**NETWORK SECURITY MANAGEMENT SYSTEM**

A Project Report Submitted to

**Chandigarh University, Gharuan, Mohali**

Towards the partial fulfillment of

The degree of

**Bachelor of Engineering**

In

**Computer Science & Engineering**



Session:- 2018-2019

**Submitted To: Submitted By:**

**Miss. Bandana Subhradeep Bhattacharya (16BCS2617)**

**(Mentor) Ananya Jindal (16BCS2855)**

**Project Teacher:**

**Miss. Sonali Rawat**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**CHANDIGARH UNIVERSITY ,GHARUAN**

**ACKNOWLEDGEMENT**

Gratitude is the most exquisite form of courtesy. Life without thankfulness is devoid of love and passion. Hope without thankfulness is lacking in one perception. Faith without thankfulness lacks strength and fortitude. The beatitude, bliss and euphoria that accompany the successful completion of any task would not be complete without the expression of appreciation of simple virtues to the people who made it possible. So with reverence, veneration honor, I acknowledge all those whose guidance and **Miss. Sonali Rawat** (Assistant Professor, Chandigarh University) for their guidance, inspiration and constructive suggestions that helped me in the preparation of this Project. I also express my deepest gratitude towards my project mentor **Miss. Bandana** for her valuable suggestions and directions throughout the development of the project. I am grateful for her cooperation during the period of my Project. Moral, intellectual and very frequently required support from all the faculty members is also hereby acknowledged.

**Teacher’s Signature:**

**Mentor Name:**

**Miss. Bandana**

**Project Teacher :**

**Miss. Sonali Rawat**

**DECLARATION**

I hereby declare that the project entitled “Network Security Management System” submitted for the B.E. (CSE) degree is my original work and the project has not formed the basis for the award of any other degree, diploma, fellowship or any other similar titles. I also declare the work presented in the report is my own work except as acknowledged in the text and foot notes, and that to my knowledge this material has not been submitted either in whole or in part, for a degree at this University or at any other such Institution.

**Signature of the Student**

**Subhradeep Bhattacharya:**

**(16BCS2617)**

**Date: Ananya:**

**(16BCS2855)**

**ABSTRACT**

Computer networks are a system of interconnected computers for the purpose of sharing digital information. The concept of a network began in 1962 when a server at the Massachusetts Institute of Technology was connected to a server in Santa Monica, California. Since that time the proliferation of computers and computer networks has increased significantly. One of the most significant challenges to networks is attacks on their resources caused by inadequate network security. The purpose of this research project was to evaluate open source, free, intrusion detection systems and how easily they can integrate into an existing network. Research was conducted for this study through a review of existing literature pertaining to intrusion detection systems and how they function. The literature also highlighted previous studies conducted on intrusion detection systems, both commercial and open source. In addition to the review of existing literature, the author conducted independent testing on three open source intrusion detection systems. The open source programs, Snort, OSSEC, and Prelude, were selected due to being highly rated in professional publications. The author created a secure simulated computer network, to ensure that each of the programs was tested in a controlled and equitable manner. The findings of this study determined that the three open source intrusion detection systems tested are as capable as commercial programs in securing a computer network.

For Internet connectivity we are also using frame relay. In this setup NAT is very essential in which we have translate live IP into local and vice-versa. In short we can say a lot of technologies are studied and implemented for the successful completion of the project.

**TABLE OF CONTENTS**

**Acknowledgementi**

**Declaration ii**

**Abstract iii**

**List of Contents iv**

**Chapter** [**1.**](#_Toc456366946) **Network Fundamentals**

1.1 Basics of Networking …………………………………..……….…………………………….1

[1.2 Components of Network](#_Toc456366949) 2

[1.3 Wireless Networks](#_Toc456366950) 3

[1.4 Advantages of Networking 3](#_Toc456366951)

[1.5 Main challenges of installing a network](#_Toc456366952) 4

[**Chapter 2. TCP/IP and OSI Models**](#_Toc456366953)

[2.1 TCP/IP network model](#_Toc456366954) 5

[2.2 Overview of TCP/IP network model 5](#_Toc456366956)

[2.3 Comparing two TCP/IP models 6](#_Toc456366957)

[2.4 OSI network model](#_Toc456366956) 6

[2.5 Comparing TCP/IP and OSI models 6](#_Toc456366957)

[2.6 OSI layers and their functions](#_Toc456366956) 7

[2.7 OSI layering concepts and benefits](#_Toc456366957) 8

[**Chapter 3**](#_Toc456366966)**. IP Address V4**

[3.1 Introduction](#_Toc456366968) 9

[3.2 Subnet Mask](#_Toc456366969) 9

[**Chapter 4**](#_Toc456366973)**. IP Routing**

[4.1 Static Routing](#_Toc456366975) 11

[4.2 Dynamic Routing 12](#_Toc456366975)

[4.3 Link State Routing](#_Toc456366975) 15

[**Chapter 5**](#_Toc456366993)**. LAN Switching**

5.1 Classification of Switching......………………………………………………………………16

[5.2 Basic Switch Administration](#_Toc456366995) 17

[**Chapter 6**](#_Toc456366998)**. IP version 6**

[6.1 Features](#_Toc456367000) 19

[6.2 Addressing Modes 2](#_Toc456367000)1

[6.3 Neighbor Discovery Protocol 23](#_Toc456367000)

[6.4 Subnetting 23](#_Toc456367000)

[6.5 Routing 2](#_Toc456367000)4

[6.6 Protocols changed to support IPv6 2](#_Toc456367000)5

**Chapter 7. Project**

[7.1 Objective](#_Toc456366968) 26

[7.2 Introduction](#_Toc456366968) 26

[7.3 Physical Network Security](#_Toc456366968) 27

7.4 Online Privacy……………………………………………………………………………….28

7.5 Access Control Lists…………………………………………………………………………30

7.6 Network Address Translation………………………………………………………………..36

[**Conclusion**](#_Toc456367005) **37**

**Future Scope 40**

[**References**](#_Toc456367006) **41**

**CHAPTER 1**

**NETWORKING FUNDAMENTALS**

**INTRODUCTION**

A computer network, often simply referred to as a Network, is a collection of computers and devices connected by communications channels that facilitates communications among users and allows users to share resources with other users. A computer network allows sharing of resources and information among devices connected to the network. Networks may be classified according to a wide variety of characteristics

* 1. **Basic of Networking**

A computer network consists of a collection of computers, printers and other equipment that is connected together so that they can communicate with each other.

School ‘Local Area

Network’ (LAN)

Modem or Router

Access to:

Internet content & learning resources, Scoilnet etc

Email communication

Cache, Proxy,

Filtering, Firewall

Server

Users

computers

Other users,

computers

File and Print Server

CD or Multimedia Servers

Printers , Scanners etc

Fig 1.1: Representation of Network in a college

Broadly speaking, there are two types of network configuration, peer-to-peer networks and client/server networks.

**Peer-to-peer networks** are more commonly implemented where less than ten computers are involved and where strict security is not necessary. All computers have the same status, hence the term 'peer', and they communicate with each other on an equal footing. Files, such as word processing or spreadsheet documents, can be shared across the network and all the computers on the network can share devices, such as printers or scanners, which are connected to any one computer.

**Client/server networks** are more suitable for larger networks. A central computer, or 'server', acts as the storage location for files and applications shared on the network. Usually the server is a higher than average performance computer. The server also controls the network access of the other computers which are referred to as the 'client' computers. Typically, teachers and students in a school will use the client computers for their work and only the network administrator (usually a designated staff member) will have access rights to the server.

**1.2 Components of a Network**

A computer network comprises the following components:

* A minimum of at least 2 computers
* Cables that connect the computers to each other, although wireless communication is becoming more common (see Advice Sheet 20 for more information)
* A network interface device on each computer (this is called a network interface card or NIC)
* A ‘Switch’ used to switch the data from one point to another. Hubs are outdated and are little used for new installations.
* Network operating system software

**Structured Cabling**

The two most popular types of structured network cabling are **twisted-pair** (also known as **10BaseT**) and **thin coax** (also known as **10Base2**). 10BaseT cabling looks like ordinary telephone wire, except that it has 8 wires inside instead of 4. Thin coax looks like the copper coaxial cabling that's often used to connect a Video Recorder to a TV.

**Network Interface Card (NIC)**

A NIC (pronounced 'nick') is also known as a network card. It connects the computer to the cabling, which in turn links all of the computers on the network together. Each computer on a network must have a network card. Most modern network cards are 10/100 NICs and can operate at either 10Mbps or 100Mbps.

Computers with a wireless connection to a network also use a network .



Fig 1.2: Network Interface Cards (NICs)

**Hub and Switch**

A hub is a device used to connect a PC to the network. The function of a hub is to direct information around the network, facilitating communication between all connected devices. However in new installations switches should be used instead of hubs as they are more effective and provide better performance. A switch, which is often termed a 'smart hub'.



Fig 1.3: An 8 port Hub



Fig 1.4: 2 Examples of 24 port Switches

**1.3 Wireless Networks**

The term 'wireless network' refers to two or more computers communicating using standard network rules or protocols, but without the use of cabling to connect the computers together. Instead, the computers use wireless radio signals to send information from one to the other. A wireless local area network (WLAN) consists of two key components: an access point (also called a base station) and a wireless card. Information can be transmitted between these two components as long as they are fairly close together (up to 100 meters indoors or 350 meters outdoors).



Fig 1.5: Wireless Access point or Wireless Base station

* 1. **Advantages of Networking**

**Speed.**

Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to floppy disks, then carrying or sending the disks from one computer to another. This method of transferring files in this manner is very time-consuming.

**Cost.**

The network version of most software programs are available at considerable savings when compared to buying individually licensed copies. Besides monetary savings, sharing a program on a network allows for easier upgrading of the program. The changes have to be done only once, on the file server, instead of on all the individual workstations.

**Centralized Software Management.**

One of the greatest benefits of installing a network at a school is the fact that all of the software can be loaded on one computer (the file server). This eliminates that need to spend time and energy installing updates and tracking files on independent computers throughout the building.

**Resource Sharing.**

Sharing resources is another area in which a network exceeds stand-alone computers. Most schools cannot afford enough laser printers, fax machines, modems, scanners, and CD-ROM players for each computer.

**Flexible Access.**

School networks allow students to access their files from computers throughout the school. Students can begin an assignment in their classroom, save part of it on a public access area of the network, then go to the media center after school to finish their work. Students can also work cooperatively through the network.

**Security.**

Files and programs on a network can be designated as "copy inhibit," so that you do not have to worry about illegal copying of programs. Also, passwords can be established for specific directories to restrict access to authorized users.

**1.5 Main challenges of installing a Network**

**Costs**

Although a network will generally save money over time, the initial costs can be substantial, and the installation may require the services of a technician.

**Requires Administrative Time.**

Proper maintenance of a network requires considerable time and expertise. Many schools have installed a network, only to find that they did not budget for the necessary administrative support.

**File Server May Fail.**

Although a file server is no more susceptible to failure than any other computer, when the files server "goes down," the entire network may come to a halt. When this happens, the entire school may lose access to necessary programs and files.

**CHAPTER 2**

**TCP/IP AND OSI MODELS**

**2.1 TCP/IP Networking Model**

A networking model, sometimes also called either a networking architecture or networking blueprint, refers to a comprehensive set of documents. Individually, each document describes one small function required for a network; collectively, these documents define everything that should happen for a computer network to work. Some documents define a protocol, which is a set of logical rules that devices must follow to communicate. Other documents define some physical requirements for networking. For example, a document could define the voltage and current levels used on a particular cable when transmitting data.

**2.2 Overview of the TCP/IP Networking Model**

The TCP/IP model both defines and references a large collection of protocols that allow computers to communicate. To define a protocol, TCP/IP uses documents called Requests for Comments (RFC). (You can find these RFCs using any online search engine.) The TCP/IP model also avoids repeating work already done by some other standards body or vendor consortium by simply referring to standards or protocols created by those groups.

**TCP/IP Application Layer**

TCP/IP application layer protocols provide services to the application software running on a computer. The application layer does not define the application itself, but it defines services that applications need. For example, application protocol HTTP defines how web browsers can pull the contents of a web page from a web server. In short, the application layer provides an interface between software running on a computer and the network itself.

**TCP/IP Transport Layer**

Although many TCP/IP application layer protocols exist, the TCP/IP transport layer includes a smaller number of protocols. The two most commonly used transport layer protocols are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

**TCP/IP Internet Layer**

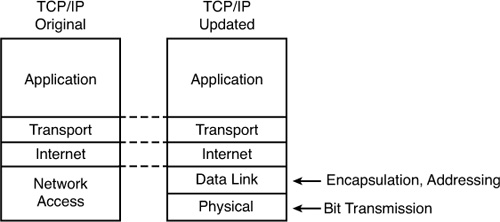
The application layer includes many protocols. The transport layer includes fewer, most notably, TCP and UDP. The TCP/IP Internet layer includes a small number of protocols, but only one major protocol: the Internet Protocol (IP).

**TCP/IP Network Access Layer**

The TCP/IP model’s network access layer defines the protocols and hardware required to deliver data across some physical network. The term network access refers to the fact that this layer defines how to access or use the physical media over which data can be transmitted.

**2.3 Comparing the Two TCP/IP Models**

The functions defined in the network access layer can be broken into two major categories: functions related directly to the physical transmission of data and those only indirectly related to the physical transmission of data. The two alternative TCP/IP models exist. Comparing the two, the upper layers are identical. The lower layers differ in that the single network access layer in one model is split into two layers to match the division of physical transmission details from the other functions. Figure shows the two models again, with emphasis on these distinctions.



**Figure 2.1** Network Access versus Data Link and Physical Layers

**2.4 OSI Networking Model**

OSI model is the layer approach to design, develop and implement network. OSI provides following advantages: -

1. Designing of network will be standard base.
2. Development of new technology will be faster.
3. Devices from multiple vendors can communicate with each other.
4. Implementation and troubleshooting of network will be easy.

**2.5 Comparing OSI and TCP/IP**

Today, the OSI model can be used as a standard of comparison to other networking models. Figure below compares the seven-layer OSI model with both the four-layer and five-layer TCP/IP models.

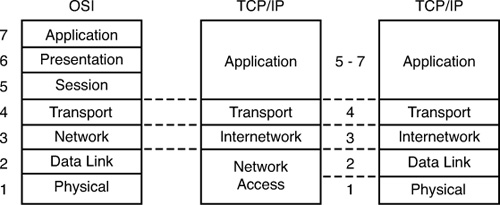


Figure 2.2: OSI Model Compared to the Two TCP/IP Models

**2.6 OSI Layers and Their Functions**

Cisco requires that CCNAs demonstrate a basic understanding of the functions defined by each OSI layer, as well as remembering the names of the layers. It is also important that, for each device or protocol referenced throughout the book, you understand which layers of the OSI model most closely match the functions defined by that device or protocol.

**Table 2.1:** Layers and Functional Description of OSI

| **Layer** | **Functional Description** |
| --- | --- |
| 7 | Layer 7 provides an interface between the communications software and any applications that need to communicate outside the computer on which the application resides. It also defines processes for user authentication. |
| 6 | This layer's main purpose is to define and negotiate data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG. Encryption is also defined by OSI as a presentation layer service. |
| 5 | The session layer defines how to start, control, and end conversations (called sessions). This includes the control and management of multiple bidirectional messages so that the application can be notified if only some of a series of messages are completed. This allows the presentation layer to have a seamless view of an incoming stream of data. |
| 4 | Layer 4 protocols provide a large number of services, as described in Chapter 6, "Fundamentals of TCP/IP Transport, Applications, and Security." Although OSI Layers 5 through 7 focus on issues related to the application, Layer 4 focuses on issues related to data delivery to another computer (for instance, error recovery and flow control). |
| 3 | The network layer defines three main features: logical addressing, routing (forwarding), and path determination. Routing defines how devices (typically routers) forward packets to their final destination. Logical addressing defines how each device can have an address that can be used by the routing process. Path determination refers to the work done by routing protocols to learn all possible routes, and choose the best route. |
| 2 | The data link layer defines the rules that determine when a device can send data over a particular medium. Data link protocols also define the format of a header and trailer that allows devices attached to the medium to successfully send and receive data. |
| 1 | This layer typically refers to standards from other organizations. These standards deal with the physical characteristics of the transmission medium, including connectors, pins, use of pins, electrical currents, encoding, light modulation, and the rules for how to activate and deactivate the use of the physical medium. |

**Table 2.2:** OSI Reference Model—Example Devices and Protocols

| **Layer Name** | **Protocols and Specifications** | **Devices** |
| --- | --- | --- |
| Application, presentation, session (Layers 5–7) | Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP | Firewall, intrusion detection systems, hosts |
| Transport (Layer 4) | TCP, UDP | Hosts, firewalls |
| Network (Layer 3) | IP | Router |
| Data link (Layer 2) | Ethernet (IEEE 802.3), HDLC, Frame Relay, PPP | LAN switch, wireless access point, cable modem, DSL modem |
| Physical (Layer 1) | RJ-45, EIA/TIA-232, V.35, Ethernet (IEEE 802.3) | LAN hub, LAN repeater, cables |

**2.7 OSI Layering Concepts and Benefits**

* **Less complex:** Compared to not using a layered model, network models break the concepts into smaller parts.
* **Standard interfaces:** The standard interface definitions between each layer allow for multiple vendors to create products that fill a particular role, with all the benefits of open competition.
* **Easier to learn:** Humans can more easily discuss and learn about the many details of a protocol specification.
* **Easier to develop:** Reduced complexity allows easier program changes and faster product development.
* **Multivendor interoperability:** Creating products to meet the same networking standards means that computers and networking gear from multiple vendors can work in the same network.

**CHAPTER 3**

**IPv4**

**3.1 Introduction**

IPv4 address is a 32-bit address. It is divided into four octets. Each octet has 8 bits. It has two parts one is network address and second is host address. In local area network, we can use private IP address, which is provided by IANA (Internet Assigning Numbering Authority). IP addresses are divided into five classes.

**Class Range N/w bits Host bits Subnet mask Total IP Valid IP**

A 1 – 126 8 24 255.0.0.0 16777216 16777214

B 128 – 191 16 16 255.255.0.0 65536 65534

C 192 – 223 24 8 255.255.255.0 256 254

D 224 – 239 it is reserved for multicast.

E 240 – 255 it is reserved for research/scientific use.

**Table 3.1** Class and Range

We can use first three classes. IANA provides private IP addresses from first three classes.

**Class Private IP Range**

A 10.0.0.0 – 10.255.255.255

B 172.16.0.0 – 172.31.255.255

C 192.168.0.0 – 192.168.255.255

**3.2 Subnet Mask**

Subnet mask is also 32-bit addresses, which tell us how many bits are used for network and how many bits are used for host address.

In Subnet mask Network bits are always 1 and Host bits are always 0.

When we are going to assign IP addresses to our computers then we have to follow some rules.

(1) All Host bits cannot be 0 (10.0.0.0), because it represent network address which is reserved for router.

(2) All Host bits cannot be 1 (10.255.255.255), because this is broadcast address of that network (10th network).

(3) All bits cannot be 0 (0.0.0.0), because this address is reserved for Default routing. Default routing is used in case of Stub n/w (means our network has one exit point).

(4) All bits cannot be 1 (255.255.255.255), because this is reserved for Broadcasting.

(5) 127.0.0.1 - This is Loopback address, which is used for self-communication or troubleshooting purpose.

C:\>ipconfig

C:\>ipconfig/all

It shows all detail.

# **CHAPTER 4**

# **IP ROUTING**

When we want to connect two or more networks using different n/w addresses then we have to use IP Routing technique. The router will be used to perform routing between the networks. A router will perform following functions for routing.

**(1) Path determination**

The process of obtaining path in routing table is called path determination. There are three different methods to which router can learn path.

i) Automatic detection of directly connected n/w.

Ii) Static & Default routing

iii) Dynamic routing

**(2) Packet forwarding**

It is a process that is by default enable in router. The router will perform packet forwarding only if route is available in the routing table.

**4.1 Static Routing**

In this routing, we have to use IP route commands through which we can specify routes for different networks. The administrator will analyze whole internetwork topology and then specify the route for each n/w that is not directly connected to the router.

#### 4.1.1 **Steps to perform static routing**

(1) Create a list of all n/w present in internetwork.

(2) Remove the n/w address from list, which is directly connected to n/w.

(3) Specify each route for each routing n/w by using IP route command.

**Router (config) #ip route <destination n/w> <mask> <next hop ip>**

**Next hop IP** it is the IP address of neighbor router that is directly connected our router.

#### Static Routing Example:

Router (config) #IP Route 10.0.0.0 255.0.0.0 192.168.10.2

### 4.1.2 **Advantages of static routing**

(1) Fast and efficient.

(2) More control over selected path.

(3) Less overhead for router.

### 4.1.3 **Disadvantages of static routing**

(1) More overheads on administrator.

(2) Load balancing is not easily possible.

(3) In case of topology change routing table has to be change manually.

### Alternate command to specify static route

Static route can also specify in following syntax: -

Old

Router (config) #Ip route 172.16.0.0 255.255.0.0 172.25.0.2

Or

Router (config) #Ip route 172.16.0.0 255.255.0.0 serial 0

### 4.1.4 **Default Routing**

Default routing means a route for any n/w. these routes are specify with the help of following syntax: -Router (conf) #ip route 0.0.0.0 0.0.0.0 <next hop>Or<Exit interface>

**4.2 Dynamic Routing**

In dynamic routing, we will enable a routing protocol on router. This protocol will send its routing information to the neighbor router. The neighbors will analyze the information and write new routes to the routing table.

The routers will pass routing information receive from one router to other router also. If there is

More than one path available then routes is compared and best path is selected. Some examples of dynamic protocol are: -

RIP, IGRP, EIGRP, OSPF

**RIP-:**

* + RIP Stands For Routing Information protocol
  + It Is a Industry standard Dynamic Routing Protocol
  + IT Is not a More Intelligent Dynamic Routing Protocol
  + It Is Basically Use For Smaller Size Organization
  + It Support Maximum 15 Routers in the Network. 16 Router Is Unreachable
  + It is denoted By R in Routing Table.
  + It’s Administrative Distance Is 120.
  + In RIP Routing protocol We cannot create A Separate Administrative boundary in The Network.
  + It Calculate the Metric In Terms Of Hop Count From source Network to destination Network. Lower the Hop count that Is the Best Route for that particular network.
  + It works on Bellman Ford algorithm
  + RIPV.1 Do Not Support VLSM
  + RIPV.2 Support VLSM

**4.2.1 Configuring RIP**

Router (config) # routers rip

Router (config) # network(directly connected network)

Router (config) #version1/version 2

Router (config) #do write

Router (config) #exit

**EIGRP-:**

* + EIGRP Stands For Enhanced Interior Gateway Routing protocol
  + It Is a Cisco standard routing protocol
  + It Is a More Intelligent routing protocol Than RIP And IGRP
  + It Is Basically Use For Medium to Lager Size Organization in the network.
  + It supports Maximum 255 Routers in The Network
  + It’s Administrative distance Is 90
  + It calculates the Metric In Terms Of Bandwidth And delay
  + EIGRP Works on DUAL(Diffusing Update Algorithm) Algorithm
  + EIGRP is denoted by D in Routing Table.
  + EIGRP Supports VLSM
  + EIGRP Creates three table In the Router

#### 4.2.2 **Configuring EIGRP**

Router (config) # Router Eigrp <As no>

Router (config) # network (directly connected network)<wild card mask>

Router (config) #No auto summary

Router (config) #do write

Router (config) #exit

**OSPF-:**

* + OSPF stands For Open shortest path First
  + It Is An Industry standard Routing protocol
  + It supports Unlimited router in the Network
  + It Is Denoted By O in routing Table
  + It’s Administrative distance is 110
  + It Is basically Use For Larger Size Organization in The Network
  + In OSPF Routing protocol We Can Create a separate administrative boundary in the Network through Area No. within The same area all of The routers Are exchanging The Route information From Neighbor router in the network.
  + It Calculates the Metric in terms of Bandwidth
  + OSPF works on DIJKSTRA Algorithm
  + It Is a More Intelligent routing protocol
  + OSPF Supports VLSM

#### 4.2.3 **Commands to configure OSPF**

Router (config) # Router ospf <process\_id>

Router (config) # network (directly connected network)<wild card mask><area area\_id>

Router (config) #do write

Router (config) #exit

**Wild Mask –** Complement of subnet mask

### **Types of Dynamic Routing Protocols**

According to the working there are two types of Dynamic Routing Protocols.

(1) Distance Vector

(2) Link State

According to the type of area in which protocol is used there are again two types of protocol:

(1) Interior Routing Protocol

(2) Exterior Routing Protocol

**4.3 Link State Routing**

This type of routing is based on link state. Its working is explained as under

(1) Each router will send Hello packets to all neighbors using all interfaces.

(2) The router from which hello replies are received are stored in the neighbor ship table. Hello packets are send periodically to maintain the neighbor table.

(3) The router will send link state information to the all neighbors. Link state information from one neighbor is also forwarded to other neighbor.

(4) Each router will maintain its link state database created from link state advertisement received from different routers.

(5) The router will use best path algorithm to store the path in routing table.

#### 4.3.1 **Router ID**

Router ID is the highest IP address of router interfaces. This id is used as the identity of the router. The first preference for selecting router ID is given to the Logical interfaces. If logical interface is not present then highest IP of physical interface is selected as router id.

4.3.2 **Backup Designated Router**

This router will work as backup for the designated router. In BDR mode, it will receive all information but do not forward this information to other non-DR router.

# **CHAPTER 5**

# **LAN SWITCHING**

Ethernet switches are used in LAN to create Ethernet networks. Switches forward the traffic on the basis of MAC address. Switches maintain a Mac Addressee table in which mac addresses and port no’s

Are used to perform switching decision. Working of bridge and switch is similar to each other.

**5.1 Classification of switches**

Switches are classified according to the following criteria: -

#### 5.1.1 **Types of switches based on working**

(1) Store & Forward

This switch receives entire frame then perform error checking and start forwarding data to the destination.

(2) Cut through

This switch starts forwarding frame as soon as first six bytes of the frame are received.

(3) Fragment-free

This switch receives 64 bytes of the frame, perform error checking and then start forwarding data.

(4) Adaptive cut-through

It changes its mode according the condition. If it sees there are errors in many frames then it changes to Store & Forward mode from Cut through or Fragment-free.

#### 5.1.2 **Types of switches based on management**

(1) Manageable switches

(2) Non-Manageable switches

(3) Semi-Manageable switches

*5.1.3* ***Types of switches based on OSI layer***

(1) Layer 2 switches (only switching)

(2) Layer 3 switches (switching & routing)

#### 5.1.4 **Types of switches based on command mode (only in Cisco)**

(1) IOS based

(2) CLI based

#### 5.1.5 **Type of switches based on hierarchical model**

(1) Core layer switches

(2) Distribution layer switches

(3) Access layer switches

#### 5.1.6 **Qualities of switch**

- No. of ports

- Speed of ports

- Type of media

- Switching or wire speed or throughput

### **5.2** **Basic Switch Administration**

IOS based switches are similar to the routers. We can perform following function on switches in a similar manner as performed on router.

(1) Access switch using console

(2) Commands to enter & exit from different mode

(3) Commands to configure passwords

(4) Manage configuration

(5) Backup IOS and configuration

(6) Configuring and resolving hostnames

(7) Managing telnet

(8) Configuring CDP

(9) Configuring time clock

(10) Configuring Banners

(11) Command line shortcuts and editing shortcuts

(12) Managing history

(13) Configure logging

(14) Boot system commands

**Following function and options are not similar in router and switch.**

(1) Default hostname is ‘Switch’

(2) Auxiliary port is not present

(3) VTY ports are mostly 0 to 15

(4) By default interfaces are enabled

(5) IP address cannot be assign to interfaces

(6) Routing configuration mode is not present

(7) Interface no. starts from 1

(8) Web access is by default enabled

(9) Configuration registry is not present in similar manner

(10) Flash memory may contain multiple files and startup-configuration is also saved in flash

### **Configuring IP and Gateway on switch**

We can configure IP address on switch for web access or telnet IP address is required for the administration of the switch. If we have to access switch from remote n/w then we will configure default gateway in addition to IP address.

**CHAPTER 6**

**IPv6**

**Overview**

Internet Protocol version 6, is a new addressing protocol designed to incorporate whole sort of requirement of future internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on Network Layer (Layer-3). Along with its offering of enormous amount of logical address space, this protocol has ample of features which addresses shortcoming of IPv4.

**6.1 Features**

The successor of IPv4 is not designed to be backward compatible. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers the following features:

* **Larger Address Space:**

In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×1038 different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world

* **Simplified Header:**

IPv6’s header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 providing the fact the IPv6 address is four times longer.

* **End-to-end Connectivity:**

Every host can directly reach other host on the Internet, with some limitations involved like Firewall, Organization’s policies, etc.

* **Auto-configuration:**

IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way absence of a DHCP server does not put halt on inter segment communication.

* **Faster Forwarding/Routing:**

Simplified header puts all unnecessary information at the end of the header. All information in first part of the header are adequate for a Router to take routing decision thus making routing decision as quickly as looking at the mandatory header.

* **IPSec:**

Initially it was decided for IPv6 to must have IPSec security, making it more secure than IPv4. This feature has now been made optional.

* **No Broadcast:**

Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any Broadcast support anymore left with it. It uses multicast to communicate with multiple hosts.

* **Anycast Support:**

This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, sends the packet to the nearest destination.

* **Mobility:**

IPv6 was designed keeping mobility feature in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with same IP address

**Enhanced Priority support:**

Where IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it.

**Smooth Transition:**

Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This assures that mechanism to save IP addresses such as NAT is not required. **Extensibility:**

One of the major advantage of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options whereas options in IPv6 can be as much as the size of IPv6 packet itself.

**6.2 Addressing Modes**

In computer networking, addressing mode refers to the mechanism how we address a host on the network. IPv6 offers several types of modes by which a single host can be addressed, more than one host can be addressed at once or the host at closest distance can be addressed.

* **Unicast**

In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment. The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment

* **Multicast**

The IPv6 multicast mode is same as that of IPv4. The packet destined to multiple hosts is sent on a special multicast address. All hosts interested in that multicast information, need to join that multicast group first.

* **Anycast**

In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, sends a Unicast message.

**Hexadecimal Number System**

Hexadecimal is positional number system which uses radix (base) of 16. Every digit in Hexadecimal can represent values from 0 to 15.

**Address Structure**

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbol.

## **Interface ID**

IPv6 has three different type of Unicast Address scheme. The second half of the address (last 64 bits) is always used for Interface ID. MAC address of a system is composed of 48-bits and represented in Hexadecimal. MAC address is considered to be uniquely assigned worldwide. Interface ID takes advantage of this uniqueness of MAC addresses.

**Global Unicast Address**

This address type is equivalent to IPv4’s public address. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.

**Global Routing Prefix**

The most significant 48-bits are designated as Global Routing Prefix which is assigned to specific Autonomous System. Three most significant bits of Global Routing Prefix is always set to 001.

**Link-Local Address**

Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. First 16 bits of Link-Local address is always set to 1111 1110 1000 0000 (FE80). Next 48-bits are set to 0, thus:

**Unique-Local Address**

This type of IPv6 address which is though globally unique, but it should be used in local communication. This address has second half of Interface ID and first half is divided among Prefix, Local Bit, Global ID and Subnet ID.

## **Special Addresses:**

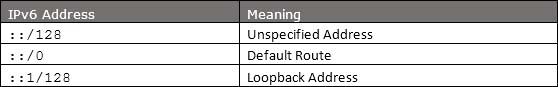


Table: 6.1

**Headers**

The wonder of IPv6 lies in its header. IPv6 address is 4 times larger than IPv4 but the IPv6 header is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All necessary information which is essential for a router is kept in Fixed Header. Extension Header contains optional information which helps routers to understand how to handle a packet/flow.

**Communication**

In IPv4, a host which wants to communicate with some other host on the network, needs first to have an IP address acquired either by means of DHCP or by manual configuration. As soon as a host is equipped with some valid IP address, it is now able to speak to any host on the subnet. To communicate on layer-3, a host also must know the IP address of the other host. Communication on a link, is established by means of hardware embedded MAC Addresses

ARP has been replaced by ICMPv6 Neighbor Discovery Protocol.

**6.3 Neighbor Discovery Protocol**

A host in IPv6 network is capable of auto-configuring itself with a unique link-local address. As soon as it is equipped with an IPv6 address, it joins a number of multicast groups. All communications related to that segment happens on those multicast addresses only. A host goes through a series of states in IPv6:

* **Neighbor Solicitation**: After configuring all IPv6’s either manually, or by DHCP Server or by auto-configuration, the host sends a Neighbor Solicitation message out to FF02::1/16 multicast address for all its IPv6 addresses in order to know that no one else occupies same addresses.
* **DAD (Duplicate Address Detection)**: When the host does not listen from anything from the segment regarding its Neighbor Solicitation message, it assumes that no duplicate address exists on the segment.
* **Neighbor Advertisement**: After assigning the addresses to its interfaces and making them up and running, the host once again sends out a Neighbor Advertisement message telling all other hosts on the segment, that it has assigned those IPv6 addresses to its interfaces.

**6.4 Subnetting**

In IPv4, addresses were created in classes. Classful IPv4 addresses clearly defines the bits used for network prefixes and the bits used for hosts on that network. IPv6 addresses uses 128 bits to represent an address which includes bits to be used for subnetting. Second half of the address (least significant 64 bits) is always used for Hosts only. Therefore, there is no compromise if we subnet the network.

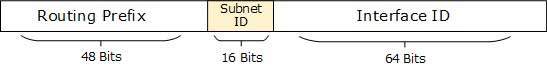


Figure: 6.1

16 Bits of subnet is equivalent to IPv4’s Class B Network. Using these subnet bits an organization can have more 65 thousands of subnets which is by far, more than enough.

**Dual Stack Routers**

A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.

**Tunneling**

In a scenario where different IP versions exist on intermediate path or transit network, tunneling provides a better solution where user’s data can pass through a non-supported IP version.

**NAT Protocol Translation**

This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With help of NAT-PT device, actual conversion happens between IPv4 and IPv6 packets and vice versa. See the diagram below:

**Route Optimization**

When a Correspondent Node initiate communication by sending packets to Mobile Node on Home Address, these packets are tunneled to Mobile Node by Home Agent. In Route Optimization mode, when the Mobile Node receives packet from Correspondent Node, it does not forward replies to Home Agent. Rather it sends its packet directly to Correspondent Node using Home Address as Source Address.

**6.5 Routing**

Routing concepts remain same in case of IPv6 but almost all routing protocol have been redefined accordingly. We have seen in Communication in IPv6 segment, how a host speaks to its gateway. Routing is a process to forward routable data choosing best route among several available routes or path to the destination. A router is a device which forwards data which is not explicitly destined to it.

**There exists two forms of routing protocols**

* **Distance Vector Routing Protocol**: The routing cost to reach a destination is calculated by means of hops between the source and destination. RIP and BGP are Distance Vector Protocols.
* **Link-State Routing Protocol**: This protocol acknowledges the state of a Link and advertises to its neighbors. Information about new links is learnt from peer routers.

**Routing protocols**

* **RIPng**

RIPng stands for Routing Information Protocol Next Generation. This is an Interior Routing Protocol and is a Distance Vector Protocol. RIPng has been upgraded to support IPv6.

* **OSPFv3**

Open Shortest Path First version 3 is an Interior Routing Protocol which is modified to support IPv6. This is a Link-State Protocol and uses Djikrasta’s Shortest Path First algorithm to calculate best path to all destinations.

* **BGPv4**

BGP stands for Border Gateway Protocol. It is the only open standard Exterior Gateway Protocol available. BGP is a Distance Vector protocol which takes Autonomous System as calculation metric, instead of number of routers as Hop. BGPv4 is an upgrade of BGP to support IPv6 routing.

**6.6 Protocols changed to support IPv6:**

* **ICMPv6**: Internet Control Message Protocol version 6 is an upgraded implementation of ICMP to accommodate IPv6 requirements. This protocol is used for diagnostic functions, error and information message, statistical purposes. ICMPv6’s Neighbor Discovery Protocol replaces ARP and helps discover neighbor and routers on the link.
* **DHCPv6**: Dynamic Host Configuration Protocol version 6 is an implementation of DHCP. Though IPv6 enabled hosts do not require any DHCPv6 Server to acquire IP address as they can be auto-configured.
* **DNS**: There has been no new version of DNS but it is now equipped with extensions to provide support for querying IPv6 addresses. A new AAAA (quad-A) record has been added to reply IPv6 query messages. Now DNS can reply with both IP versions (4 & 6) without any change in query format.

**Chapter 7**

**Project**

**Network Security Management System**

**7.1 Objective**

Our vulnerability to cyber-attacks continues to escalate as technology continues to move into mobile devices and everyday business practices. You can't hide from the danger and hope you won't be targeted. Now is the time to take control of your network security

Network Security is a branch of computer science that involves in securing a computer network and network infrastructure devices to prevent unauthorized access, data theft, network misuse, and device and data modification. Another function of Network Security is in preventing DoS (Denial of Service) attacks and assuring continuous service for legitimate network users. Network Security involves proactive defence methods and mechanisms to protect data, network and network devices from external and internal threats.

Data is the most precious factor of today’s businesses. Top business organizations spend billions of dollars every year to secure their computer networks and to keep their business data safe. Imagine the loss of all important research data on which the company has invested millions of dollars and working for years!!!

We are dependent on computers today for controlling large money transfers between banks, insurance, markets, telecommunication, electrical power distribution, health and medical fields, nuclear power plants, space research and satellites. We cannot negotiate security in these critical areas.

As the complexity of the systems and the networks are increasing, vulnerabilities are also increasing and the task of securing the networks is becoming more complex.

This makes Network Security an essential part of today's businesses.

So in this project we will deal with various types of network securities and how to manage them to create a secured industrial network.

**7.2 Introduction**

With all of the vital personal and business data being shared on computer networks every day, security has become one of the most essential aspects of networking. No one recipe to fully safeguard networks against intruders exists. Network security technology improves and evolves over time as the methods for both attack and defence grow more sophisticated.

**7.3 Physical Network Security**

The most basic but often overlooked element of network security involves keeping hardware protected from theft or physical intrusion.

Corporations spend large sums of money to lock their [network servers](https://www.lifewire.com/servers-in-computer-networking-817380), [network switches](https://www.lifewire.com/definition-of-network-switch-817588) and other core network components in well-guarded facilities. While these measures aren't practical for homeowners, households should still keep their [broadband routers](https://www.lifewire.com/what-is-a-broadband-router-816301) in private locations, away from nosy neighbour’s and house guests.

Widespread use of mobile devices makes physical security that much more important. Small gadgets are especially easy to leave behind at travel stops or to have fall out of pockets. News stories in the press abound of local residents having their smartphones stolen in public places, sometimes even while using them. Be alert to the physical surroundings whenever using mobile devices, and conscientiously put them away when done.

Finally, stay in visual contact with a phone when loaning it to someone else: A malicious person can steal personal data, install monitoring software, or otherwise “hack” phones in just a few minutes when left unattended.

An alarming number of ex-boyfriends/girlfriends, spouses, and neighbour’s get accused of such acts.

**Password Protection**

Passwords are an extremely effective system for improving network security if applied properly. Unfortunately, some don't take password management seriously and insist on using bad, weak (meaning, easy to guess) passwords like “123456” on their systems and networks.

Following just a few common-sense best practices in password management greatly improves the security protection on a computer network:

* set *strong passwords*, or passcodes, on all devices that join the network
* change the default administrator password of network routers
* do not share passwords with others more often than necessary; set up [guest network](https://www.lifewire.com/guest-network-for-home-tutorial-818204) access for friends and visitors if possible
* change passwords when they may have become too widely known

**Spyware**

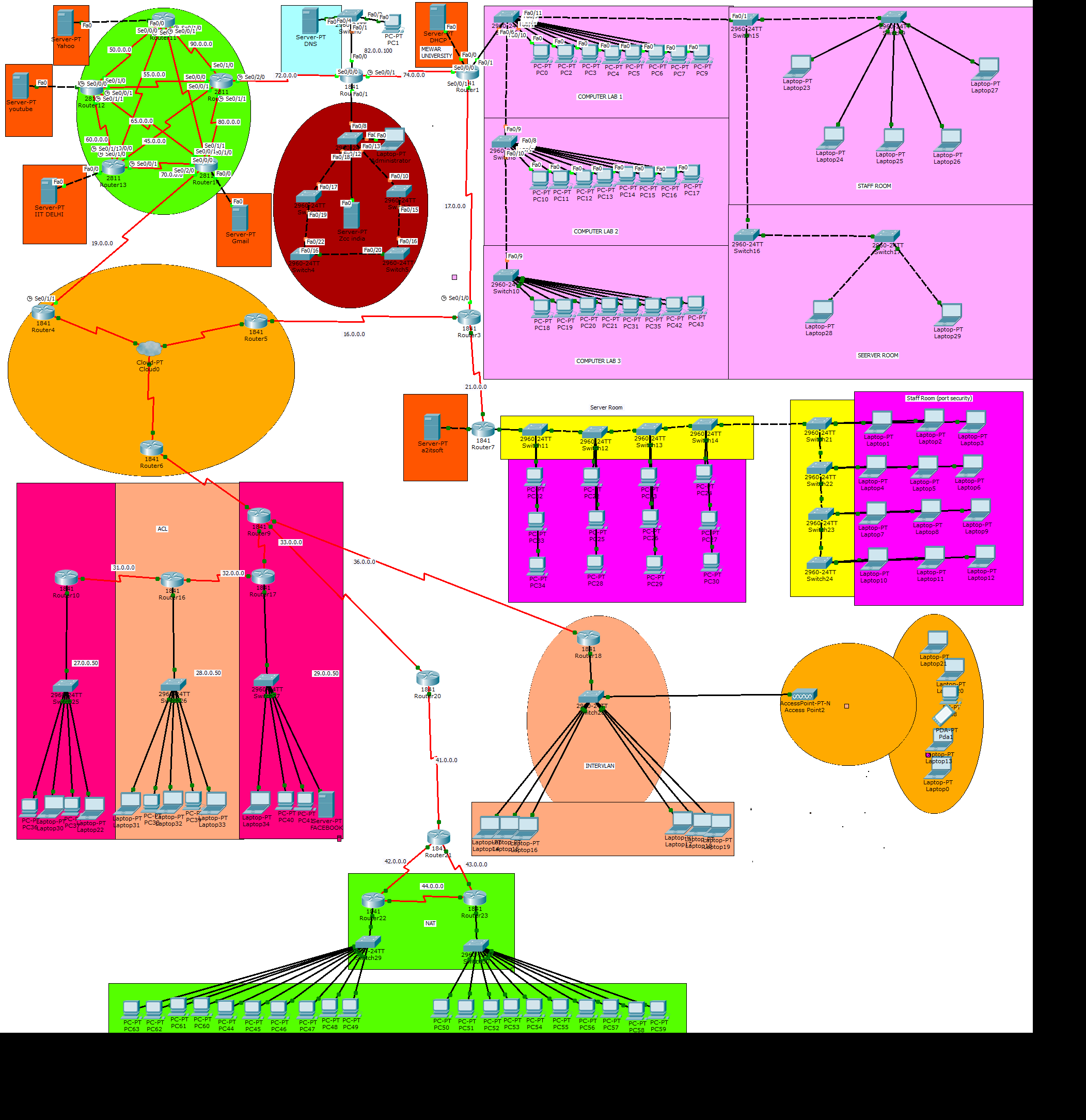
Even without physical access to the devices or knowing any network passwords, illicit programs called *spyware* can infect computers and networks, typically by visiting Web sites. Much spyware exists on the Internet. Some spyware monitors a person’s computer usage and Web browsing habits and reports this information back to corporations, who use it to create more targeted advertising. Other spyware attempts to steal personal data. One of the most dangerous forms of spyware, [key logger software](https://www.lifewire.com/definition-of-keylogger-817998) captures and sends the history of all keyboard key presses a person makes, ideal for capturing passwords and credit card numbers. All spyware on a computer attempts to function without the knowledge of people using it, thereby posing a substantial security risk.

Because spyware is notoriously difficult to detect and remove, security experts recommend installing and running reputable anti-spyware software on computer networks.

**7.4 Online Privacy**

Personal stalkers, identity thieves and perhaps even government agencies monitor people’s online habits and movements well beyond the scope of basic spyware. [Wi-Fi hotspot](https://www.lifewire.com/wifi-hotspots-explained-818310) usage from commuter trains and automobiles reveal a person’s location, for example. Even in the virtual world, much about a person’s identity can be tracked online through the [IP addresses](https://www.lifewire.com/what-is-an-ip-address-818393) of their networks and their social network activities.

Techniques to protect a person’s privacy online include [anonymous Web proxy servers](https://www.lifewire.com/free-anonymous-web-proxy-servers-818058), although maintaining full privacy online is not fully achievable through today’s technologies.

**Elements used in project**

**7.5 Access Control lists**

Cisco Access Control Lists are the set of conditions grouped together by name or number. These conditions are used in filtering the traffic passing from router. Through these conditions we can filter the traffic; either when it enters in router or when it exits from router.

**What is access control list?**

Basically ACL is the integrated feature of IOS software that is used to filter the network traffic passing through the IOS devices. Network traffic flows in the form of packets. A packet contains small piece of data and all necessary information which are required to deliver it. By default when a router receives a packet in interface, it takes following actions:-

* Grab destination address from the packet
* Find an entry for destination address in routing table
* If match found, forwards the packet from associate interface
* If no match found, discard the packet immediately.

This default behaviour does not provide any security. Anyone who know the correct destination address can send his packet through the router. For example following figure illustrates a simple network.

In this network, no security policy is applied on router. So router will not be able to distinguish between user’s packet and adversary’s packet. From router’s point of view, both packets have correct destination address so they should be forwarded from exit interface.

Suppose we tell the router that only 10.0.0.10 has the right to access the 30.0.0.1. To match with this condition router will take following actions:-

* Grab source and destination address from the packet
* Match both addresses with given condition
* If packet is not arrived from 10.0.0.10, drop the packet immediately.
* If packet is not intended from 30.0.0.1, drop the packet immediately.
* If both condition match find an entry for destination address in routing table
* If match found, forwards the packet from associate interface
* If no match found, discard the packet immediately.



Now only the packets from 10.0.0.10 are allowed to pass from router. With this condition adversary will not be able to access the server. We can create as much conditions as we want. Technically these conditions are known as ACLs. Besides filtering unwanted traffic, ACLs are used for several other purposes such as prioritizing traffic for QoS (Quality of Services), triggering alert, restricting remote access, debugging, VPN and much more. Due to complexity, these uses of ACLs are not tested in CCNA level exams. CCNA level exams test only basic uses of ACLs such as filtering the traffic and blocking specific hosts.

Okay now we have basic understating of what ACLs are and what they do. In next section we will understand technical concept of ACLs.

**Direction and location of ACLs**

A packet interacts with three locations during its journey from router:-

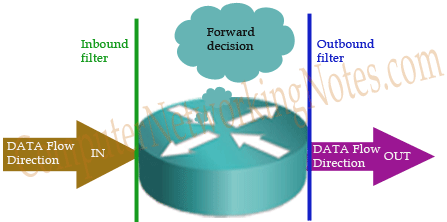
1. Packet arrives in interface (Entrance)
2. Router makes forward decision
3. Packet outs from interface (Exit)

We cannot filter the packet in the middle of router where it makes forward decision. Decision making process has its own logic and should not be interfered for filtering purpose. After excluding this location, we have two locations; entrance and exit. We can apply our ACLs conditions on these locations.

ACL conditions applied on entrance work as **inbound** filter. ACL conditions applied on exit work as **outbound** filter.

Inbound ACLs filter the traffic before router makes forward decision. Outbound ACLs filter the traffic after the router makes forward decision.

An ACL filter condition has to two actions; permit and deny. We can permit certain types of traffic while blocking rest or we can block certain types of traffic while allowing rest.



**Key points**

* We must have to apply ACLs on interface which process the packet.
* ACLs must be applied in data flow direction. Inbound ACLs must be placed in entrance interface. Outbound ACLs must be placed in exit interface.

|  |  |  |
| --- | --- | --- |
| **Router without ACLs** | **Router with inbound ACLs** | **Router with outbound ACLs** |
| Packet enters in router. | Packet enters in router. | Packet enters in router. |
| Grab source and destination address from the packet | Grab source and destination address from the packet | Grab source and destination address from the packet |
|  | *Run ACL conditions to determine the action. If deny condition matches, drop the packet immediately. If permit condition matches, let the packet enter in router.* |  |
| Find an entry for destination address in routing table | Find an entry for destination address in routing table | Find an entry for destination address in routing table |
| If match found, forwards the packet from associate interface. If no match found, discard the packet. | If match found, forwards the packet from associate interface. If no match found, discard the packet. | If match found, forwards the packet from associate interface. If no match found, discard the packet. |
|  |  | *Run ACL conditions to determine the action. If deny condition matches, drop the packet immediately. If permit condition matches, let the packet out from interface.* |
| Packet outs from router. | Packet outs from router. | Packet outs from router. |

* Once applied, ACL will filter every packet passing through the interface.

Types of ACLs

There are two types of ACLs:

1. Standard ACLs (1 – 99 and 1300 - 1999)
2. Extended ACLs (100 – 199 and 2000 - 2699)

### Standard ACLs (1 – 99 and 1300 - 1999)

ACLs are the part of Cisco IOS from its beginning. In earlier days simple filtering was sufficient. Standard ACLs are used for normal filtering. Standard ACLs filter the packet based on its source IP address.

### Extended ACLs (100 – 199 and 2000 - 2699)

Over the time security becomes more challenging. To mitigate current security threats, advance filtering is required. Extended ACLs takes this responsibility. Extended ACLs can filter a packet based on its sources address, destination address, port number, protocol and much more.

### Named ACLs

Named ACLs are the extended version of existing ACLs. Named standard ACL is the extended version of standard ACL. Named extended ACL is the enhanced version of extended ACL. Existing ACLs (Standard and Extended) assign a unique number among all the ACLs. While Named ACLs assign a unique name among all the ACLs.

I will explain above ACLs in detail with examples in next parts of this article.

#### **General guide line for ACL**

* ACLs are always processed from top to down in sequential order.
* A packet is compared with ACL conditions until it finds a match.
* Once a match is found for packet, no further comparison will be done for that packet.
* Interface will take action based on match condition. There are two possible actions; permit and deny.
* If permit condition match, packet will be allowed to pass from interface.
* If deny condition match, packet will be destroyed immediately.
* Every ACL has a default deny statement at end of it.
* If a packet does not meet with any condition, it will be destroyed (by the last deny condition).
* Empty ACL will permit all traffic by default. Implicit deny condition will not work with empty ACL.
* Implicit (default last deny) condition would work only if ACL has at least one user defined condition.
* ACL can filter only the traffic passing from interface. It cannot filter the traffic originated from router on which it has been applied.
* Standard ACL can filter only the source IP address.
* Standard ACL should be placed near the destination devices.
* Extended ACL should be placed near the source devices.
* Each ACL needs a unique number or name.
* We can have only one ACL applied to an interface in each direction; inbound and outbound.

That’s all for this part. In next part of this article I will explain Standard Access Control List configuration commands in detail with examples.

**7.6 NAT**

When communicating to devices in a public network, your device needs to use a source address that is a public address. NAT device enables private IPv4 to connect to the Internet. NAT enable you to change an IP address in a packet to a different address. Usually, NAT connects two networks and translates the private (inside local) addresses into public addresses (inside global) before packets are forwarded to another network. In other word Address translation allows you to translate your internal private addresses to public addresses before these packets leave your network.

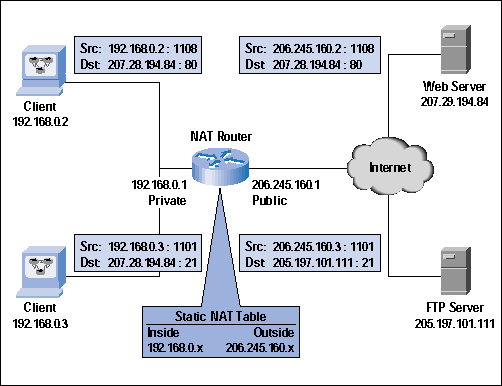
### Situation where you should use NAT

* Your ISP did not provide you sufficient public IP address
* Your company is going to merge in a company which use same address space
* Where you want to hide your internal IP address space from outside
* You want to assign the same IP address to multiple machines

### There are three types of NAT

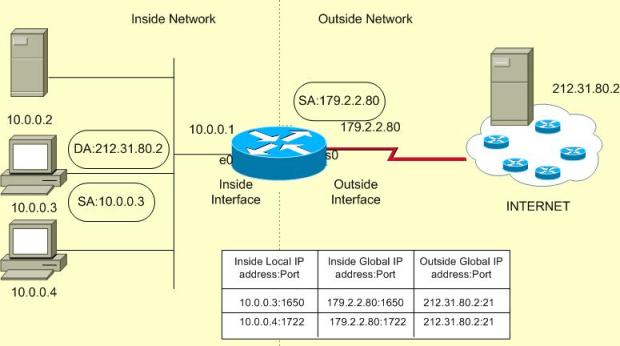
* Static
* Dynamic
* PAT

## **STATIC NAT**



In static NAT manual translation is performed by an address translation device, translating one IP address to a different one. If you have 100 devices, you need to create 100 static entries in the address translation table. Typically, static translation is done for inside resources that outside people want to access.

## **Dynamic NAT**

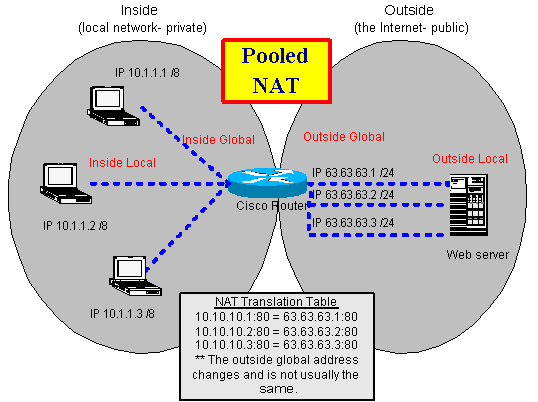


Dynamic NAT is mostly used when inside users needs to access outside resources. The global address assigned to the internal user isn't important, since outside devices don't directly connect to your internal users they just return traffic to them that the inside user requested.

Dynamic NAT is used when inside use wants to access external resource. When an inside user sends traffic through the address translation device, say a router, it examines the source IP address and compares it to the internal local address pool. If it finds a match, then it determines which inside global address pool it should use for the translation. It then dynamically picks an address in the global address pool that is not currently assigned to an inside device. The router adds this entry in its address translation table, the packet is translated, and the packet is then sent to the outside world. If no matching entry is found in the local address pool, the address is not translated and is forwarded to the outside world in its original state.

When returning traffic comes back into your network, the address translation device examines the destination IP addresses and checks them against the address translation table. Upon finding a matching entry, it converts the global inside address to the local inside address in the destination IP address field of the packet header and forwards the packet to the inside network

## **PAT**



With PAT, all devices that go through the address translation device have the same global IP address assigned to them, so the source TCP or UDP port numbers are used to differentiate the different connections. If two devices have the same source port number, the translation device changes one of them to ensure uniqueness.

Major difference between NAT and PAT is In NAT Only IP addresses are translated (not port numbers).

### Disadvantages of Address Translation

Three main disadvantage with address translation are:

* Each connection has an added delay.
* Troubleshooting is more difficult.
* Not all applications work with address translation.

## **Address Translation Terms and Types**

|  |  |
| --- | --- |
| **Term** | **Explanation** |
| Inside | Addresses located on the inside of your network |
| Outside | Addresses located outside of your network |
| Local | The IP address physically assigned to a device |
| Global | The public IP address physically or logically assigned to a device |
| Inside local IP address | The IPv4 address that is assigned to a host on the inside network |
| Inside global IP address | A legitimate IPv4 address assigned by the ISP that represents one or more inside local IPv4 addresses to the outside world |
| Outside global IP address | An outside device with a registered public IP address |
| Outside local IP address | An outside device with an assigned private IP address |
| Static NAT | A manual address translation is performed between two addresses and possibly port numbers. |
| Dynamic NAT | An address translation device automatically performs address translation between two addresses and possibly port numbers. |
| Port Address Translation (PAT) | Many inside IP addresses are translated to a single IP address, where each inside address is given a different TCP or UDP port number for uniqueness. |

**Conclusion**

This chapter covers a very large and important area of computer security: networks and distributed applications. As the world becomes more connected by networks, the significance of network security will certainly continue to grow. Security issues for networks are visible and important, but their analysis is similar to the analysis done for other aspects of security. That is, we ask questions about what we are protecting and why we are protecting it.

In a sense, security in networks is the combination and culmination of everything we know about security, and certainly everything we have discussed in this book so far. A network's security depends on all the cryptographic tools at our disposal, good program development processes, operating system controls, trust and evaluation and assurance methods, and inference and aggregation controls.

Networks and their security remind us that good software engineering practices can go a long way toward making software difficult to attack. When a network and its components are structured, designed, and architected well, the resulting system presents solid defenses and avoids potential single points of failure. And a well-engineered network is easy to change as it evolves; because it is easier to understand, changes seldom introduce unintentional flaws.

Until now we have stressed technical controls, which can be very effective in protecting our computing assets. But many security losses come from trusted insiders—either honest people making honest, human mistakes or dishonest insiders able to capitalize on their knowledge or privileges. In the next chapter we consider administrative controls, such as security policies, user awareness, and risk analysis, as a way to address the insider threat.

**FUTURE SCOPE**

Active Networking is vital to career growth. Often confused with selling, Networking is actually about building long-term relationships and a good reputation over time. It involves meeting and getting to know people who you can assist, and who can potentially help you in return. Your network includes everyone from friends and family to work colleagues and members of groups to which you belong.

In today’s word networking is most necessary but everyone wants a secured network in this project I used NAT which provide us a fully secured LAN network. Security is much more difficult in network; this project can control the user of network and make a secure network. In this project, we replace a router with a pc. In this project ACL used which provide us the service to deny any service from the network.

**References**

1. <https://www.google.co.in/search?q=local+area+network&source=lnms&tbm=isch&sa=X&ved=0ahUKEwig7PTKsMbTAhUJuY8KHdbqBEoQ_AUIBigB&biw=1366&bih=613#tbm=isch&q=local+area+network+for+collegehttp://>
2. <http://vfu.bg/en/e-Learning/Computer-Networks--Introduction_Computer_Networking.pdf>
3. <http://www.sfu.ca/~sihengw/ENSC427_Group9/Final%20Report%20.pdf>
4. <http://research.ijcaonline.org/volume48/number18/pxc3880401.pdf>
5. <http://www.cisco.com/c/en/us/td/docs/net_mgmt/active_network_abstraction/3-7/reference/guide/ANARefGuide37.pdf>
6. <http://digitalcommons.uncfsu.edu/cgi/viewcontent.cgi?article=1011&context=macsc_wp>
7. <http://ieeexplore.ieee.org/document/5474509/>
8. <http://phucchau.tran.free.fr/book/O%27Reilly%20->
9. <http://www.net130.com/tutorial/cisco-pdf/routingtcpipv1.pdf>
10. <ftp://ftp.hp.com/pub/networking/software/A-C13-Adv_Routing.pdf>
11. http://cd1.edb.hkedcity.net/cd/tech\_edu/handout/Files/Computer\_Networking\_and\_Data\_Communications\_Day3\_AM.pdf