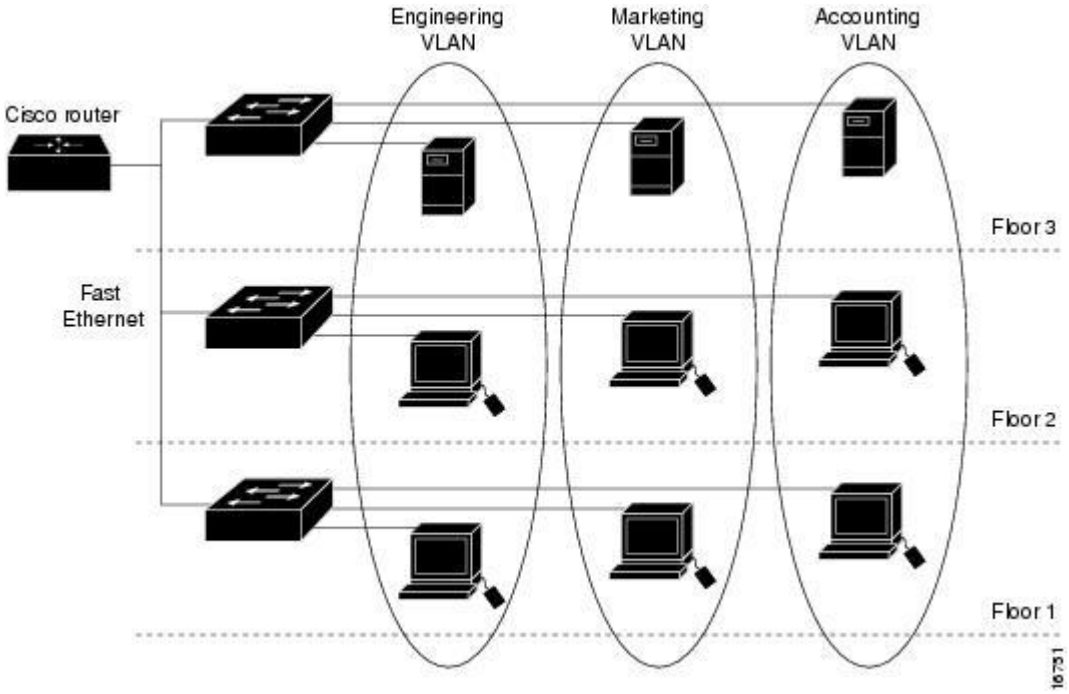

Figure 3.1 Sample VLANs

VLANs are often associated with IP subnetworks. For example, all of the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. We must assign LAN interface VLAN membership on an interface-by-interface basis (this is known as interface-based or static VLAN membership).

We can set the following parameters when we create a VLAN in the management domain:

- VLAN number
- VLAN name
- VLAN type
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- VLAN number to use when translating from one VLAN type to another

VLAN Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when creating and modifying VLANs in our network:

- Before creating a VLAN, put the Catalyst 4500 series switch in VTP server mode or VTP transparent mode. If the Catalyst 4500 series switch is a VTP server, we must define a VTP domain. For information on configuring VTP, see "Understanding and Configuring VTP."
- The Cisco IOS **end** command is not supported in VLAN database mode.
- We cannot use **Ctrl-Z** to exit VLAN database mode.

With Cisco IOS Release 12.2(25)EW and later, Catalyst 4500 series switches support 4096 VLANs in compliance with the IEEE 802.1Q standard. These VLANs are organized into three ranges: reserved, normal, and extended.

Some of these VLANs are propagated to other switches in the network when we use the VLAN Trunking Protocol (VTP). The extended-range VLANs are not propagated, so we must configure extended-range VLANs manually on each network device.

Table 3.1.1 VLAN ranges.

VLANs	Range	Usage	Propagated by VTP
0, 4095	Reserved	For system use only. We cannot see or use these VLANs.	N/A
1	Normal	Cisco default. We can use this VLAN but we cannot delete it.	Yes
2-1001	Normal	Used for Ethernet VLANs; we can create, use, and delete these VLANs.	Yes
1002-1005	Normal	Cisco defaults for FDDI and Token Ring. We cannot delete VLANs 1002-1005.	Yes
1006-4094	Extended	For Ethernet VLANs only. When configuring extended-range VLANs, note	No

		the following: Layer 3 ports and some software features require internal VLANs. Internal VLANs are allocated from 1006 and up. We cannot use a VLAN that has been allocated for such use. To display the VLANs used internally, enter the **show vlan internal usage** command. Switches running Catalyst product family software do not support configuration of VLANs 1006-1024. If we configure VLANs 1006-1024, ensure that the VLANs do not extend to any switches running Catalyst product family software. We must enable the extended system ID to use extended range VLANs. See the "Enabling the Extended System ID" section.	

We can configure the following parameters for VLANs 2 through 1001:

- VLAN name
- VLAN type
- VLAN state (active or suspended)
- SAID
- STP type for VLANs

VLAN Default Configuration

Table 3.1.2 Ethernet VLAN Defaults and Ranges

Parameter	Default	Valid Values
VLAN ID	1	1-4094
VLAN name	VLAN*x*, where *x* is a number assigned by the software.	No range
802.10 SAID	100,001	1-4,294,967,294
MTU size	1500	1500-18,190
Translational bridge 1	1002	0-1005
Translational bridge 2	1003	0-1005
VLAN state	active	active; suspend; shutdown

3.2 Overview of Port Security

Port security limits the number of valid MAC addresses allowed on a port. The MAC addresses of legitimate devices are allowed access, while other MAC addresses are denied. Any additional attempts to connect by unknown MAC addresses generate a security violation.

We can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When we assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside

the group of defined addresses. If we limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a workstation attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs.

After we have set the maximum number of secure MAC addresses on a port, the secure addresses are included in an address table in one of these ways:

- We can configure all secure MAC addresses by using the **switchport port-security mac-address** mac_address interface configuration command.
- We can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
- We can configure a number of addresses and allow the rest to be dynamically configured.

- We can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts. Although sticky secure addresses can be manually configured, it is not recommended.

  We can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling *sticky learning*. To enable sticky learning, enter the **switchport port-security mac-address sticky** command. When we enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.

  The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If we save the sticky secure

MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If we do not save the configuration, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

After the maximum number of secure MAC addresses is configured, they are stored in an address table. To ensure that an attached device has the full bandwidth of the port, configure the MAC address of the attached device and set the maximum number of addresses to one, which is the default.

A security violation occurs if the maximum number of secure MAC addresses has been added to the address table and a workstation whose MAC address is not in the address table attempts to access the interface.

We can configure the interface for one of these violation modes, based on the action to be taken if a violation occurs:

- Restrict—A port security violation restricts data, causes the SecurityViolation counter to increment, and causes an SNMP Notification to be generated. The rate at which SNMP traps are generated can be controlled by the snmp-server enable traps port-security trap-rate command. The default value ("0") causes an SNMP trap to be generated for every security violation.
- Shutdown—A port security violation causes the interface to shut down immediately. When a secure port is in the error-disabled state, we can bring it out of this state by entering the **errdisable recovery cause** psecure-violation global configuration command or we can manually reenable it by entering the **shutdown** and **no shut down** interface configuration commands. This is the default mode.

  We can also customize the time to recover from the specified error disable cause (default is 300 seconds) by entering the **errdisable recovery interval** interval command.

Default Port Security Configuration

Table 3.2.1 Default Port Security Configuration

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Aging	Disabled
Aging type	Absolute
Static Aging	Disabled
Sticky	Disabled

Port Security Guidelines and Restrictions

Follow these guidelines when configuring port security:

- A secure port cannot be a trunk port.
- A secure port cannot be a destination port for Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel port-channel interface.
- A secure port and static MAC address configuration are mutually exclusive.

3.3 Overview of ACL (Access Control List)

ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface. It is a table that tells a computer operating system which gives access rights for each user to particular system object. Access control lists can generally be configured.

Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. Our router examines each packet to determine whether to forward or drop the packet, on the basis of the criteria we specified within the access lists.

Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information. Note that sophisticated users can sometimes successfully evade or fool basic access lists because no authentication is required.

Why We Should Configure Access Lists

There are many reasons to configure access lists; for example, we can use access lists to restrict contents of routing updates or to provide traffic flow control. One of the most important reasons to configure access lists is to provide security for our network, which is the focus of this chapter.

We should use access lists to provide a basic level of security for accessing our network. If we do not configure access lists on our router, all packets passing through the router could be allowed onto all parts of our network.

Access lists can allow one host to access a part of our network and prevent another host from accessing the same area. In Figure 14, host A is allowed to access the Human Resources network, and host B is prevented from accessing the Human Resources network.

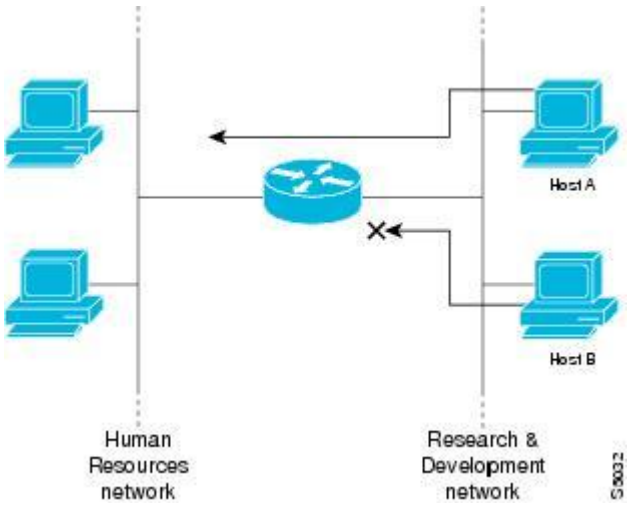

Figure 3.2 Using Traffic Filters to Prevent Traffic from Being Routed to a Network

We can also use access lists to decide which types of traffic are forwarded or blocked at the router interfaces. For example, we can permit e-mail traffic to be routed, but at the same time block all Telnet traffic.

When to Configure Access Lists

Access lists should be used in "firewall" routers, which are often positioned between our internal network and an external network such as the Internet. We can also use access lists on a router positioned between two parts of our network, to control traffic entering or exiting a specific part of our internal network.

To provide the security benefits of access lists, we should at a minimum configure access lists on border routers—routers situated at the edges of our networks. This provides a basic buffer from the outside network, or from a less controlled area of our own network into a more sensitive area of our network.

On these routers, we should configure access lists for each network protocol configured on the router interfaces. We can configure access lists so that inbound traffic or outbound traffic or both are filtered on an interface.

Access lists must be defined on a per-protocol basis. In other words, we should define access lists for every protocol enabled on an interface if we want to control traffic flow for that protocol.

Basic versus Advanced Access Lists

This chapter describes how to use standard and static extended access lists, which are the basic types of access lists. Some type of basic access list should be used with each routed protocol that we have configured for router interfaces.

Besides the basic types of access lists described in this chapter, there are also more advanced access lists available, which provide additional security features and give us greater control over packet transmission. These advanced access lists and features are described in the other chapters within the part "Traffic Filtering and Firewalls."

Overview of Access List Configuration

Each protocol has its own set of specific tasks and rules that are required in order for us to provide traffic filtering. In general, most protocols require at least two basic steps to be accomplished. The first step is to create an access list definition, and the second step is to apply the access list to an interface.

The following sections describe these two steps:

- Creating Access Lists
- Applying Access Lists to Interfaces

Note that some protocols refer to access lists as *filters* and refer to the act of applying the access lists to interfaces as *filtering*.

Creating Access Lists

Create access lists for each protocol we wish to filter, per router interface. For some protocols, we create one access list to filter inbound traffic, and one access list to filter outbound traffic.

To create an access list, we specify the protocol to filter, we assign a unique name or number to the access list, and we define packet filtering criteria. A single access list can have multiple filtering criteria statements.

Cisco recommends that we create our access lists on a TFTP server and then download the access lists to our router. This approach can considerably simplify maintenance of our access lists. For details, see the "Creating and Editing Access List Statements on a TFTP Server" section later in this chapter.
The protocols for which we can configure access lists are identified in Table 16.

This section has the following sections:

- Assigning a Unique Name or Number to Each Access List
- Defining Criteria for Forwarding or Blocking Packets
- Creating and Editing Access List Statements on a TFTP Server

Assigning a Unique Name or Number to Each Access List

When configuring access lists on a router, we must identify each access list uniquely within a protocol by assigning either a name or a number to the protocol's access list.

We can specify access lists by names for the following protocols:

- Apollo Domain
- IP
- IPX
- ISO CLNS
- NetBIOS IPX
- Source-route bridging NetBIOS

We can specify access lists by numbers for the protocols listed in Table 16. Table 16 also lists the range of access list numbers that is valid for each protocol.

Table 3.3.1 Protocols with Access Lists Specified by Numbers

Protocol	**Range**
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Ethernet type code	200-299
Ethernet address	700-799
Transparent bridging (protocol type)	200-299
Transparent bridging (vendor code)	700-799
Extended transparent bridging	1100-1199
DECnet and extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Source-route bridging (protocol type)	200-299
Source-route bridging (vendor code)	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099

Standard VINES	1-100
Extended VINES	101-200
Simple VINES	201-300

Defining Criteria for Forwarding or Blocking Packets

When creating an access list, we define criteria that are applied to each packet that is processed by the router; the router decides whether to forward or block each packet on the basis of whether or not the packet matches the criteria.

Typical criteria we define in access lists are packet source addresses, packet destination addresses, and upper-layer protocol of the packet. However, each protocol has its own specific set of criteria that can be defined.

For a single access list, we can define multiple criteria in multiple, separate access list statements. Each of these statements should reference the same identifying name or number, to tie the statements to the same access list. We can have as many criteria statements as we want, limited only by the available memory. Of course, the more statements we have, the more difficult it will be to comprehend and manage our access lists.

The Implied "Deny All Traffic" Criteria Statement

At the end of every access list is an implied "deny all traffic" criteria statement. Therefore, if a packet does not match any of our criteria statements, the packet will be blocked.

The Order in Which We Enter Criteria Statements

Note that each additional criteria statement that we enter is appended to the *end* of the access list statements. Also note that we cannot delete individual statements after they have been created. We can only delete an entire access list.

The order of access list statements is important! When the router is deciding whether to forward or block a packet, the Cisco IOS software tests the packet against each criteria statement in the

order in which the statements were created. After a match is found, no more criteria statements are checked.

If we create a criteria statement that explicitly permits all traffic, no statements added later will ever be checked. If we need additional statements, we must delete the access list and retype it with the new entries.

Applying Access Lists to Interfaces

For some protocols, we can apply up to two access lists to an interface: one inbound access list and one outbound access list. With other protocols, we apply only one access list which checks both inbound and outbound packets.

If the access list is inbound, when the router receives a packet, the Cisco IOS software checks the access list's criteria statements for a match. If the packet is permitted, the software continues to process the packet. If the packet is denied, the software discards the packet.

If the access list is outbound, after receiving and routing a packet to the outbound interface, the software checks the access list's criteria statements for a match. If the packet is permitted, the software transmits the packet. If the packet is denied, the software discards the packet.

CHAPTER 4

PACKET TRACER

Packet Tracer is a cross-platform visual simulation program designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Students enrolled in a CCNA Academy program can freely download and use the tool free of charge for educational use.

In addition to simulating certain aspects of computer networks, Packet Tracer can also be used for collaboration. As of Packet Tracer 6.3, Packet Tracer supports a multi-user system that enables multiple users to connect multiple topologies together over a computer network. Packet Tracer also allows instructors to create activities that students have to complete. Packet Tracer is often used in educational settings as a learning aid. Cisco Systems claims that Packet Tracer is useful for network experimentation.

Packet Tracer is a cross-platform network simulator designed by Cisco Systems to run on Mac OS, Linux and Microsoft Windows. A similar Android app is also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a "cable" item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BDP, to the extents required by the current CCNA curriculum. As of version 5.3, Packet Tracer also supports the Border Gateway Protocol.

Version 6.0 added support for IOS version 15 and Hot Standby Routing Protocol. Version 6.2 added support for various DHCP, EIGRP and OSPF commands, improved support for Zone-Based Firewall policies. As of version 6.3, Packet Tracer supports an embedded web server with JavaScript and CSS support. The command line can be used for creating a router-to-pc connection.

Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs. Packet Tracer is commonly used by CCNA Academy students, since it is available to them for free. However, due to functional limitations, it is intended by Cisco to be used only as a learning aid, not a replacement for

Cisco routers and switches. The application itself only has a small number of features found within the actual hardware running a current Cisco IOS version. Thus, Packet Tracer is unsuitable for modelling production networks. It has a limited command set, meaning it is not possible to practice all of the IOS commands that might be required.

Packet Tracer can be useful for understanding abstract networking concepts, such as the Enhanced Interior Gateway Routing Protocol by animating these elements in a visual form. Packet Tracer is also useful in education by providing additional components, including an authoring system, network protocol simulation and an assessment system.

CHAPTER 5

CONFIGURATION & IMPLEMENTATION

Our Network topology has been given below:

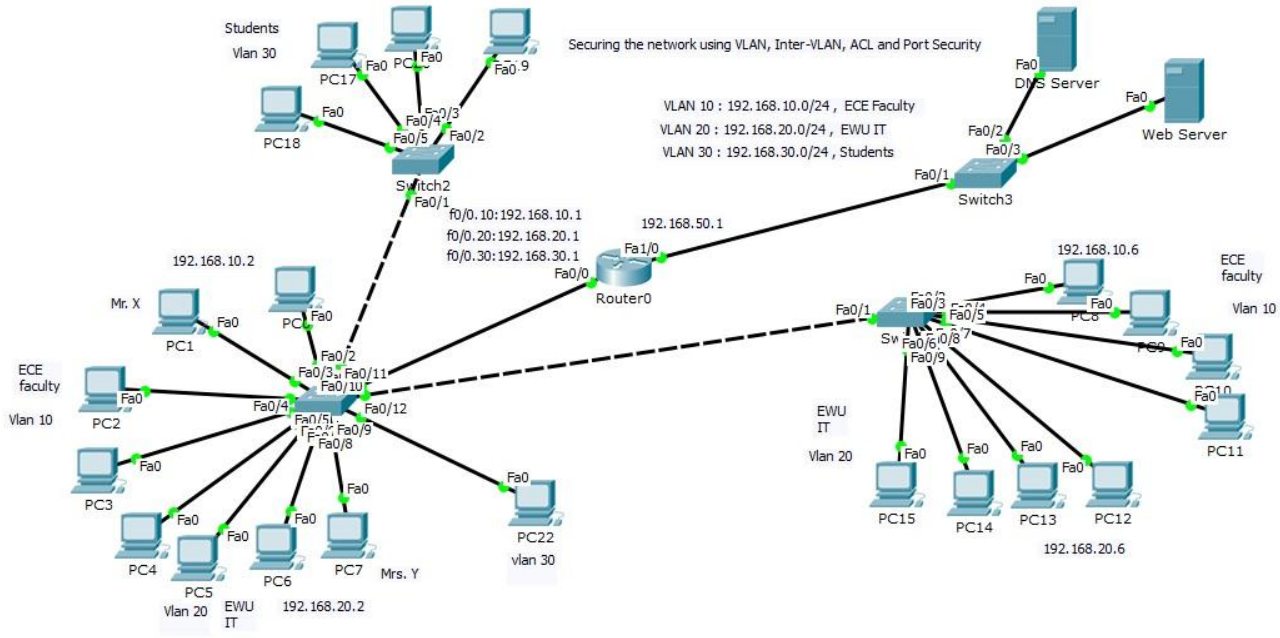

Figure 5.1 Network Topology

Device Requirements:

In our configuration, we have used the following devices:

Table 5.1 Device Requirements

Device	Quantity	Model
PCs	21	Generic
Switch	3	Cisco 2950
Router	1	Cisco 2811
DNS Server	1	Generic
HTTP Server	1	Generic
Cables : Straight-through and cross-over CAT 5e		

IP Table of our network:

Table 5.2 IP Table

VLAN/Device/Interface	IP address/ Network Address	Subnet Mask
VLAN 10	192.168.10.0	255.255.255.0
VLAN 20	192.168.20.0	255.255.255.0
VLAN 30	192.168.30.0	255.255.255.0
F0/0.10	192.168.10.1	255.255.255.0
F0/0.20	192.168.20.1	255.255.255.0
F0/0.30	192.168.30.1	255.255.255.0
F1/0	192.168.50.1	255.255.255.0
DNS Server	192.168.50.2	255.255.255.0
HTTP Server	192.168.50.2	255.255.255.0

IP Configuration of a PC:

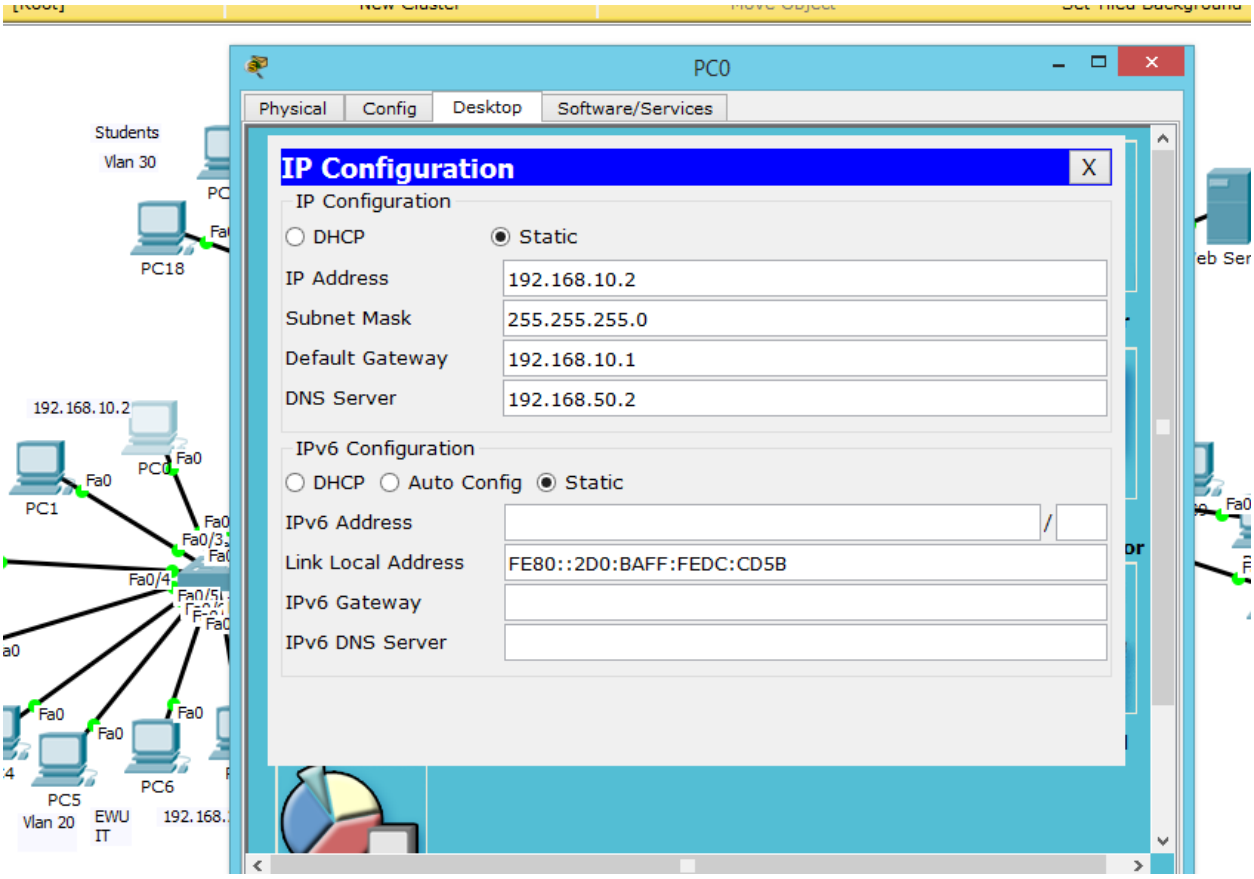

Figure 5.2 IP Configuration of a host

<u>Router Configuration:</u>

hostname Router
interface FastEthernet0/0
no shutdown
duplex auto
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0

interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0

interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0

interface FastEthernet1/0
ip address 192.168.50.1 255.255.255.0
no shutdown

ip access-group 120 out

access-list 120 deny tcp host 192.168.10.3 host 192.168.50.3 eq www
access-list 120 deny tcp host 192.168.20.5 host 192.168.50.3 eq www
access-list 120 permit ip any any
end

VLAN Creation & Assigning on the switch 1

Switch>enable
Switch#configure terminal
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit

Switch(config)#enable password cisco
Switch(config)#enable secret cisco1
Switch(config)#exit

Switch#configure terminal
Switch(config)#line vty 4 15
Switch(config-line)#password cisco
Switch(config-line)#exit
Switch(config)#^Z

Switch#configure terminal

Switch(config-if)#vlan 10
Switch(config-vlan)#name ECE
Switch(config-vlan)#exit

Switch(config)#vlan 20
Switch(config-vlan)#name IT
Switch(config-vlan)#exit

Switch(config)#vlan 30
Switch(config-vlan)#name Students
Switch(config-vlan)#exit

Switch(config)#^Z

Switch#configure terminal

Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 10

Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport access vlan 10

Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport access vlan 10

Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport access vlan 10

Switch(config)#interface fastEthernet 0/6
Switch(config-if)#switchport access vlan 20

Switch(config)#interface fastEthernet 0/7
Switch(config-if)#switchport access vlan 20

Switch(config)#interface fastEthernet 0/8
Switch(config-if)#switchport access vlan 20

Switch(config)#interface fastEthernet 0/9
Switch(config-if)#switchport access vlan 20

Switch(config)#interface fastEthernet 0/12
Switch(config-if)#switchport access vlan 30

Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk

Switch(config)#interface fastEthernet 0/11
Switch(config-if)#switchport mode trunk

Switch(config)#interface fastEthernet 0/10
Switch(config-if)#switchport mode trunk

VLAN Creation & Assigning on the switch 2

Switch>enable
Switch#configure terminal
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit

Switch(config)#enable password cisco
Switch(config)#enable secret cisco1
Switch(config)#exit

Switch#configure terminal
Switch(config)#line vty 4 15
Switch(config-line)#password cisco
Switch(config-line)#exit
Switch(config)#^Z

Switch#configure terminal

Switch(config)#vlan 30
Switch(config-vlan)#name Students
Switch(config-vlan)#exit

Switch(config)#^Z

Switch#configure terminal

Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 30

Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport access vlan 30

Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport access vlan 30

Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk

VLAN Creation & Assigning on the switch 3

Switch>enable
Switch#configure terminal
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit

Switch(config)#enable password cisco
Switch(config)#enable secret cisco1
Switch(config)#exit

Switch#configure terminal
Switch(config)#line vty 4 15
Switch(config-line)#password cisco
Switch(config-line)#exit
Switch(config)#^Z

Switch#configure terminal

Switch(config-if)#vlan 10
Switch(config-vlan)#name ECE
Switch(config-vlan)#exit

Switch(config)#vlan 20
Switch(config-vlan)#name IT
Switch(config-vlan)#exit

Switch(config)#^Z

Switch#configure terminal

Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 10

Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport access vlan 10

Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport access vlan 10

Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport access vlan 10

Switch(config)#interface fastEthernet 0/6
Switch(config-if)#switchport access vlan 20

Switch(config)#interface fastEthernet 0/7
Switch(config-if)#switchport access vlan 20

Switch(config)#interface fastEthernet 0/8
Switch(config-if)#switchport access vlan 20

Switch(config)#interface fastEthernet 0/9
Switch(config-if)#switchport access vlan 20

Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk

DNS Server Setup:

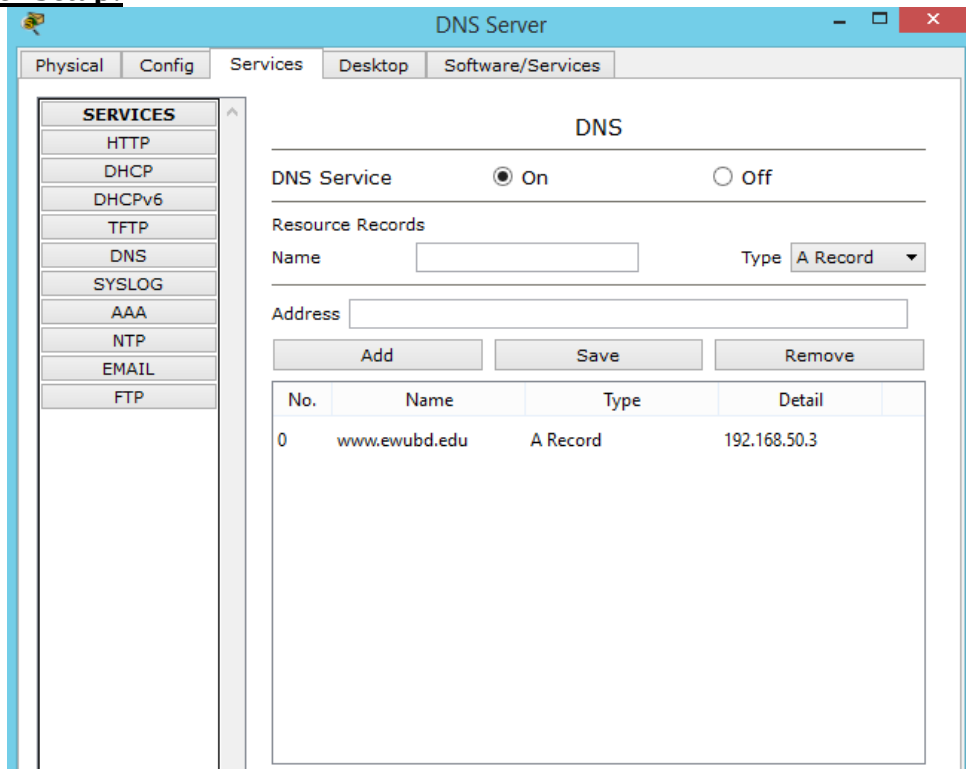

Figure 5.3 DNS Server Configuration

Web Server Setup:

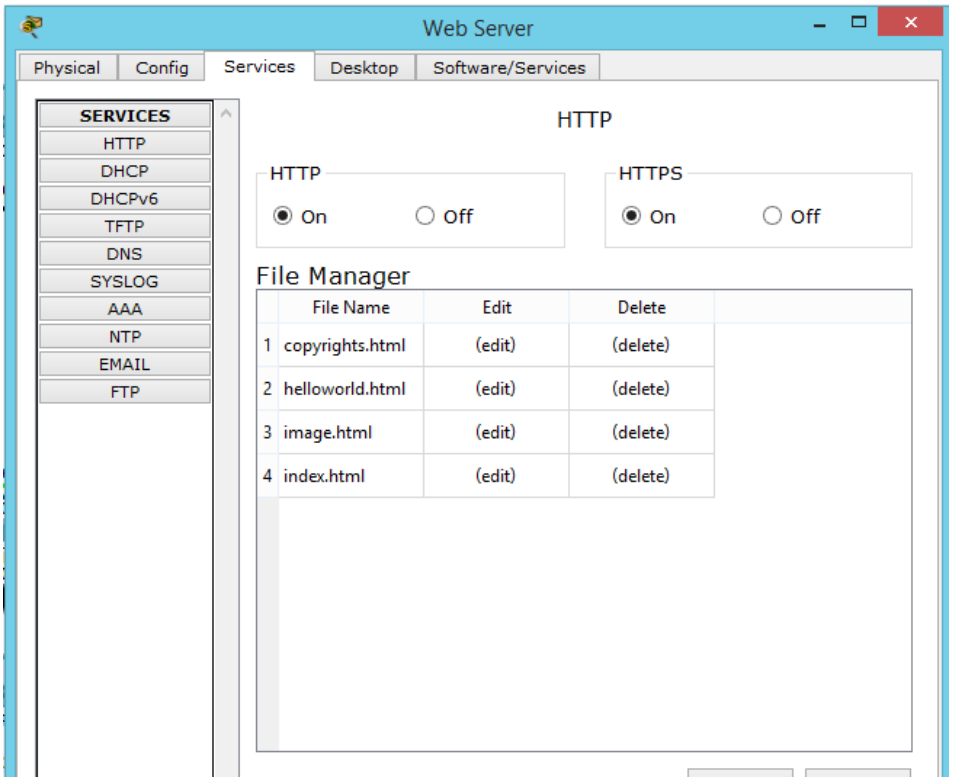

Figure 5.4 Web Server Configuration

Commands for the port security on the switch 1:

Switch(config)#int f0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address 00D0.BADC.CD5B

Switch(config-if)#switchport port-security max

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#int f0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address 0001.C775.6AE5

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#int f0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 00D0.5811.1977
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#int f0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 0003.E46E.0E0C
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#int f0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 0040.0B0B.E510
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#int f0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 0005.5E00.E7BB
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#int f0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 000B.BED5.CA48

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#int f0/9

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address 00D0.97D3.1111

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#int f0/12

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address 00E0.F9A9.1551

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#exit

Access Control List configuration on the Router:

Router(config)#access-list 120 deny tcp host 192.168.10.3 192.168.50.3 0.0.0.0 eq www
Router(config)#access-list 120 deny tcp host 192.168.20.5 192.168.50.3 0.0.0.0 eq www
Router(config)#access-list 120 permit ip any any

Router(config)#int f1/0
Router(config-if)#ip access-group 120 out
Router(config-if)#

CHAPTER 6

DISCUSSIONS

After configuration, we have got the following achievements:

1. We can create numbers of networks on the switches by using VLAN technology.

2. Here every PC is binded with port number and its MAC address. For this reason, no unauthorized PC, laptop can be a part of the network. If any unauthorized PC or laptop try to connect with the switch, then the port will be turn off and hence no further communication can take place for this unauthorized PC, laptop.

From the Figure 6.1, we can see that an unauthorized user is trying to get access of the access. Later he/she takes the cable of PC0 and connect with the laptop to get the access.

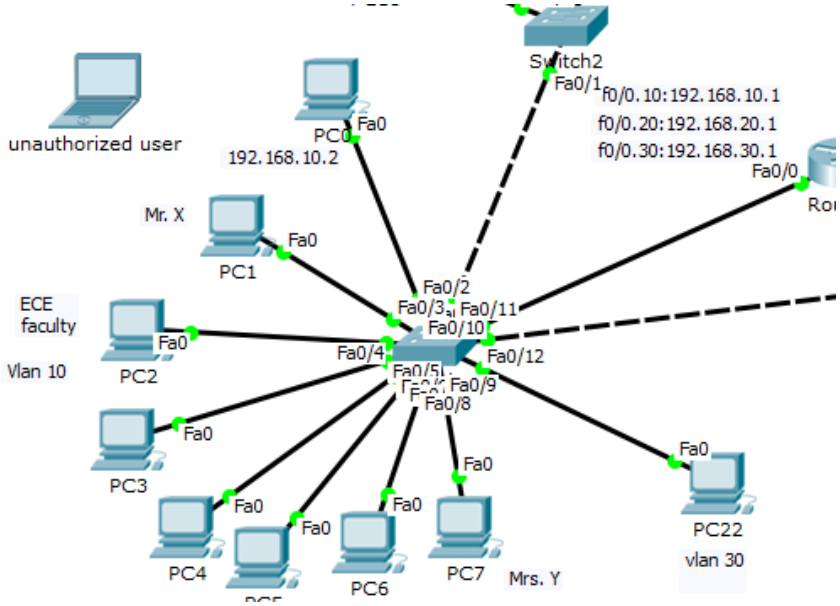

Figure 6.1 Port- security 1

But as the switchport port security has been enabled here, so the unauthorized can't communicate with others though the laptop is connected with the network cable. When he/she tries to communicate with other, the port of the switch will be shutdown (see Figure 6.2, the port is colored red that means shutdown) as the MAC address of the unknown laptop has not been included or binded on the switch.

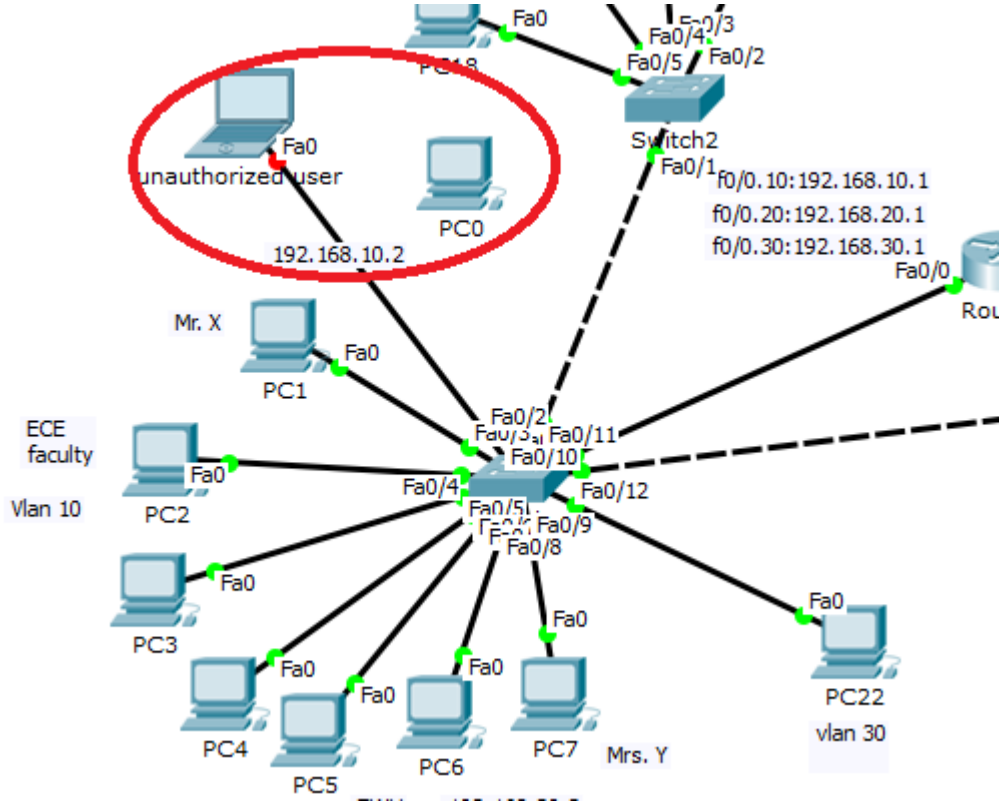

Figure 6.2 Port- security 2

3. No one can change the VLAN by themselves.

4. By using ACL we can restrict someone to the use of the network asset. For example, in our configuration, Mr. X and Mrs. Y can't access HTTP service from the web server. All others can communicate with each other, even these two PCs can ping or do any other communication except HTTP service. In this way we can restrict anyone to access any service of the network.

5. We can use the router as a firewall by using the ACL commands.

6. By using router's subinterfaces feature, we can reuse the router's limited fast Ethernet ports for multiple networks with the help of VLAN technology. In our case, we have used 1 physical port for 3 networks. If we don't use subinterface feature, then we were needed 3 fast Ethernet ports for 3 different networks.

CHAPTER 7

CONCLUSION

In Networking, authentication and access management have emerged as major issues which threaten to hinder progress. In this project work, we have discussed such threats and their solutions. VLAN, inter-VLAN communication, switch port security and ACL can play a very vital role to mitigate such unauthorized access problems. We have compared here with a simple network and the network with the implementation of VLAN, inter-VLAN communication, switch port security and ACL. It has been found significant differences in the view of security issues. The whole project works have been implemented in Cisco's packet tracer version 6.3. In future, the whole work will be extended to the real devices with other security protocol implementation such as routing security, encryption of the routing information, dynamic NAT security and so one. We also wish to do these in IPv6 network.

REFERENCES

[1] Akin T.," Hardening Cisco Routers," O'Reilly & Associates, 2002.

[2] Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," In Proceedings International Conference on Advanced Communication Technology, 2004.

[3] Chen S., Iyer R., and Whisnant K., "Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors," In Proceedings of the 2002 International Conference on Dependable Systems & Network, Washington, D.C., 2002.

[4] Kim H., "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, FEBRUARY 2004.

[5] Rybaczyk P., "Cisco Router Troubleshooting Handbook ", M&T Books, 2000.

[6] Jo S., "Security Engine Management of Router based on Security Policy," proceedings of world academy of science, engineering and technology, volume 10, ISSN 1307-688, 2005.

[7] Q. Ali., and Alabady S., "Design and Implementation of A Secured Remotely Administrated Network," In Proceedings International Arab Conference on Information Technology, ACIT'2007.

[8] Alabady S. , "Design and Implementation of a Network Security Model using Static VLAN and AAA Server," In Proceedings International Conference on Information & Communication Technologies: from Theory to Applications, ICTTA'2008.

[9] Shastry Y., Klotz S., and Russell R., "Evaluating the effect of iSCSI protocol parameters on performance, " In Proceedings of the Parallel and Distributed Computing and Networks, 2005

[10 " Network Security 1 ", Cisco system,Inc. 2006.