NETWORK SECURITY WITH RESPECT TO ROUTING,

BY

EDEKE PATRICK

PGD/MCS/2007/1229

A PROJECT SUBMITTED TO THE DEPARTMENT OF MATHEMATICS /COMPUTER SCIENCE, FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF POST – GRADUATE DIPLOMA IN COMPUTER SCIENCE

JULY, 2010

DECLARATION

I Patrick Edeke declare that this research is my original work and to the best of my knowledge has not been carried out by any other person, neither has it been presented else where for the award of any degree.

_____ _____

Patrick Edeke **Date**

CERTIFICATION

This is to certify that the work carried out by EDEKE Patrick meets the regulation governing the award of Postgraduate Diploma in Computer Science in the department of Mathematics and Computer Science, in the School of Science Education Federal University of Technology, Minna.

Alhaji Danladi Hakimi	_____	_____
Supervisor	Signature	Date
Dr. U Y Abubakar	_____	_____
Head of Department	Signature	Date
External Examiner	_____	_____
	Signature	Date

DEDICATION

For Late.Chief Efanga Luke Edeke (Popsy) & Late. Dr. Jane Uno (Momsy), Cyril & Lorenzo. God Almighty the Alpha & Omega.

ACKNOWLEDGEMENT

Though weeping may endureth for the night; Joy doeth comes in the morning.

I give honour to GOD Almighty for His unending blessings from His inexhaustible store of grace and for benevolently supporting me throughout the course of this programme.

My profound gratitude goes to my supervisor Alhaji Danladi Hakimi for his thorough supervision and constructive criticism of the project. It is also my desire to thank the Head of Department, Dr. N.I Akinwande, , Dr M. Jiya, Engr. Abba Suleiman, Mr Abraham O, Mr Idris Onotu, Dr. V.O. Waziri and Mal. A. Ndanusa for his unsurpassed understanding and all lecturers in the department.

My deepest admiration goes to M D Ladan (my miracle) whose timely intervention in my being is an act of God. Mr Lawrence Edeke who has always been there even to a fault. Surveyor Ndekedekhe Uno, Late.Mr Kingsley Onyeama (Choco), Mr Kenneth Chukwuemeka Onyeama (Papin) The Ochiaga 1 of Minna, Engr. Micheal Edeke, Mr. Mathew Adamu (2pac), Mal. Aliyu Abubakar Isah, Ms Tolu Johnson, Ms Miriam Chukwu, Mr Philip Uno, Mr Victor Uno and a host of many personalities too numerous to mention. I pray that God in His infinite mercies will grant you all your heart desires.

Conclusively, my sincere and heartfelt appreciation goes out to Mr Gbolohan A. Bolarin without him this research work would have been but a mirage, I will like to say a big thank you to all my course mates. It has been a joy ride all the way with you guys. God will meet you all at the point of your needs.

TABLE OF CONTENTS

ABSTRACT

Computer networking and its essence cannot be over emphasize as this technology have brought about easy, cheap and fastest means of information transfer using computers across the globe. Relevant as it is, computer users stand the risk of compromising the sacredness of information to a set of well developed persons referred to as hackers and crackers, who pilfer for competition or fun, or better still financial reasons as this culminate to most of this activities. This project work is aimed at showing the construction of wide area network (WAN) and how to impede those threats posed by the hackers and crackers alike.

CHAPTER ONE

1.0 GENERAL INTRODUCTION

1.1 Introduction

Computers and computer networking have evolved over the years. The process of invention and commercialization are complicated the by making the history of computer networking complex.

Computers were large electromechanical devices prone to failure in the 1940's. Semi-conductor transistor invention created the possibility of building smaller and more reliable computers in 1947. The evolution was a continuous one and in 1950's large institution began using the mainframe computers that were run by punch card programs. Not until the late 1950's did the integrated circuit s that has several millions of transistors on one small piece of semi-conductor was invented.

Smaller computers referred to as minicomputers came into existence in the late 1960's and early 1970's. Although these minicomputers were considerable large by modern standards. Microcomputers came to limelight in 1977, introduce by Apple computer company. This gave birth to the concept of personal computer, IBM then introduce its first personal computer in 1981. The widespread use of computers at home came as a result of the user-friendly MAC, the open architecture IBM personal computer and the further micro-miniaturization of integrated circuits.

The u sage of the point-to-point or dial-up concept materialised in the mid 1980's, this involves the sharing of files by a user with a stand-alone computer using modems to connect to other computers. Further expansion was done on this concept by the use of computer (bulletin boards) that was the central point

of communication in a dial-up connection. This concept had its limitations and draw backs as each bulletin board required one modem per connection.

All through the 60's to the 90's, the Department of Defence were engaged in the development of a wide area networks (WAN) for military and scientific reasons. This was obviously design to combat the limitations of encountered in the dial-up/point-to-point communication used in bulletin boards. It had the capacity of allowing multiple users using different paths. The network itself would determine how to move data to and fro from one computer to another, instead just being able to communicate with one computer at a time.

The Department of Defence WAN gave birth to the INTERNET (networks of all networks). The overall importance and significance of the INTERNET in our everyday life should be given an underscore. It is a valuable resource and connection to it is essential for education, business, industry, medicine, to mention but a few.

Connecting to the internet requires careful planning as the internet is a public place. Security of information is often very vital. At the rate at which security threats is proliferating in computer networks, it won't be out place to place system security in a higher scale when setting up a computer network.

System security has two aspects; the first being the security system built to protect physical hardware against theft, vandalization, etc. The second being data security which comes under the aegis of data protection. Data security protects data against unauthorized access. Certain information is considered inviolable as such their sanctity must be protected. Be that as it may be, some individuals (members of the public or those of the company) may want to pry into such inaccessible areas either for espionage reason or to gratify their

curiosity just for the fun of it. For whatever reasons, this activity is not allowed as it is criminal and will put the establishment in a bad situation.

1.2 Statement of The Problem

Now as in the past, data integrity which form the major bedrock has at one time or the other been faced with a lot of problems. Poor security measures and the nefarious activities of hackers and crackers have made this problem an uneasy one to solve..

This twin problem has inhibited the integrity and security of data in a networked organisation. This can also be said about the lackadaisical attitude that are exhibited by the human software that are suppose to ensure the integrity and security of these data.

The time is come for networked organisations to eliminate this problem. There is no doubt that every networked organisation is incapable of healthy development unless the integrity and security of its data is guaranteed.

1.3 Aims and Objectives

1.3.1 Aims of The Study

The level of success of any networked organization is dependent on how much security is applied to their systems. The aim of this project is to highlight the insecurity nature of a networked organization by hackers and crackers alike.

This work is also poised at highlighting and understanding clearly the security risks faced in connecting to the internet and probably proffers measures that could be affected to combat and counter such problems.

1.3.2 Objectives of The Study

The objectives of this study are as follows;

1. How routers allow for the completion of a network design, implementation and setting up the physical layout of the network to ensure security.

2. How routers can be used to checkmate the nefarious activities of hackers and crackers alike.

3. That configuring the router correctly with basic router configuration and setting up a TFTP server on one of the workstations shall be of upmost importance when trying to set-up a security system for a networked organization.

4. How to create and apply access control lists (ACL) on the appropriate router and interface, and to also troubleshoot and test all connectivity on access control lists.

1.4 Methodology

There are many methods employed by different people to secure data; amongst are:

a) Password method :- obviously one of the oldest methods of data security.

b) Biometrics :- used to protect data by validating a user's access right through finger prints, voice recognition, capillary patterns in the retina of a person's eye, e.t.c.

c) Smart card technology:- which involves the use of magnetic card which allows a user to access data after inserting it into a smart card reader attached to a client computer.

d) Authenticating control mechanism:- fitted with an encryption system to facilitate encoding or making of data.

The method intended to be used in this course work is in respect to routing (routers). This involves the use of routing protocols by routers to determine the path a packet/data could take to a remote destination. This is done by configuring the routers and updating the router about the internetwork.

1.5 Significance of The Study

The benefits of this course work cannot be overemphasis bearing in mind that the world is going dynamically in the information technology era. The integrity and safeguarding of data is of utmost priority. This project work is deem at highlighting different methods protecting data with particular respect to the use of routers. Different Governmental organisations are deposed to using this method to safeguard their vital information.

The banking industry that deals in a very volatile set of data have over the years adopted this method of data security as they are involved in sending a host of data across the public network (internet) in retrospect any organisation or individual whose quest is to preserve the integrity of data is advised to adopt this method of data security.

1.6 Scope/ Limitation of The Study

To research security policies and their effectiveness with emphasis on the current events with network administrators shall be the intent of this study. This study will also try to deal completely and comprehensively with how computer

internet operating system (IOS) works for this reasons, the of this project work will be restricted around network security with respect to routers.

The knowledge of Networking (LAN and WAN) will be relevant as it pertains to facilitate they use of routers in network security. A security system on its own remains an abstract entity or concept if it does not secure any defined system, it is therefore pertinent to build an application that will drive the essence and logic of the security system to a concrete pedestal. It will be worthwhile to mention that the limitations encountered with this work was time constraint that was pertinently coupled with financial problems.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Security Concept

Security covers a wide range of issues amongst them are software based and relate to maintaining the integrity of the network, its resources and its devices (Yusuf, 2004). It also means ensuring that programs cannot inadvertently access memory they are not cleared to use by the operating system and that one program cannot tamper with or even damage the data belonging to another. Other issues involve caring for the physical well being of the network and its data through measures such as fire proofing and regularly scheduled data backups. Several approaches have covered the network in ensuring that people and programs are legitimate and communications cannot readily be hijacked by electronic eavesdroppers.

More security concepts lie in protecting the internal network from access by unauthorized individuals and also protecting the transportation of information over the internet. It is of great importance that, the privacy and security of people's personal financial information should be jealously guarded (John,2004).

2.2 Security Approaches

Encryption, which is used to scramble transmitted data and make them unreadable; and virtual private network, which use a tunneling to turn the public internet into a secure communications medium, is some of the techniques and approaches deployed when securing the network. The use of software devices such as digital signature is another approach.

Encryption

Though digital signatures are valuable in the authentication and validation of programs and messages, encryption of important files before essentially transmitting them is an even higher level of security approach (Tyson & Jeff, 2001). This involves turning the files to unreadable gibberish to everyone but the sender and the receiver. The process involves turning a readable message (plain text) into a garbled version (cipher text) for transmission.

Virtual Private Network (VPN)

A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger networks (such as the Internet), as opposed to running across a single private network (Andrew, 2002). The Link Layer protocols of the virtual network are said to be tunneled through the transport network. One common application is to secure communications through the public Internet, but a VPN does not need to have explicit security features such as authentication or content encryption. For example, VPNs can also be used to separate the traffic of different user communities over an underlying network with strong security features, or to provide access to a network via customized or private routing mechanisms.

VPN service providers may offer best-effort performance, or may have a defined service level agreement (SLA) with their VPN customers. Generally, a VPN has a topology more complex than point-to-point.

Tunneling protocols can be used in a point-to-point topology that would generally not be considered a VPN, because a VPN is expected to support

arbitrary and changing sets of network nodes (Townsley, 1999). Since most router implementations support software-defined tunnel interface, customer-provisioned VPNs often comprise simply a set of tunnels over which conventional routing protocols run. Provider-Provisioned VPNs (PPVPNs), however, need to support the coexistence of multiple VPNs, hidden from one another, but operated by the same service provider.

From the security standpoint, VPNs either trust the underlying delivery network, or must enforce security with mechanisms in the VPN itself. Unless the trusted delivery network runs only among physically secure sites, both trusted and secure models need an authentication mechanism for users to gain access to the VPN.

Authentication before VPN connection

A known trusted user, sometimes only when using trusted devices, can be provided with appropriate security privileges to access resources not available to general users. Servers may also need to authenticate themselves to join the VPN.

A wide variety of authentication mechanisms exist. VPNs may implement authentication in devices including firewalls, access gateways, and others. They may use passwords, biometrics, or cryptographic methods. Strong authentication involves combining cryptography with another authentication mechanism. The authentication mechanism may require explicit user action, or may be embedded in the VPN client or the workstation.

Trusted Delivery Networks

Trusted VPNs (sometimes referred to APNs - Actual Private Networks) do not use cryptographic tunneling, and instead rely on the security of a single provider's network to protect the traffic. In a sense, they elaborate on traditional network- and system-administration work.

- Multi-Protocol Label Switching (MPLS) is often used to overlay VPNs, often with quality-of-service control over a trusted delivery network.
- Layer 2 Tunneling Protocol (L2TP) which is a standards-based replacement, and a compromise taking the good features from each, for two proprietary VPN protocols: Cisco's Layer 2 Forwarding (L2F) (obsolete as of 2009) and Microsoft's Point-to-Point Tunneling Protocol (PPTP).

Security Mechanisms

Secure VPNs use cryptographic tunneling protocols to provide the intended confidentiality (blocking snooping and thus Packet sniffing), sender authentication (blocking identity spoofing), and message integrity (blocking message alteration) to achieve privacy. When properly chosen, implemented, and operated, such techniques can provide secure communications over unsecured networks.

Secure VPN protocols include the following:

- IPsec (IP security) - commonly used over IPv4, and a "standard option" in IPv6.

- SSL/TLS, used either for tunneling the entire network traffic, as in the OpenVPN project, or for securing what is, essentially, a web proxy is called SSL VPN. SSL, though a framework more often associated with e-commerce, has been built-upon by a number of vendors to provide remote access VPN capabilities. A major practical advantage of an SSL VPN is that it can be accessed from the locations that restrict external access to SSL-based e-commerce websites only, thereby preventing VPN connectivity using IPsec protocols. SSL-based VPNs are vulnerable to trivial Denial of Service attacks mounted against their TCP connections because latter are inherently unauthenticated.

- Open VPN, an open standard VPN. A variation of SSL VPN, it can run over UDP. Clients and servers are available for all major operating systems.

- DTLS, used by Cisco for a next generation VPN product called Cisco AnyConnect VPN. DTLS solves the issues found when tunneling TCP over TCP as is the case with SSL/TLS

- SSTP from Microsoft introduced in Windows Server 2008 and Windows Vista Service Pack 1. SSTP tunnels PPP or L2TP traffic through an SSL 3.0 channel.

- L2TPv3 (Layer 2 Tunneling Protocol version 3), a new release.

- VPN Quarantine. The client machine at the end of a VPN could be a threat and a source of attack; this has no connection with VPN design and most VPN providers leave it to system administration to secure. There are solutions that provide VPN Quarantine services which run end point checks on the remote client while the client is kept in a quarantine zone until healthy. Microsoft ISA Server 2004/2006 together with VPN-Q 2006 from Winfrasoft or an application called QSS (Quarantine Security Suite) provides this functionality.

- MPVPN (Multi Path Virtual Private Network). Ragula Systems Development Company owns the registered trademark "MPVPN".

- Cisco VPN, a proprietary VPN used by many Cisco hardware devices. Proprietary clients exist for all platforms; open-source clients also exist.

Mobile VPNs are VPNs for mobile and wireless users. They apply standards-based authentication and encryption technologies to secure communications with mobile devices and to protect networks from unauthorized users. Designed for wireless environments, Mobile VPNs provide an access solution for mobile users who require secure access to information and applications over a variety of wired and wireless networks. Mobile VPNs allow users to roam seamlessly across IP-based networks and in and out of wireless-coverage areas without losing application sessions or dropping the secure VPN session. For instance, highway patrol officers require access to mission-critical applications as they travel between different subnets of a mobile network, much as a cellular radio has to hand off its link to repeaters at different cell towers.

The Host Identity Protocol (HIP), under study by the Internet Engineering Task Force, is designed to support mobility of hosts by separating the role of IP addresses for host identification from their locator functionality in an IP network. With HIP a mobile host maintains its logical connections established via the host identity identifier while associating with different IP addresses when roaming between access networks.

Basically, a VPN is a private network that uses a public network (internet) to connect remote sites of users together. Instead of using a dedicated, real-world connections such as leased lines, a uses a "virtual" connections routed through the internet from the organisation's private network to the remote site or employee. In essence, VPN is a cost-effective means of using a public network (internet) to provide secure, private, computer-to-computer communications between Local Area Network (LAN) and between Wide Area Network (WAN).

Digital Signature

A digital signature or digital signature scheme is a type of asymmetric cryptography (Whitfie, 1976). For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything representable as a bitstring:

examples include electronic mail, contracts, or a message sent via some other cryptographic protocol (katz & Lindell, 2007).

A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

- A signing algorithm which, given a message and a private key, produces a signature.

- A signature verifying algorithm which given a message, public key and a signature, either accepts or rejects.

Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify on that message and the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

In their foundational paper, Goldwasser, Micali, and Rivest lay out a hierarchy of attack models against digital signatures:

1. In a key-only attack, the attacker is only given the public verification key.
2. In a known message attack, the attacker is given valid signatures for a variety of messages known by the attacker but not chosen by the attacker.
3. In an adaptive chosen message attack, the attacker first learns signatures on arbitrary messages of the attacker's choice.

They also describe a hierarchy of attack results:

1. A total break results in the recovery of the signing key.
2. A universal forgery attack results in the ability to forge signatures for any message.
3. A selective forgery attack results in a signature on a message of the adversary's choice.
4. An existential forgery merely results in some valid message/signature pair not already known to the adversary.

The strongest notion of security, therefore, is security against existential forgery under an adaptive chosen message attack.

Some common reasons for applying a digital signature to communications include:

Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages (Anna, 2002). When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as non-malleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature will invalidate the signature (Shafi, Silvio & Ronald,1988). Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

Additional Security Precautions

Putting the Private Key on a Smart Card

All public key / private key cryptosystems depend entirely on keeping the private key secret (Leslie,1979). A private key can be stored on a user's computer, and protected by a local password, but this has two disadvantages:

- the user can only sign documents on that particular computer
- the security of the private key depends entirely on the security of the computer

A more secure alternative is to store the private key on a smart card. Many smart cards are designed to be tamper-resistant. In a typical digital signature implementation, the hash calculated from the document is sent to the smart card, whose CPU encrypts the hash using the stored private key of the user, and then

returns the encrypted hash. Typically, a user must activate his smart card by entering a personal identification number or PIN code (thus providing two-factor authentication). If the smart card is stolen, the thief will still need the PIN code to generate a digital signature (Wenbo, 2004). This reduces the security of the scheme to that of the PIN system, although it still requires an attacker to possess the card. A mitigating factor is that private keys, if generated and stored on smart cards, are usually regarded as difficult to copy, and are assumed to exist in exactly one copy. Thus, the loss of the smart card may be detected by the owner and the corresponding certificate can be immediately revoked. Private keys that are protected by software only may be easier to copy, and such compromises are far more difficult to detect.

Using Smart Card Readers with a Separate Keyboard

Entering a PIN code to activate the smart card commonly requires a numeric keypad. Some card readers have their own numeric keypad. This is safer than using a card reader integrated into a PC, and then entering the PIN using that computer's keyboard (Michael, 1979). Readers with a numeric keypad are meant to circumvent the eavesdropping threat where the computer might be running a keystroke logger, potentially compromising the PIN code. Specialized card readers are also less vulnerable to tampering with their software or hardware and are often EAL3 certified.

Some Digital Signature Algorithms

- Full Domain Hash, RSA-PSS etc., based on RSA
- DSA
- ECDSA
- ElGamal signature scheme
- Undeniable signature
- SHA (typically SHA-1) with RSA
- Rabin signature algorithm
- Pointcheval-Stern signature algorithm
- BLS
- Schnorr signature
- ECQV
- Aggregate signature - a signature scheme that supports aggregation: Given n signatures on n messages from n users, it is possible to aggregate all these signatures into a single signature whose size is constant in the number of users. This single signature will convince the verifier that the n users did indeed sign the n original messages.

Proxy

In computer networks, a proxy server is a server (a computer system or an application program) that acts as a go-between for requests from clients seeking resources from other servers (Andrew, 2002). A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides

the resource by connecting to the relevant server and requesting the service on behalf of the client. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server. In this case, it 'caches' responses from the remote server, and returns subsequent requests for the same content directly.

A proxy server has two purposes:

- To keep machines behind it anonymous (mainly for security).
- To speed up access to a resource (via caching). It is commonly used to cache web pages from a web server.

A proxy server that passes requests and replies unmodified is usually called a gateway or sometimes tunneling proxy.

A proxy server can be placed in the user's local computer or at various points between the user and the destination servers or the Internet. A reverse proxy is a proxy used as a front-end to accelerate and cache in-demand resources (such as a web page).

Redundant Array of Inexpensive Disks (R.A.I.D)

This is a multi-level set of strategies concentrated on protecting the data on network disks (Sean, 2004). It is the repository of virtually everything that travels over, or stored on the network. R.A.I.D basically protects data by mirroring (duplicating) data or by stripping data across multiple disks.

2.3 Networking Concept

Anyone that you might want to meet or contact in the world is only five to six people contacts away from you.

A healthy and active link to a network is a vast resource available to every individual at a low personal cost. It can help you to achieve a range of goals that otherwise might be too hard or out of reach.

A key point to understand is that networking is achieved at low personal cost (Wendell, 2001). I am not suggesting that networking is a quick fix or fad idea that can be easily adopted to make things better for a while. However, it can provide immediate results for those prepared to invest their time and energy.

Many of the definitions of networking highlighted may surprise some people, in as much as they suggest that networking is an altruistic activity involving giving and sharing, rather than taking.

In summary, networking definitions may include;

- A power that comes from a spirit of giving and sharing.

- A willingness to honour ourselves, our relationship and our connections with the universal flow.

- A way of sending out into the system what we have and what we know, and having it return to re-calculate continually through the network.

- An organised way of creating links from people we know to people they know for a specific purpose.

- Giving, contributing to and supporting others without keeping score.

• People caring about people.

• Fostering self-help, and the exchange of information; seeking to change society and work life and to share resources.

• Ensuring the right to ask a favour without hooks.

2.4 Network Topology

In computer networking, topology refers to the layout of connected devices (John, 2004). This article introduces the standard topologies of networking.

Think of a topology as a network's virtual shape or structure. This shape does not necessarily correspond to the actual physical layout of the devices on the network. For example, the computers on a home LAN may be arranged in a circle in a family room, but it would be highly unlikely to find a ring topology there.

Network topologies are categorized into the following basic types:

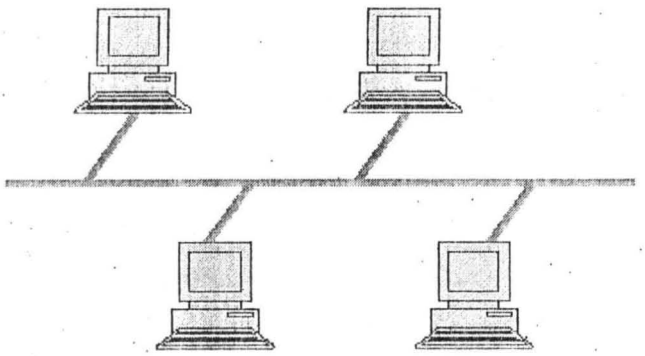
- bus
- ring
- star
- tree
- mesh

More complex networks can be built as hybrids of two or more of the above basic topologies.

Bus Topology

Bus networks use a common backbone to connect all devices. A single cable that is the backbone, functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.

Ethernet bus topologies are relatively easy to install and don't require much cabling compared to the alternatives. 10Base-2 ("ThinNet") and 10Base-5 ("ThickNet") both were popular Ethernet cabling options many years ago for bus topologies. However, bus networks work best with a limited number of devices. If more than a few dozen computers are added to a network bus, performance problems will likely result. In addition, if the backbone cable fails, the entire network effectively becomes unusable.

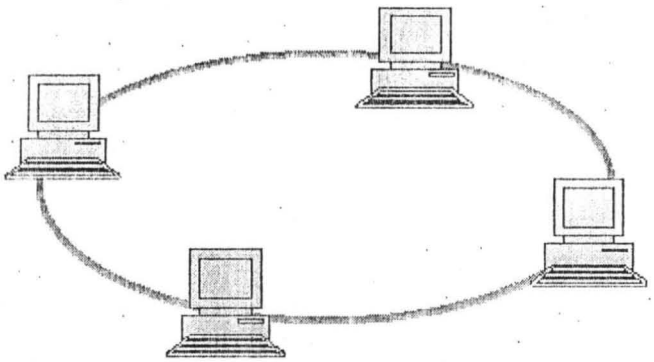


Ring Topology

In a ring network, every device has exactly two neighbours for communication purposes. All messages travel through a ring in the same direction (either

"clockwise" or "anticlockwise"). A failure in any cable or device breaks the loop and can take down the entire network.

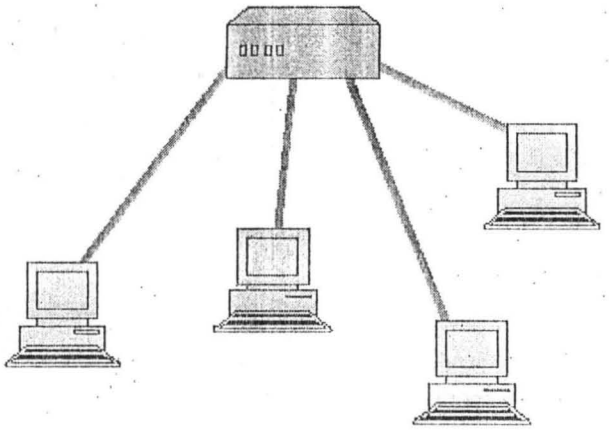
To implement a ring network, one typically uses FDDI, SONET, or Token Ring technology. Ring topologies are found in some office buildings or school campuses.



Star Topology

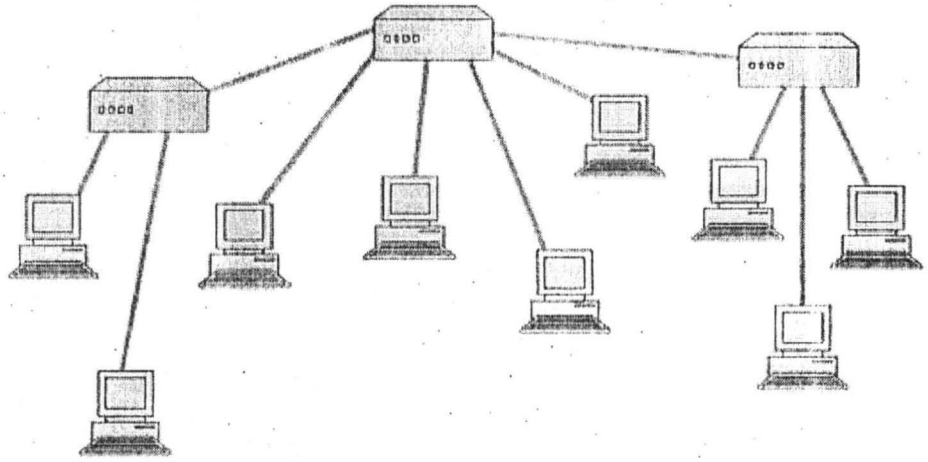
Many home networks use the star topology. A star network features a central connection point called a "hub" that may be a hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.

Compared to the bus topology, a star network generally requires more cable, but a failure in any star network cable will only take down one computer's network access and not the entire LAN. (If the hub fails, however, the entire network also fails.)



Tree Topology

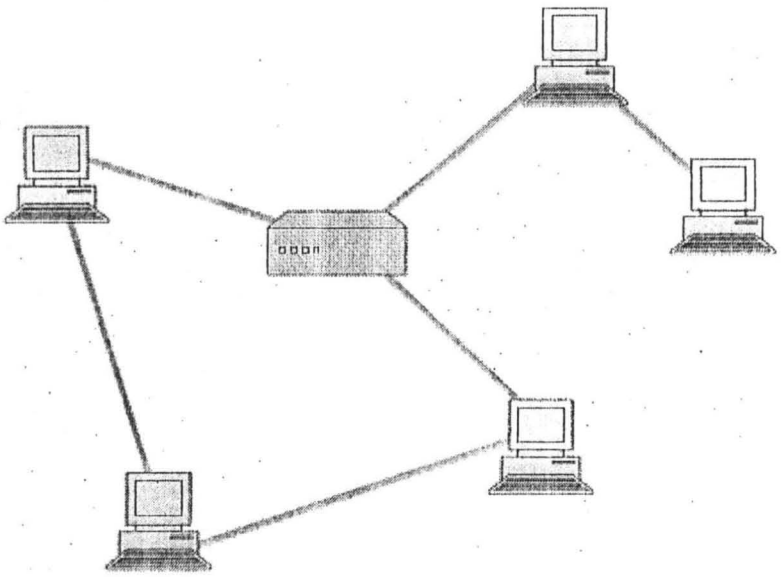
Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus and each hub functions as the "root" of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.



Mesh Topology

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that even in a ring, although two cable paths exist, messages can only travel in one direction.) Some WANs, most notably the Internet, employ mesh routing.

A mesh network in which every device connects to every other is called a full mesh. As shown in the illustration below, partial mesh networks also exist in which some devices connect only indirectly to others.



Summarily, topologies remain an important part of network design theory. One can probably build a home or small business computer network without understanding the difference between a bus design and a star design, but becoming familiar with the standard topologies gives you a better understanding of important networking concepts like hubs, broadcasts, and routes.

2.5 Networking Tools

Network tools are devices used during the set up of a network either local area network (LAN), or wide area network (WAN), and virtual private network (VPN).

Router: A network device that transmits packets message, routing them over the best route available at the time. Routers are used to connect multiple segments, including those based on different architectures and protocols.

Repeater: A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances.

Because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the Physical layer, the first layer of the OSI model.

Digipeater: A "digipeater" is a blend meaning "digital repeater", particularly used in amateur radio. Store and forward digipeaters generally receive a packet radio transmission and then retransmit it on the same frequency, unlike repeaters that receive on one and transmit on another frequency. A digipeater that is placed in the path between the two end stations reduces the effective "throughput" by 50% since each digipeater has to spend half it's time listening and half transmitting.

Repeaters are often used in trans-continental and submarine communications cables, because the attenuation (signal loss) over such distances would be unacceptable without them. Repeaters are used in both copper-wire cables carrying electrical signals, and in fibre optics carrying light.

Bridge: A bridge can be used to connect networks, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN

Brouter: A Bridge Router or brouter is a network device that works as a bridge and as a router. The brouter routes packets for known protocols and simply forwards all other packets as a bridge would.

Brouters operate at both the network layer for routable protocols and at the data link layer for non-routable protocols. As networks continue to become more complex, a mix of routable and non-routable protocols has led to the need for the combined features of bridges and routers. Brouters handle both routable and non-routable features by acting as routers for routable protocols and bridges for non-routable protocols. Bridged protocols might propagate throughout the network, but techniques such as filtering and learning might be used to reduce potential congestion.

Switch: A network switch is a computer networking device that connects network segments.

The term commonly refers to a Network bridge that processes and routes data at the Data link layer (layer 2) of the OSI model. Switches that additionally process data at the Network layer (layer 3 and above) are often referred to as Layer 3 switches or Multilayer switches.

The term network switch does not generally encompass unintelligent or passive network devices such as hubs and repeaters.

As with hubs, Ethernet implementations of network switches support either 10/100 Mbit/s or 10/100/1000 Mbit/s ports Ethernet standards. Large switches may have 10 Gbit/s ports. Switches differ from hubs in that they can have ports of different speed.

The network switch, packet switch (or just switch) plays an integral part in most Ethernet local area networks or LANs. Mid-to-large sized LANs contain a number of linked managed switches. Small office, home office (SOHO) applications typically use a single switch, or an all-purpose converged device such as gateway access to small office/home office broadband services such as DSL router or cable, Wi-Fi router. In most of these cases, the end user device contains a router and components that interface to the particular physical broadband technology, as in the Linksys 8-port and 48-port devices.

RJ-45: Registered Jack 45 is a connector used with twisted-pair wiring, similar to telephone jack but larger than telephone jack.

Hub: A device that operates on the physical layer that, distribute an inbound network signal to many outbound connections. Hub can either be active, passive or intelligent largely dependent on the mode of operations. Active when it acts as a connection point and possesses the ability to regenerate signals while passive when it simply act as a connection point. When it has additional capabilities of configuring a network, it is said to be intelligent.

2.6 Connecting A Network

Connecting a network has to do with a physical and logical connection. The physical connection is done by connecting a specialized expansion card such as a modem or a network interface card (NIC) from a computer to a network (Larry & Bruce, 2003). Protocols are used in the logical connection. A protocol is a formal description of a set of rules and conventions that govern how devices on a network communicate.

A network is connected using at least two workstations; it might be connected to the internet or simple between two computers.

2.6.1 Ethernet:

Ethernet is a local area technology connected devices in close proximity. It is a widely used network that formed the basis for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard for bus networks that rely on CSMA/CD to control network transmissions (Worcester Polytechnic Institute, 2008). The basic frame format and the IEEE sub layers of OSI layers 1 and 2 remain consistent across all forms of Ethernet. Ethernet speed can be 10Mpbs, 100Mpbs, 1000Mpbs or 10000Mpbs.

2.6.2 Token Ring

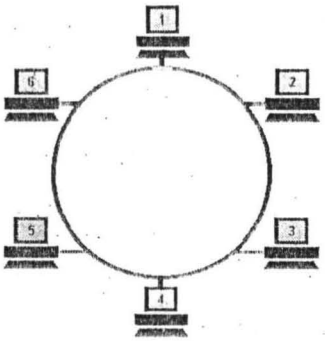
A Token Ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time (Andrew, 2003). The Token Ring

protocol is the second most widely-used protocol on local area networks after Ethernet. The IBM Token Ring protocol led to a standard version, specified as IEEE 802.5. Both protocols are used and are very similar. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second. Very briefly, here is how it works:

1. Empty information frames are continuously circulated on the ring.
2. When a computer has a message to send, it inserts a token in an empty frame (this may consist of simply changing a 0 to a 1 in the token bit part of the frame) and inserts a message and a destination identifier in the frame.
3. The frame is then examined by each successive workstation. If the workstation sees that it is the destination for the message, it copies the message from the frame and changes the token back to 0.
4. When the frame gets back to the originator, it sees that the token has been changed to 0 and that the message has been copied and received. It removes the message from the frame.
5. The frame continues to circulate as an "empty" frame, ready to be taken by a workstation when it has a message to send.

The token scheme can also be used with bus topology LANs.

The standard for the Token Ring protocol is Institute of Electrical and Electronics Engineers (IEEE) 802.5. The Fiber Distributed-Data Interface (FDDI) also uses a



In the example above, machine 1 wants to send some data to machine 4, so it first has to capture the free Token. It then writes its data and the recipient's address onto the Token.

The packet of data is then sent to machine 2 who reads the address, realizes it is not its own, so passes it on to machine 3. Machine 3 does the same and passes the Token on to machine 4.

This time it is the correct address and so number 4 reads the message. It cannot, however, release a free Token on to the ring; it must first send the message back to number 1 with an acknowledgement to say that it has received the data

The receipt is then sent to machine 5 who checks the address, realizes that it is not its own and so forwards it on to the next machine in the ring, number 6.

Machine 6 does the same and forwards the data to number 1, who sent the original message.

Machine 1 recognizes the address, reads the acknowledgement from number 4 and then releases the free Token back on to the ring ready for the next machine to use.

That's the basics of Token Ring and it shows how data is sent, received and acknowledged, but Token Ring also has a built in management and recovery

system which makes it very fault tolerant. Below is a brief outline of Token Ring's self maintenance system.

Token Ring Self Maintenance

When a Token Ring network starts up, the machines all take part in a negotiation to decide who will control the ring, or become the 'Active Monitor' to give it its proper title. This is won by the machine with the highest MAC address who is participating in the contention procedure, and all other machines become 'Standby Monitors'.

The job of the Active Monitor is to make sure that none of the machines are causing problems on the network, and to re-establish the ring after a break or an error has occurred. The Active Monitor performs Ring Polling every seven seconds and ring purges when there appears to be a problem. The ring polling allows all machines on the network to find out who is participating in the ring and to learn the address of their Nearest Active Upstream Neighbour (NAUN). Ring purges reset the ring after an interruption or loss of data is reported.

Each machine knows the address of its Nearest Active Upstream Neighbour. This is an important function in a Token Ring as it updates the information required to re-establish itself when machines enter or leave the ring.

When a machine enters the ring it performs a lobe test to verify that its own connection is working properly, if it passes, it sends a voltage to the hub which operates a relay to insert it into the ring.

If a problem occurs anywhere on the ring, the machine that is immediately after the fault will cease to receive signals. If this situation continues for a short period of time it initiates a recovery procedure which assumes that its

NAUN is at fault, the outcome of this procedure either removes its neighbour from the ring or it removes itself.

2.7 Internet Protocol (IP) Networking

The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP (Siyan, 1997).

IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose the Internet Protocol defines addressing methods and structures for datagram encapsulation (Valencia, 1998). The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4) is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6) is being deployed actively worldwide.

2.7.1 Internet Protocol (IP) Encapsulation

Data from an upper layer protocol is encapsulated as packets/datagrams (the terms are basically synonymous in IP). Circuit setup is not needed before a host may send packets to another host that it has previously not communicated with (a characteristic of packet-switched networks), thus IP is a connectionless protocol. This is in contrast to Public Switched Telephone Networks that require the setup of a circuit before a phone call may go through (connection-oriented protocol).

Because of the abstraction provided by encapsulation, IP can be used over a heterogeneous network, i.e., a network connecting computers may consist of a combination of Ethernet, ATM, FDDI, Wi-Fi, token ring, or others. Each link layer implementation may have its own method of addressing (or possibly the complete lack of it), with a corresponding need to resolve IP addresses to data link addresses. This address resolution is handled by the Address Resolution Protocol (ARP) for IPv4 and Neighbor Discovery Protocol (NDP) for IPv6.

2.7.2 Internet Protocol (IP) Routing

Routing protocols are protocols used by a router to determine the path a packet could take to a remote destination.

Types of Routing

- Static Routing
- Default Routing
- Dynamic Routing

Static Routing entails the administrator manually updating the router about the internetwork.

Router (Config)# IP route<IP add of remote network><subnet mask>

<next hop router interface><AD>

Router A(Config)#IP route192.168.30.1, 255.255.255.0

192.168.10.2

Static routing occurs when you manually add routes in each router's routing table.

Default Routing uses default to send packets to a remote destination network not in the routing table to the next hop router. It is used only on stub networks (networks one exit path out of the network)

Router (Config)#IP classless

Dynamic Routing is when protocols are used to find networks and update routing tables on routers.

A routing protocol defines a set of rules used by a router when it communicates routing information between neighbour routers.

2.8 Network Address

Perhaps the most complex aspects of IP are IP addressing and routing. Addressing refers to how end hosts become assigned IP addresses and how subnetworks of IP host addresses are divided and grouped together (Valencia, 1998). IP routing is performed by all hosts, but most importantly by internetwork routers, which typically use either interior gateway protocols (IGPs) or external gateway protocols (EGPs) to help make IP datagram forwarding decisions across IP connected networks

2.9 Local Area Network (LAN)

A local area network (LAN) is a computer network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an airport (TTC Mobile Manual, 2008). The defining characteristics of LANs, in contrast to wide-area networks (WANs). include their usually higher data-

transfer rates, smaller geographic place, and lack of a need for leased telecommunication lines.

Ethernet over unshielded twisted pair cabling, and Wi-Fi are the two most common technologies currently in use.

Early LAN cabling had always been based on various grades of co-axial cable, but IBM's Token Ring used shielded twisted pair cabling of their own design, and in 1984 StarLAN showed the potential of simple Cat3 unshielded twisted pair; the same simple cable used for telephone systems. This led to the development of 10Base-T (and its successors) and structured cabling which is still the basis of most LANs today.

Although switched Ethernet is now the most common data link layer protocol and IP as a network layer protocol, many different options have been used, and some continue to be popular in niche areas. Smaller LANs generally consist of one or more switches linked to each other, often with one connected to a router, cable modem, or ADSL modem for Internet access.

Larger LANs are characterized by their use of redundant links with switches using the spanning tree protocol to prevent loops, their ability to manage differing traffic types via quality of service (QoS), and to segregate traffic via VLANs. Larger LANS also contain a wide variety of network devices such as switches, firewalls, routers, load balancers, sensors and so on.

LANs may have connections with other LANs via leased lines, leased services, or by 'tunneling' across the Internet using VPN technologies. Depending on how the connections are made and secured, and the distance involved, they become a Metropolitan Area Network (MAN), a Wide Area Network (WAN), or a part of the Internet.

2.9.1 Wireless Local Area Network (WLAN)

A wireless LAN (WLAN) is a wireless local area network that links two or more computers or devices using spread-spectrum or OFDM modulation technology based to enable communication between devices in a limited area (TTC Mobile Manual, 2008). This gives users the mobility to move around within a broad coverage area and still be connected to the network.

For the home user, wireless has become popular due to ease of installation, and location freedom with the gaining popularity of laptops.

Advantages

The popularity of wireless LANs is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless LAN technology. Benefits of wireless LANs include:

Convenience: The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.

Mobility: With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.

Productivity: Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location. For example, a hospital or warehouse may implement Voice over WLAN applications that enable mobility and cost savings.

Deployment: Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).

Expandability: Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.

Cost: Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labour associated to running physical cables.

Disadvantage

Wireless LAN technology, while replete with the conveniences and advantages described above has its share of downfalls. For a given networking situation, wireless LANs may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology.

Security: Wireless LAN transceivers are designed to serve computers throughout a structure with uninterrupted service using radio frequencies. Because of space and cost, the antennas typically present on wireless networking cards in the end computers are generally relatively poor. In order to properly receive signals using such limited antennas throughout even a modest area, the wireless LAN transceiver utilizes a fairly considerable amount of power. What this means is that not only can the wireless packets be intercepted by a nearby adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user. In fact, there are even computer users dedicated to locating and sometimes even cracking into wireless networks, known as wardrivers. On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires, but this is not an issue with wireless packets. To combat this consideration, wireless networks users usually choose to utilize various encryption technologies available such as Wi-Fi Protected Access (WPA).

Range: The typical range of a common 802.11g network with standard equipment is on the order of tens of metres. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly.

Reliability: Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects (such as multipath, or especially in this case Rician fading) that are beyond the control of the network administrator. Among the most insidious

problems that can affect the stability and reliability of a wireless LAN are microwave ovens and analog wireless transmitters such as baby monitors. In the case of typical networks, modulation is achieved by complicated forms of phase-shift keying (PSK) or quadrature amplitude modulation (QAM), making interference and propagation effects all the more disturbing. As a result, important network resources such as servers are rarely connected wirelessly.

Speed: The speed on most wireless networks (typically 1-108 Mbit/s) is reasonably slow compared to the slowest common wired networks (100 Mbit/s up to several Gbit/s). There are also performance issues caused by TCP and its built-in congestion avoidance. For most users, however, this observation is irrelevant since the speed bottleneck is not in the wireless routing but rather in the outside network connectivity itself. For example, the maximum asymmetrical digital subscriber line (ADSL) throughput (usually 8 Mbit/s or less) offered by telecommunications companies to general-purpose customers is already far slower than the slowest wireless network to which it is typically connected. That is to say, in most environments, a wireless network running at its slowest speed is still faster than the internet connection serving it in the first place. However, in specialized environments, higher throughput through a wired network might be necessary. Newer standards such as 802.11n are addressing this limitation and will support peak throughput in the range of 100-200 Mbit/s.

Architecture

Stations

All components that can connect into a wireless medium in a network are referred to as stations.

All stations are equipped with wireless network interface cards (WNICs).

Wireless stations fall into one of two categories: access points, and clients.

Access points (APs), normally routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with.

Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

Basic service set

The basic service set (BSS) is a set of all stations that can communicate with each other.

There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS.

Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

An independent BSS (IBSS) is an ad-hoc network that contains no access points, which means they cannot connect to any other basic service set.

An infrastructure can communicate with other stations not in the same basic service set by communicating through access points.

Extended service set

An extended service set (ESS) is a set of connected BSSes. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

Distribution system

A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells.

Peer-to-Peer Wireless LANs

An ad-hoc network is a network where stations communicate only peer to peer (P2P) (TTC Mobile Manual, 2008). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).

A peer-to-peer (P2P) network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network.

If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer.

802.11 specs define the physical layer (PHY) and MAC (Media Access Control) layers. However, unlike most other IEEE specs, 802.11 includes three alternative PHY standards: diffuse infrared operating at 1 Mbit/s in; frequency-hopping spread spectrum operating at 1 Mbit/s or 2 Mbit/s; and direct-sequence spread spectrum operating at 1 Mbit/s or 2 Mbit/s. A single 802.11 MAC standard is based on CSMA/CA (Carrier Sense Multiple Access with Collision

Avoidance). The 802.11 specification includes provisions designed to minimize collisions. Because two mobile units may both are in range of a common access point, but not in range of each other. The 802.11 has two basic modes of operation: Ad hoc mode enables peer-to-peer transmission between mobile units. Infrastructure mode in which mobile units communicate through an access point that serves as a bridge to a wired network infrastructure is the more common wireless LAN application the one being covered. Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included shared-key encryption mechanisms: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA, WPA2), to secure wireless computer networks

2.10 Concept Of Virtual LAN Operation (VLAN).

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location (Vinton & Robert, 1974). A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. By definition, switches may not bridge IP traffic between VLANs as it would violate the integrity of the VLAN broadcast domain.

This is also useful if someone wants to create multiple Layer 3 networks on the same Layer 2 switch. For example if a DHCP server (which will broadcast its presence) were plugged into a switch it would serve anyone on that switch that was configured to do so. By using VLANs you easily split the network up so some hosts won't use that server and default to Link-local addresses.

Virtual LANs are essentially Layer 2 constructs, compared with IP subnets which are Layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN or have one subnet spread across multiple VLANs. Virtual LANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to one another and this correspondence is useful during the network design process.

By using VLAN, one can control traffic patterns and react quickly to relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration.

2.10.1 Requirements For Inter-VLAN Communication

It is important to point out that you don't have to configure a VLAN until your network gets so large and has so much traffic that you need one. Many times, people are simply using VLAN's because the network they are working on was already using them.

For inter-VLAN communication there has to be a router and switches must be configured as trunk ports.

Another important fact is that, on a Cisco switch, VLAN's are enabled by default and ALL devices are already in a VLAN. The VLAN that all devices are already in is VLAN 1. So, by default, you can just use all the ports on a switch and all devices will be able to talk to one another.

When a VLAN is needed?

You need to consider using VLAN's in any of the following situations:

- You have more than 200 devices on your LAN
- You have a lot of broadcast traffic on your LAN
- Groups of users need more security or are being slowed down by too many broadcasts?
- Groups of users need to be on the same broadcast domain because they are running the same applications. An example would be a company that has VoIP phones. The users using the phone could be on a different VLAN, not with the regular users.
- Or, just to make a single switch into multiple virtual switches.

Why Not Just Subnet My Network?

A common question is why not just subnet the network instead of using VLAN's? Each VLAN is a separate broadcast domain and has its own subnet mast. The benefit that a VLAN provides over a subnetted network is that devices in different physical locations, not going back to the same router, can be on the same network. The limitation of subnetting a network with a router is that all devices on that subnet must be connected to the same switch and that switch must be connected to a port on the router.

Types Of Link In VLAN

1) **Access link** allows switch port to be a member of one VLAN. Features of Access link include;
   - The use of straight through cables to connect switch to host
   - It carries only one VLAN traffic
2) **Trunk link** allows for inter-switch and inter-VLAN communication. Features of Trunk link include;
   - It carries a traffic of multiple VLAN
   - It facilitates inter-VLAN connection when connected to a layer 3 device
   - A Trunk link can carry traffic of a multiple VLAN up to 1005 at the same time.

VLAN Frame Tagging

This simply refers to frame identification methods. In frame tagging, user defined ID are uniquely assigned to each frame for specific VLANs. It is also referred to as VLAN ID. Each VLAN is assigned a VLAN ID that uniquely identifies which VLAN it belongs.

Types of Frame Tagging

1) **802.1q** is the IEEE frame tag encapsulation. It is used to encapsulate non-Cisco devices and switches. 2950 switches support 802.1q

2) **Interswitch link (ISL):** Cisco proprietary protocol that is used only with Cisco devices. It is default frame tagging encapsulation on all Cisco devices.

VLAN Trunking Protocol (VTP)

VTP was created by Cisco, its main objective being to manage all configured VLANs across a switched internetwork. It also maintains consistency throughout that network. To get a VTP to manage a network, a VTP server must be created.

Configuring a VTP server.

2950 (Config)# vtp mode server

Device mode already VTP server

2950 (Config)# vtp domain ttc

2950 # copy run start

Configuring Trunk Ports

2950 (Config) # int f0/11

2950 (Config) # switch port mode trunk

2950 (Config) # speed 100

2950 (Config) # duplex full

Repeat these set of commands for all trunk ports

Configuring a VTP client

2950 (Config) # vtp mode client

2950 # copy run start

Configuring access ports for a specific VLAN

2950 (Config) # int f0/1

2950 (Config-if) # switch port access VLAN 2

2950 # copy run start

2950 (Config) # int fo/2

2950 (Config-if) # switch port access VLAN 3

2950 # copy run start

Configuring the VTP for a remote network management

2950 (Config) #enable secret Cisco

2950 (Config) # line con 0

2950 (Config-line) # password Cisco

2950 (Config-line) # login

2950 (Config-line) # exit

2950 (Config) # int VLAN 1

2950 (Config-if) # IP add 192.168.10.2, 255.255.255.224

2950 # copy run sart

Configuring VLAN

In a 2950 switch, create VLAN in the privilege mode of the VTP server

2950 # VLAN database

2950 (VLAN) # VLAN 2 name finance

2950 (VLAN) # VLAN 3 name medical

2950 (VLAN) # apply

2950 (VLAN) # exit

2950 # copy run start

2.11 Wide Area Network (WAN)

A wide area network (WAN) is a data communication network spanning a large geographical area such as state, province or country. Transmission facilities provided by common carriers are often used by WAN. Several characteristics distinguish WAN from LAN, these includes;

- They connect devices that are separated by wide geographical areas.
- They used the service of carriers such as the Regional Bell Operating Companies.

- They use serial connections of various types of access bandwidth over large geographical areas.
- A wide area network (WAN) operates at the physical layer and the data link layer of the OSI reference model. It interconnects LANs that are separated by large geographical areas. WAN provide for the exchange of data packets and frames between routers and switches and the LAN they support.

2.12 Bandwidth

The amount of data/information that can flow through a network connection in a given period of time is referred to as bandwidth (Computer Association of Nigeria, 2002). Bandwidth measurement is based on the type of signal, analog or digital used in carrying the data/information.

Analog:- These are the type of signal used in radios and voice telephone where data/information travels as a continuously variable wave.

Digital:- This is the signal that allows data/information to travel in a discrete on/off pulse over the communication medium. These signals are typical of modems.

Throughput:- This refers to the actual measure of bandwidth at a specific time of day using specific internet routes while a specific set of data/information is transmitted on the network.

Common factors that determine throughput,

- Type of data being transferred.
- Network topology
- Number of host on the network
- User computer
- Server computer
- Power conditions

Limitations

Bandwidth variation depends largely on the type of media as well as the LAN and WAN technology being used. Signal travel through twisted-pair copper wire, coaxial cable, optical fibre and air. The physical differences in the way s signal travel result in the fundamental limitations on the data/information carrying capacity of a given medium. However, the actual bandwidth of a network is determined by a combination of the physical media and the technology chosen for signaling and detection of network signals.

Importance of Bandwidth

It is essential to understand the concept of bandwidth when studying networking for the following reasons;

Bandwidth is not free. It is possible to buy equipment for a local area network (LAN) that will provide nearly unlimited bandwidth over a long period of time. For wide area network (WAN) connections, it is almost always necessary to buy bandwidth from a service provider. The decision on the right material and equipments to use is the responsibility of the network manager.

Bandwidth is finite. Regardless of the media used to build the network, there are limits on the capacity of that network to carry data/information. Optical fibre has the physical potential to provide virtually limitless bandwidth.

Bandwidth is a key factor in analyzing network performance, designing new networks and understanding the internet. Understanding the tremendous impact of bandwidth and throughput on network design and performance is quite important. Information flow as a string bits from computer to computer throughout the world.

CHAPTER THREE

3.0 SYSTEM ANALYSIS AND DESIGN

3.1 Introduction

Routers are network devices that transmit message packets, routing them over the best route available at a time. A router has the ability to make intelligent decisions regarding the best path for delivery of data on the network (Balabi, 2000). Routers are basically used to connect multiple network segments including those based on differing architectures and protocols.

Cisco technology is built around the Cisco Internetwork Operating System (IOS) which is the software that controls the routing and switching functions of internetworking devices.

3.2 Internal Components of A Router

The exact architecture of a router varies between router models, notwithstanding they share common major internal components.

Central Processing Unit (CPU): Obviously the brain of the router that is saddled with the responsibility of executing instructions in the operating system. Among its task are; system initialization, routing functions and network interface control. The CPU is a microprocessor.

Random Access Memory (RAM): It is basically used for routing table information, fast switching cache, running configuration and packet queues. RAM provides run time space for executable Cisco IOS software and its subsystems in most routers. RAM contents are lost when power is removed.

They are generally dynamic random access memory (DRAM) and be upgraded by adding dual-in-line memory modules (DIMM).

Flash: The flash memory is used for the storage of a full Cisco IOS software image. The router normally acquires the default IOS from the flash. These images can be upgraded by loading a new image into the flash. An executable copy of the IOS is transferred to the RAM during the boot process in most routers, while the IOS may be directly from the flash in other routers.

Non Volatile Random Access Memory (NVRAM): This used to store the start-up configuration of the router. NVRAM is implemented using separate electronically erasable programmable read-only-memory (EEPRAM).

Interface: The LAN, WAN and Console/AUX ports make up the router interface. The LAN interface has controller chips that provide the logic for connecting the system to the media. The WAN interface includes serial port, ISDN and integrated channel service units (CSU). They also have special controller chips for the interfaces; these may be fixed configuration or modular. The Console/AUX ports are serial ports primarily used for the initial configuration of the router. They are used for terminal sessions from the communication ports on the computer or through a modem.

Read Only Memory (ROM): Used for permanent storage of start up diagnostic code (ROM monitor).Its main task is hardware diagnostics during router boot up and leading the Cisco IOS software from flash to RAM.

Buses: The system bus and CPU bus are major components of most routers. The system bus is used for communication between the CPU and the interfaces and/or expansion slots, while the later is used by the CPU for accessing components from router storage. The bus is known for the transfer of instructions and data to and from specific addresses.

Power Supply: It provides the necessary power to operate the internal components. Larger routers use multiple or modular power supply. In some smaller routers, power supply may be external to the router.

3.3 External Components of A Router

A router connection is made of three types: LAN interface, WAN interface and management port.

LAN interface allows the router to connect to the local area network media. This is usually some form of Ethernet. It could also be another form of LAN technology such as Token Ring or Asynchronous Transfer Mode (ATM).

Wide Area Network connections provide connections through a service provider to a distant site or the internet. This is usually a serial connection or any number of other WAN interfaces. A CSU is required to connect the router to the local connection of the service provider in some type of WAN interface, while with others the router may be connected directly to the service provider.

Management Port provides a text-based connection for the configuration and troubleshooting of the router. The management interfaces are the console and auxiliary ports which are E1A-232 asynchronous serial ports. They are connected to the communication port of the host.

3.3.1 Connecting LAN Interface

The router is usually connected to the LAN using an Ethernet or fast Ethernet interface. It communicates with the LAN via a hub/switch using a straight-through cable for the connection.

In situation where the router is directly connected to a computer or another router, a crossover cable is required. The correct interface should be used, for damage could occur to the router or other networking devices if the wrong interface is used.

The eight pin RJ-45, RJ-48 or RJ-49 is the connector required to connect these interface.

3.3.2 Connecting WAN Interface

WAN services are usually leased from service providers. The Customer Premises Equipment (CPE) is to the Data Terminal Equipment (DTE) which is connected to the service provider using data circuit terminating equipment (DCE) device, commonly a modem or channel service unit/data service unit (CSU/DSU). This device converts data from the DTE into an acceptable form to the WAN service provider.

3.3.3 Management Port Connections

The console ports and the auxiliary ports are the asynchronous serial ports designed as the management ports. The console port is used for the initial configuration of the router. To prepare the router for initial start-up and configuration, an RS-232 ASCII terminal is attached to the system console port and then configuration commands can be entered to set up the router.

The auxiliary port is rarely used except in situation where the router configured so as to be connected to a modem to use a telephone line.

Once the initial configuration is entered into the router through the management port, the router can then be connected to the network for monitoring or troubleshooting. The control displays router start-up, debugging and error messages by default, it can also be when the networking services have not been started or have failed. The control port can be used for password recovery.

3.4 Router User Interface

The Cisco IOS software uses a command-line interface (CLI) as the traditional console environment. The IOS is a core technology that extends across most of the Cisco product line. This environment is accessible through different methods, one of them being through a console session. A console uses slow serial connections directly from a computer/terminal to the console connection on the router. The CLI can also be accessed by the use of a dial-up connection using a modem or null modem connected to the router. To establish a Telnet session with the router, at least one interface must be configured with IP address and virtual terminal session must be configured for login and passwords.

Router User Interface Modes

The Cisco command line interface uses a hierarchical structure that requires entry into different modes to accomplish particular tasks. For instance, to configure a router interface, the user must enter interface configuration mode. All configuration entered apply only to that particular interface. Each configuration mode is indicated with a distinctive prompt and allows only commands that are appropriate for that mode.

The IOS provides a command interpreter service known as the command executive (EXEC). The EXEC validates and executes a command after it has been entered. The Cisco IOS is also serving as a security feature that separates

the EXEC sessions into two access levels viz user EXEC mode and privileged EXEC mode.

The user EXEC mode often referred to as the "view-only" mode allows only a limited number of basic monitoring commands. It does not allow any command that might change the configuration of the router.

The privilege EXEC mode accesses all router commands. It can be configure to demand for user password before accessing it, for added security it can also be configured to require a user ID. This allows only authorised users to access the router.

3.5 Router LAN And WAN

Even though router can be use to segment a LAN, its major use is a WAN device. Routers have both LAN and WAN interfaces. WAN technologies are frequently used to connect routers and they communicate with each other by WAN connections. Routers are the backbone of large intranets and the internet. They operate at layer 3 of the OSI model, making decisions based on network addresses. The two major functions of a router are the selection of best path for and the switching of frames to the proper interface. Routers accomplish this by building routing tables and exchanging network information with other routers. A router may be exclusively a LAN or WAN device or it may sit at the boundary between a LAN and a WAN.

A WAN is said to operate at the physical layer and at the data link layer. This does not mean that the other five layers of the OSI model are not found in a WAN, it simply means that the characteristics that separate a WAN from a LAN are typically found at the physical layer and the data link layer. One of the major roles of a router in WAN is to route packets at layer 3 which is also

obtainable in LAN. Therefore the primary role of a router in Wan is to provide connections to and between the various WAN physical and data link standards.

3.6 Routing Basics

The Cisco operating system or Cisco IOS is the operating system software of most routers. It is the embedded software architecture in all Cisco routers and also the operating system of the catalyst switches. It is no news that, without the operating system the hardware does not have any capabilities.

The Cisco internetwork operating systems posses three distinctive operating modes;

CISCO IOS:- The operation of a router requires the use of the full Cisco IOS image as stored in the flash. The IOS is executed directly from the flash in some devices, however, most Cisco routers require a copy of the IOS loaded into RAM and also executed from RAM. Some IOS images are stored in the in flash in compressed format and have to be expanded when copied to RAM.

ROM MONITOR:- This performs the bootstrap process and provides low-level functionality and diagnostics. It is used to recover from system failures and in the recovery of lost password; it cannot be accessed through any of the network interfaces. It can only be accessed by way of a direct, physical connection through the console port.

BOOT ROM:- The router allows a limited subset of the Cisco feature when it is running in Boot ROM. Boot ROM is primarily used to replace the Cisco IOS image that is stored in flash.

CHAPTER FOUR

4.0 IMPLEMENTATION

4.1 Networking Security With Respect To Routing

It is the responsibility of the network administrator to figure out how to deny unwanted access to the network while providing internal users with appropriate access to necessary services. Security tools like password, call-backs equipment and physical security devices are helpful; they often lack the flexibility of basic traffic filtering and specific controls most administrators prefer. For instance, a network administrator might want to grant users access to the internet but not permit external users telnet access to or into the local area network (LAN).

Routers provide basic traffic filtering capabilities, such as blocking internet traffic with access control list (ACL). An ACL is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols (Vinton and Robert,1974). ACL can be as simple as a single line intended to permit packets from a specific host. Or they can be extremely complex sets of rules and conditions that can precisely define traffic and shape the performance of router processes.

4.2 Wide-Area Internet Routing Security

Routing is the process by which a packet is sent from one place to another. Every packet has a source and a destination, and routing is the mechanism which determines the path a packet should take in order to reach the specified destination (Vinton and Robert,1974). Routing on the Internet can be classified into two areas: local routing and wide-area routing. Local routing transports a packet to a host within particular network once it has reached that network.

Wide-area internet routing deals with transporting a packet between networks, i.e., across the Internet itself.

One of the burgeoning problems that is yet to be appropriately addressed from a practical standpoint is the security of wide-area Internet routing. Various researches have proposed authenticated route advertisements, which are explored below. Certain wide-area routing protocols have attempted to address some of the security issues associated with internet routing. However, some of the fundamental questions remain with respect to wide-area internet routing security, including the following:

1. Does the issue of wide area routing boil down to a problem of authentication, or is it more fundamentally an issue of robustness? Specifically, in the context of wide area routing, is the threat really a malicious user injecting bad routes into the Internet infrastructure, or rather is it simply a problem of designing an extension to the exterior gateway protocols that is robust to operator error?
2. Who and what are the legitimate threats in such a case? Often, the ability to do large-scale damage implies access to a backbone router; therefore, are these entities really vulnerable to "script kiddies," or should we really only be concerned with people who might have access to the Internet's backbone routers (i.e., the previously fired network administrators of large ISPs)?

A brief overview of the Border Gateway Protocol (BGP), the protocol currently used as a communication between routers to disseminate routing information between autonomous systems will be considered. Next, will be the exploration of some historical "attacks" that employ BGP and also consideration of current research in these areas, such as Secure BGP (S-BGP).

Overview of BGP

The Border Gateway Protocol (BGP) is an exterior gateway protocol which is used to distribute routing information in the Internet. From the perspective of BGP, the Internet is partitioned into a number of autonomous systems (AS), each of which performs their own internal routing (usually done by applying an open shortest-path first (OSPF) algorithm, such as Dijkstra's algorithm). An autonomous system is typically established as a particular administrative domain. An ISP such as BBN is AS-1; MIT is AS-3. However, link state protocols do not scale to the size of the Internet, because they require each router to have a consistent, accurate view of the entire network topology, and involve flooding, i.e., sending messages on every output link, thus generating a high amount of extraneous traffic. BGP, on the other hand, has mechanisms to prevent routing loops between autonomous systems, and it scales well because it is incremental: once routes are established, only changes (i.e., "updates" and "withdrawals") are advertised.

Each AS then has a BGP speaker, a router which runs the BGP routing process, which advertises all of the networks for which it has reachability information, i.e., all of the networks for which it has a path to reach. If a particular AS wants traffic to be routed to it for a given set of addresses, it then advertises those networks through a route advertisement. Similarly, an AS can also agree to be a "transit-AS": if one AS gains information about another network's reachability via another AS, it can advertise that it has reachability to that network, too, if it agrees to route packets to that network. BGP is a "path-vector" routing protocol; that is, advertisements include an attribute known as the AS-PATH, a list of AS that much be traversed to reach the advertised network. Inclusion of the AS-PATH attribute also allows routing loops to be easily detected. Path vector

algorithms such as BGP scale linearly with the number of nodes (AS's), rather than with the square of the number of nodes, as link-state protocols scale.

The basic idea here is that the Internet is partitioned into administrative domains called autonomous systems, and that each AS advertises the set of networks that it knows how to reach. With this basic understanding of BGP, it's possible now to examine some of the historical attacks mounted against BGP, as well as some of the threats associated with the protocol.

Threats

Misconfiguration

There is one particularly well known example of damage that can be caused by misconfiguring a BGP peer. This occurs when a particular AS (say "AS-10") is transited by two other AS's (AS-20 and AS-30), both of which send full BGP tables to that AS. Misconfiguration occurs as follows:

- When AS-10 hears the full BGP tables from the other ASes, it will redistribute these routes internally within the AS (using iBGP, OSPF, etc.)
- The routing table of AS-10 is then redistributed back to the exterior BGP as originating from AS-10.
- Now AS-20 and AS-30 think that the entire internet originates within the AS-10 network.

The upshot is that all Internet-bound traffic from any AS that is peering with AS-10 will attempt to route traffic through AS-10, thus saturating the network and making the Internet inaccessible to these peers.

This assumes that the AS is not performing any filtering of iBGP messages with respect to its eBGP announcements.

Lack of Filtering

An AS can filter out certain route announcements based on certain attributes. For example, if a certain AS receives an announcement from an IP address that it does not recognize, or is not from a certain AS, then it will not accept that route advertisement. Many of the large internet service providers (ISPs), such as Sprint, AT&T, UUNet, etc., who provide access to the Internet backbone, do not filter out these routes. This is largely due to the fact that most entities obtain their Internet access from smaller ISPs (Qwest, etc.). When a smaller ISP adds a new user/network, it wants to be able to grant that user instant connectivity, and not have to tell the larger ISP that it's OK to advertise routes to these new networks. As a result, many of the larger ISP's perform no filtering of updates at all. Accepting all routes indiscriminately obviously provides potential for misconfiguration and catastrophic failure.

Blackholing

"Blackholing" a route essentially occurs when a particular AS announces a route to a network that that AS essentially does not have. Any peer that hears an update corresponding to a blackholed route will send packets to the AS destined for the blackholed route, and packets will be dropped. It has been asserted that blackholing is one of the most effective denials of service attacks on the internet to date.

One example of purposeful blackholing exists whereby an AS announces blackholed networks to peers via BGP multihop, and the next hop information (i.e., how to get to the next AS in the route) would be changed to an address which would simply drop the packets.

One particularly disturbing implication of this is that it is possible to target someone else's network and blackhole it by announcing that you have a route to their network when you in fact don't. An indication that your network has been blackholed is a sudden drop in traffic to your network.

An interesting man-in-the-middle attack can also be performed in a blackholing-type fashion, if a malicious AS announces a route that it wants to blackhole, but then establishes a machine on its internal network that performs some of the same functionality as the machine on the blackholed network. This might allow such an attack as masquerading as the machine that the end host thinks it is talking to, or simply sniffing all traffic that is sent between two end hosts.

Blackholing can be accomplished if the AS is not filtering its iBGP update messages, or via forged BGP "UPDATE" messages.

IP Spoofing

The forging of the opening of a BGP session is extremely difficult, because responses from the spoofed interface must also be disabled. Additionally, the end host will also be expecting full BGP tables, and route flapping, the frequent addition and withdrawal of a route from the routing tables; will surely occur if the session opening is not performed properly.

However, it is possible to insert forged BGP "UPDATE" messages (i.e., route updates) into an existing BGP session between two peers since the only sequence number included in the UPDATE packets are the TCP sequence

numbers. This means that a malicious AS could potentially spoof the BGP UPDATE messages; spoofing BGP update messages boils down to essentially performing spoofing of TCP messages. (Note that this attack is not possible against modern versions of Cisco's IOS.)

Defences

To protect against IP spoofing, Cisco's IOS allows the use of MD5 hashes for authentication of peers, and picks random TCP ISNs, thus making the insertion of a forged update message particularly difficult.

Additionally, Stephen Kent et al. have proposed a protocol referred to as Secure Border Gateway Protocol (S-BGP), which reportedly verifies the authenticity and authorization of BGP control traffic (particularly route update and withdrawal messages); furthermore, this protocol does not induce undue overhead and is incrementally deployable.

S-BGP must be adopted by ISPs, and requires PKI support by registries that allocate AS numbers to the ISPs. The architecture employs three main techniques: PKI, attestations, and IPsec. PKI is employed to verify IP address block ownership by a given AS, the relationship of an organization and a set of AS numbers, and BGP router IDs to AS numbers. Using this infrastructure, it is possible for BGP routers to authenticate one another. Attestations essentially allow each BGP speaker that receives a route advertisement to verify that each AS along the route is authorized to advertise the route and that the "origin" AS is authorized to advertise the given block of IP addresses. IPsec is used to provide data integrity with respect to the control information passed between two BGP speakers and also defends against replay attacks.

Security for wide-area Internet routing, specifically BGP, should be defined generally as the correct operation of BGP speakers, since any attack that inhibits this functionality could be considered successful. Specifically, a secure implementation of BGP ensures:

- integrity of UPDATE messages
- reliable receipt of messages by the intended recipients
- the peer sending the update is authorized to advertise the given information
- the AS that originates the route is authorized to represent the networks contained in the advertisement
- an AS withdrawing a route was previously authorized to advertise that route
- ASes in the AS-PATH attribute actually contain a valid path from the origin to the destination (to guard against cut-and-paste and replay attacks)

The unique aspect with regard to the security of Internet routing is that "secure" Internet routing fundamentally means "correct" Internet routing. As such, authentication mechanisms, protection against forged UPDATE messages, and similar protection are not silver bullets in any respect. In particular, correct Internet routing must prevent against the propagation of errors that can result from misconfiguration and emergent properties due to router interaction (i.e., Cisco routers with Bay routers, etc.), detecting anomalies appropriately, and generally ensuring the proper delivery of packets.

In the case of Internet routing, any operation that does not result in appropriate packet forwarding behaviour can be deemed an attack. It is clear that BGP is not robust to all of these attacks; furthermore, S-BGP still fails to address

misconfiguration issues (does it really matter whether a BGP speaker is authenticated or not if the operator is injecting erroneous routes into the Internet?). The challenge, then, is to devise a solution for robust wide-area Internet routing.

4.3 Access Control Lists (ACL)

The proper use and configuration of access lists is a vital part of router configuration. This is largely due to the fact that, access lists are a vital networking accessories contributing heavily to the efficiency and optimization of a network. Access lists enables network administrators considerable huge amount of control over traffic flow throughout the internetwork. With the use of access lists, administrators can obtain basic statistic on packet flow there by making possible the implementation of security policies.

ACL instructs the router on types of packets to accept or deny as the case may be.

Reasons for Access Control List (ACL)

It limits network traffic and increase network performance. By restricting video traffic, ACL could greatly reduce the network load and consequently increase network performance.

ACL are known to provide traffic flow control. It can restrict the delivery of routing updates, if updates are not required because of network conditions. Bandwidth is preserved.

ACL also provide a basic level of security for network access. It can allow one host to access a part of a network and prevent another host from accessing the same area. For instance, host A is allow access to the human resources network and host B is prevented from accessing it. It allows an administrator to control what areas a client can access on a network.

ACL decides which types of traffic are forwarded or blocked at the router interface. It permits e-mail traffic to be routed, but block all telnet traffic. It screens certain host so as to either allow or deny access to part of a network. It grants or denies user permission to access only certain types of files such as FTP or HTTP.

All packets passing through the router will be allowed on all parts of the network if ACL are not configured on the router.

How Access Control List (ACL) Work

ACL is a group of statements that define whether packets are accepted or rejected at inbound and outbound interfaces. These decisions are made by catching a condition statement in an access list and then performing to accept or reject action defined in the statement.

The order in which ACL statement are placed is important. The Cisco internetwork operating system (IOS) tests the packets against each condition statement in order from the top of the list to the bottom. Once a match is found in the list, accept or reject action is performed and no other ACL statement is checked. If a condition that permits all traffic is located at the top of the list, no statements added below that will ever be checked. If additional conditional statements are needed in an access list, the entire ACL must be deleted and recreated with the new condition statements. If the packet is accepted in the

interface, it will then be checked against routing table entries to determine the destination interface and switch to that interface. Next, the router checks whether the destination interface has an ACL; if an ACL exists, the packet is now tested against the statements in the list and if the packet matches a statement, the action of accepting or rejecting the packet is performed.

Creating Access Control List (ACL)

Access control list are created in the global configuration mode. During the configuration of the ACL on the router, each ACL must be uniquely identified by assigning a number to it. This number identifies the type of access list created and must fall within the range numbers that is valid for that type of access list. After the proper command mode is entered and the type number is decided upon, the user enters the access list statement using the keyword access-list, followed by the proper parameters. Creating the access list is the first half of using them on a router, the second half of the process is assigning them to the proper interface.

ACL are assigned to one or more interface and can filter inbound traffic or outbound traffic using the access-group command. This command is issued in the interface configuration mode. The filter direction can be set back to check packets that are travelling into or out of an interface.

When determining if the ACL is addressing inbound or outbound traffic, the network administrator needs to look at the interfaces from inside the router. It is of utmost importance to know the that traffic coming in from an interface is filtered by an inbound access list, traffic going out of the interface is filtered by the outbound access list.

Basic rules to be adhered to when creating and applying access list;

- One access list per protocol per direction.
- Standard access list should be applied closest to the destination
- Extended access list should be applied closest to the source
- Use the inbound and outbound interface as if you are looking at the port from inside the router
- Statements are sequentially processed from the top of the list to the bottom of the list until a match is found then the packet is denied
- There is an implicit deny at the end of all access list. This will not appear in the configuration listing
- Access list entries should filter in the order from specific to general. Specific host should be denied first before groups or general
- The match condition is examined first, the permit or deny is examined only if the match is true
- Never work with an access list that is actively applied
- Use a text editor to create comments outlining the logic then fill in the statement
- An IP access list will send an ICMP host unreachable message to the sender of the rejected packet and will discard the packet in the bit bucket
- Outbound filters do not affect traffic originating from the local router

Access Control List (ACL) Verification

These are many show commands that will verify the content and placement of ACL on the router. It is also a good practice to test the access list with sample traffic to ensure that the access list logic is correct.

The show IP interface command displays IP interface information and indicates whether any ACL are set.

The show access-list command displays the content of all ACL on the router. To see a specific list, add the ACL name or number as an option for this command.

The show running-configuration command will also reveal the access list on a router and the interface assignment information.

4.3.1 Access Control List (ACL) Types

Standard Access Control List:- The source addresses of the routed packets are checked by standard ACL. The comparison will result in either permit or deny access for an entire protocol suite, based on the network, subnet and host addresses. For instance, packets coming in FAO/O are checked for source address and protocol. If they are permitted, they packets are then routed through the router to an output interface. If they are not permitted, they are dropped at the incoming interface. The standard version of the access-list global configuration command is used to define a standard ACL with a number in the range of 1 to 99. The full syntax of the standard ACL command is

- Router (Config) #access-list

- Access-list-number (deny/permit) [source-wadcard] [log]

Extended Access Control List:- Extended ACL are often used more than the standard ACL because they provide greater range of control. This ACL checks the source and destination packets addresses as well as being able to check for protocols and port numbers. An extended ACL can allow e-mail traffic from FAO/O to specific SO/O destinations while denying file transfers and web browsing. Extended ACL uses an access-list number in the range 100 to 199.

The IP access-group command links an existing extended ACL to an interface. The format of the command goes thus;

- Router (Config) # IP access-group access-lists-number {in/out}

IP Named Access Control List:- IP named ACL were introduced in Cisco IOS software, allowing standard and extended ACL to be given names instead of numbers. A named ACL is created with the IP access-list command. This places the user in the ACL configuration mode that specifies one or more conditions to be permitted or denied. This determines whether the packet is passed or dropped when the ACL statement s matches. Its advantages include:

- Intuitively identify all ACL using an alphanumeric name

- Eliminate the limit of 789 simple and 799 extended ACL

- Named ACL provide the ability to modify ACL without deleting and then reconfigure.

Access Control List (ACL) Placing

If traffic is going to be filtered, ACL should be placed where it has the greatest impact on increasing efficiency. The general rule is to put the extended ACL as close as possible to the source of the traffic denied. Standard ACL do not specify destination addresses, so they should be placed as close to the destination as possible. An administration can only place an access list on a device that they control, therefore access list placement must be determined in the context of where the network administrator's control extends.

4.4 Firewall

A firewall is an architectural structure that exists between the user and the outside world to protect the internal network from intruders (Kent & Stephen, 2000). Network firewalls consist of several different machines that work together to prevent unwanted and illegal access. Firewalls, when deployed in conjunction with packet filtering routers, can be used to establish multi-layer, secure gateways throughout the ISP network. With the router configured to block all connections except those appropriate to specific servers, the firewall can be used to perform more fine-grained filtering of traffic. Firewalls can perform immense inspection of packets using knowledge of the specific application protocols being used. As a result, firewalls can allow easily-spoofed protocols, for example file transfer protocol (FTP) and most UDP-based protocols to pass safely through the firewall while dropping suspicious packets which are not received in the correct context.

Firewalls can be used to perform detailed logging of traffic to internal hosts, which is important for detecting any intrusion attempts. Encryption-enabled firewalls can be used to set up virtual private networks (VPN) which can be used in electronic commerce applications and for interconnecting remote corporate customers (Rekhter & Li, 1995). Finally, Network Address Translation (NAT) features can be used to hide internal network addresses, enhancing security and enabling an ISP to allocate more private IP addresses than they actually have available. Although firewalls can host proxy services, the most secure networks are protected by servers hosting only the firewall software.

4.4.1 Firewall Types

• CheckPoint FireWall-1 can be hosted on any Sun server, and it provides a good balance between cost and security. FireWall-1 addresses all of the security concerns discussed above, and also contains proxies which can be used both for ISP firewalls and for protecting corporate networks.

• SunScreen SPF-200 is a high-performance software solution that provides a significantly higher level of security by using a dedicated, hardened version of the Solaris operating environment. The most significant advantage to SunScreen SPF-200 is that it establishes a transparent network device with no IP address. Since it is invisible to intruders, it is highly impervious to intrusion. SunScreen SPF-200 can be installed on a wide range of Sun servers, allowing ISPs to configure firewalls to meet desired performance levels.

• SunScreen EFS has several benefits that are particularly important to ISPs. It utilizes the same enhanced packet filtering engine as SunScreen SPF-200 software. SunScreen EFS It is multi-threaded, which allows it to fully-utilize multiprocessor servers from Sun. It can be administered from a secure Web browser interface. Finally, SunScreen EFS is a low-cost approach that can be used to add an additional layer of security to each server within the ISP's firewall-protected sub-networks.

4.4.2 Firewall Categories

Generally firewalls can be categorized into four groups depending on their degree of security and the field where it is applied.

- Packet Filtering Gateways
- Application Gateways
- Hybrid Gateways
- Circuit Level Gateways

SUMMARY

Gateway Type	High Risk Environment	Medium Risk Environment	Low Risk Environment
Packet Filtering	Unacceptable	Minimal	Recommended
Application	Effective	Recommended	Effective
Hybrid	Recommended	Effective	Effective
Example	Hospital	University	Flower Shop

Packet Filtering Gateways

Packet filtering routers are the first line of defence, as they allow packets to be routed based on source and destination IP addresses, and source and destination TCP or UDP port numbers. This is the basic mechanism by which an ISP can ensure, for example, that only HTTP requests can be made of a Web server. Packet filtering routers are necessary, but not sufficient, for establishing a secure ISP network. A primary shortcoming is that routers do not provide a logging facility that can be used to detect and track intrusion attempts. Also, rule sets can be quite complex and prone to error. Finally, since routers are also stateless, they cannot perform complex analysis of transactions with internal hosts.

Advantages

- Fast
- Flexible
- Transparent
- Easy to filter access at host or network
- Inexpensive: can use existing router to implement.

Disadvantages

- Filtering is based only on source address, destination address or port
- Does not protect against IP or DNS address spoofing
- Attacker will have direct access to any host on the internal network
- Does not support strong user authentication
- Provides little or no audit trail
- Reveals internal network topology to outside network entities
- Does not provide enough granulation for most security policies
- Does not support certain traffic protocols

Application Gateways

Application gateways allow or drop packets by ensuring that the protocol specification is correct.

Application gateways are server- based programs termed proxy servers that run on a firewall. Proxies take external requests; examine them from a security perspective and then forward legitimate and trusted requests to the appropriate internal network host.

Advantages:

- Configure so that firewall is the only host address that is visible to an outside network.
- Use separate proxy servers for separate services (e.g. TELNET, FTP, HTTP, RLOGIN)
- Application gateways support strong user authentication
- Application gateways provide detail/audit controls at the application level.
- Strong user access controls

Disadvantages

- Requires special Proxy for each service (TELNET, FTP, HTTP, RLOGIN e.tc)
- Applications Gateways makes it slower to implement new services
- Some level of inconveniences is notable by end users
- Application Gateway does not support client software that does not support redirection

Hybrid Gateways

These are commonly known as complex Gateways that connects two firewall types. Series connections enhance security while parallel connections leave the security perimeter only as strong as the weakest component. It is always advisable to connect in series.

Circuit Level Gateways

Circuit level gateways create a virtual circuit between local and remote networks. The originator opens a port to the gateway and the gateway opens a connection to the same port on the remote machine.

Circuit-level Gateways relay packets without inspecting them. They provide minimal audit capabilities and no application specific controls.

Advantages

- Transparent to users
- Excellent fio relaying outbound traffic

Disadvantages

- Inbound traffic is risky
- Must provide new clients program

CHAPTER FIVE

5.0 CONCLUSION AND RECOMMENDATION

5.1 Conclusion

Networking security with respect to routing is very essential to the development of networking technology.

This project has brought about the need for networking environments to make a proficient maximization of the latest networking tools in order to secure their activities from intruders, hackers and all unauthorized personnel.

Implementation of this project will certainly raise the level of assurance that the sanctity of people and programs are preserved and legitimate: communications cannot be readily hijacked by electronic eavesdroppers.

5.2 Recommendation

The network core is the trusted domain of a single organization. It includes network devices that typically only have internal (trusted) interfaces that are wholly within and controlled by a single group or administrative domain. For enterprises and SPs alike, with rare exceptions, external IP traffic should never be destined to core network infrastructure. Generally, the only packets destined to these devices should be internal control plane and management plane traffic generated by other network elements or management stations also within the same administrative domain. A well-designed network edge security policy may greatly limit the exposure of the network core to attacks. Even so, human error, misconfigurations, change management, and exception cases dictate that core security mechanisms must be defined and deployed in support of defence in depth and breadth principles. Such core policies help to mitigate the risk if edge policies are inadvertently bypassed.

The primary role of security in the core is to protect the core, not to apply policy to mitigate transit attacks within the data plane. Such attacks should be filtered at the network edge to mitigate the risk of transit attack traffic from adversely affecting transit authorized traffic. Further, anti-spoofing protection mechanisms need to be deployed at the edge; otherwise, it is not possible to accurately verify IP source addresses, which increases the risk of IP spoofing attacks. Nevertheless, control and management plane security policies are applied in support of the defence in depth and breadth strategy to protect the core in the event that edge policies are bypassed.

Networking being an important aspect of information technology, enables multiple system units to share and exchange resources. It is therefore my recommendation that the following points should be considered;

- One access list per protocol per direction should be used on the network.
- Well structured firewalls should be used to protect the internal network from intruders.
- Routers with well created ACL should be used in networking environments to enable a proper management of traffic and denial of unwanted access to the network which could jeopardise the operation of internal users of the network.
- For optimal usage, effectiveness and reliability, it is my recommendation that governments and academic institutions should implement this networking technology, since it involves the sharing of files, resources and updating of records via the networks.
- Organisations implementing the networking technology should ensure that their staffs have the proper training required to make use of the networking facilities.

- Networking environments should constantly have power supply as routers and other networking tools require steady power supply to function properly.

REFERENCES

Andersson; L. & Madsen; T. (2005) Provider Provisioned Virtual Private Network(VPN) Terminology, RFC 4026

Andrew, M. (Jan. 2002) "VPNs and VPN Technologies"

Andrew S. T., (2003), "Computer Networks", Pearson Education International, New Jersey.

Anna Lysyanskaya, PhD thesis, MIT, (2002) "Signature Schemes and Applications to Cryptographic Protocol Design".

Balabi, .H, (2000) "Internet Routing Architectures". Cisco Press. Indianapolis.

Bush, .R, & Meyer, .D, (Dec 2002) "Some Internet Architectural Guidelines and Philosophy",RFC 3439.

Communications of the ACM (Feb.1978) "A Method For Obtaining Digital Signatures and Public-Key Cryptosystems," 21(2): 120-126.

Computer Association of Nigeria, (2002) "Network Technologies and Security Issues" (NETSI).

Dennis .C, (2005) "Editor, E-Commerce and the Law of Digital Signatures", Oceana Publications.

Francois, A. & Cullen, J. (Jan 2007). "Network Address Translation (NAT) Behavioural Requirements for Unicast UDP", RFC 4787.

Gleeson; B *et al.* (2000) IP Based Virtual Private Networks, RFC 2764

Hamzeh, .K, et al., (July 1999) Point-to-Point Tunneling Protocol (PPTP), RFC 2637

P. Hermann; (2008) Roaming zwischen Wireless Local Area Networks. VDM Verlag, Saarbrücken, ISBN 978-3-8364-8708-5.

Hutchison D. "Local Networking Architecture" Addison Wesley publishers Ltd. London

Ido, D & Wes, N. (Nov.2006) "Broadband Routers and Firewalls"

IEEE Transactions on Information Theory, (Nov. 1976) "New Directions in Cryptography"IT-22(6):644-654.

Joanne, W. "Step up to networking" Microsoft Press:

Johns Hopkins Bloomberg School of Public Health (2007) "History of Wireless" http://www.jhsph.edu/wireless/history.html.

John, R. (May 2004) "CCSP Self-Study: Advanced AAA Security for Cisco Router Networks".

John, W. "TCP/IP Networks", O'Reilly and Associates, Inc

Katz, J. and Lindell, Y.,(2007) "Introduction to Modern Cryptography", Chapman & Hall/CRC Press

Kent, Stephen, et al. (Feb. 2000) "Secure Border Gateway Protocol (S-BGP) -- Real World Performance and Deployment Issues". In Proceedings of the Network and Distributed System Security Symposium (NDSS 2000), San Diego, CA.

Lamport, L., (Oct. 1979) "Constructing digital signatures from a one-way function",

Larry, L., Bruce, S. D, (2003) "Computer Networks: A Systems Approach", Morgan Kaufmann, ISBN 155860832X

Lorna .B, (2004) "Electronic Signatures Law and Regulation", Sweet & Maxwell.

Michael; O. R. (Jan. 1979) "Digitalized signatures as intractable as factorization.", Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science,

Muthukrishnan, K. & Malis, A., (2000) A Core MPLS IP VPN Architecture, RFC 2918

Nagarajan; A. (2004) Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN), RFC 3809

Nic, M., (2009) "CSIRO settles on wireless patent". ABC Science Online. http://www.abc.net.au/science/articles/2009/04/23/2550483.html

Peter, H. (2000) "Local Area Network", 3rd Edition, Continuum 2000

Y. Rekhter *et al.*, (1999) Address Allocation for Private Internets, RFC 1919

Rekhter, Y. & Li, Tony. (March 1995). "A Border Gateway Protocol (BGP-4)" RFC 1771,

Rosen; E. & Rekhter; Y (1999) Internet Engineering Task Force (IETF), RFC 2547 BGP/MPLS VPNs

Shafi .G, Silvio .M, & Ronald .R. (Apr. 1988). A digital signature scheme secure against adaptive chosen-message attacks.", SIAM Journal on Computing, 17(2):281-308,

Sean, C. (Jun 2004) "General Design Considerations for Secure Networks"

Schellenkens, M. H. M., (2004) "Electronic Signatures Authentication Technology from a Legal Perspective", TMC Asser Press.

Selinam M., (2006) "CSIRO hits back on Wireless". The Australian. http://australianit.news.com.au/articles/0,7204,20475012^15306,00.html

Siyan; K. (1997) Inside TCP/IP, New Riders Publishing, 1997. ISBN 1-56205-714-6

Stephen .M, (2007) "Electronic Signatures in Law" Tottel, second edition.

Technical Report CSL-98, SRI International,

Thomas; K., (2006). Beginning Ubuntu Linux: From Novice to Professional. Apress.

Townsley, W. *et al.*, (1999) Layer Two Tunneling Protocol "L2TP", RFC 2661

Tyson, Jeff. "How Encryption Works." 06 April 2001

Valencia, A. *et al.*, (1998) IP Based Virtual Private Networks, RFC 2341

Vinton; G. C, Robert E. K. (May 1974) "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Vol. 22, No. 5,

Wendell, O. (2001) "Cisco Certified Network Administrator (CCNA)",

Worcester Polytechnic Institute, (2008) "The First IEEE Workshop on Wireless LANs http://www.cwins.wpi.edu/wlans91/scripts/preface.html

Worcester Polytechnic Institute, (2008) "The Second IEEE Workshop on Wireless LANs http://www.cwins.wpi.edu/wlans96/scripts/summary.html

Yusuf, B. (Jul 2004) "Cisco Asks, Can Security Skills Be Certified?"