Unit III

CHAPTER 3

Secure Network Design

Syllabus Topic : Secure Network Design

3.1 Secure Network Design

Q. 3.1.1 Explain secure network design with its various aspects. (Ref. Secs. 3.1, 3.1.1, 3.1.2) **(5 Marks)**

- Organizations are leveraging the power of the Internet to connect with all types of external entities such as customers, peer organizations and suppliers, etc. This access is intended to enable a simple and smooth mechanism for dissemination of information, to conduct a variety of business functions and to provide remote access to systems and data.
- It is difficult to find an organization, irrespective of their size, that does not leverage the Internet in some respect as a part of its operation.
- Enterprises must make their information, property and platforms available to themselves remotely and to third parties, often including sensitive IP material and data. The underlying design of the network plays an integral role in an organization's ability to effectively manage and secure access to its data.
- The boundary between an organization's network and the Internet or a peered network is known as an Electronic Security Perimeter (ESP). Within this perimeter all owned computing assets and potential storage locations for organization data can be found, sometimes including third-party systems.
- The underlying design of the network will play an integral role both in defining the electronic boundaries and in enabling an organization to effectively protect, manage and secure access to information assets within that perimeter.
- Sometimes, an organization's intellectual property can reside outside of this perimeter which requires additional consideration when planning for the protection of enterprise data.

- One of the most significant problem areas for security groups is defining the appropriate boundary for the ESP and being aware of what actions can inadvertently change that boundary.
- From a pure design perspective, the time must be spend to consider the hardship it will cause later if the design cannot accommodate growth or, worse, misses critical gaps and introduces un-comprehended and unforeseen risks.

Syllabus Topic : Introduction to Secure Network Design

3.1.1 Introduction to Secure Network Design

Q. 3.1.2 Explain secure network design with its various aspects. (Ref. Secs. 3.1, 3.1.1, 3.1.2) **(5 Marks)**

- Network analysis, architecture, and design are processes used to produce designs that are logical, reproducible, and defensible. These processes are interconnected, in that the output of one process is used directly as input to the next, thus creating flows of information from analysis to architecture, and from architecture to design.
- Network analysis entails learning what users, their applications, and devices need from the network. It is also about understanding network behaviour under various situations. Network analysis also defines, determines, and describes relationships among users, applications, devices, and networks. In the process, network analysis provides the foundation for all the architecture and design decisions to follow.
- The purpose of network analysis is two fold: first, to listen to users and understand their needs; and second, to understand the system. In analyzing a network we examine the state of the existing network, including whatever problems it may be having.
- We develop sets of problem statements and objectives that describe what our target network will be addressing. And we develop requirements and traffic flows, as well as mappings of users, applications, and devices, in support of our problem statements and objectives. As such, network analysis helps us understand what problems we are trying to solve, and in the process we compile information that will be used in developing the architecture and design.
- Network architecture uses the information from the analysis process to develop a conceptual, high-level, end-to-end structure for the network. In developing the network architecture we make technology and topology choices for the network.

- We also determine the relationships among the functions of the network (addressing/routing, network management, performance, and security), and how to optimize the architecture across these relationships. There usually is not a single "right" architecture or design for a network; instead there are several that will work, some better than others.
- The architecture and design processes focus on finding those best candidates for architecture and design (optimized across several parameters) for your conditions.
- The network architecture process determines sets of technology and topology choices; the classes of equipment needed; and the relationships among network functions. Network design provides physical detail to the architecture. It is the target of our work, the culmination of analysis and architecture processes.
- Physical detail includes blueprints and drawings of the network; selections of vendors and service providers; and selections of equipment (including equipment types and configurations).
- During network design we use an evaluation process to make vendor, service provider, and equipment selections, based on input from the network analysis and architecture.
- You will learn how to set design goals, such as minimizing network costs or maximizing performance, as well as how to achieve these goals, through mapping network performance and function to your design goals and evaluating your design against its goals to recognize when the design varies significantly from these goals.
- Network design is also about applying the trade-offs, dependencies, and constraints developed as part of the network architecture.
- Trade-offs, such as cost versus performance or simplicity versus function, occur throughout the design process, and a large part of network design concerns recognizing such trade-offs (as well as interactions, dependencies, and constraints) and optimizing the design among them. As part of the design process you will also learn how to develop evaluation criteria for your designs.

3.1.1.1 Acceptable Risk

- It is management's responsibility to set their company's level of risk. As a security professional, it is your responsibility to work with management and help them understand what it means to define an acceptable level of risk.
- Each company has its own acceptable risk level, which is derived from its legal and regulatory compliance responsibilities, its threat profile, and its business drivers and

impacts. This article explains how to go about defining an acceptable level of risk based on a threat profile and business drivers.

- Some organizations unintentionally take on more risk than they intend to by being unaware of the legislative instruments that they are subject to within a legal jurisdiction.
- During the development of the policies that will guide the design of the systems and networks, management should spend the time and effort necessary to determine if any of these special legal considerations apply.
- Many enterprises inadvertently violate certain laws without even knowing that they are doing so (for example, storing credit card storing patient data without factoring in Health Insurance Portability and Accountability Act [HIPAA] provisions).
- This modifies the level of residual risk actually produced after the controls are applied, since the planned controls may not address risks that are not clearly defined prior to control plan development.
- A significant but often missed or under-considered factor in determining an appropriate security design strategy is to identify how the network will be used and what is expected from the business it supports.
- Some key network design strategies include deciding network design models, designing an appropriate network model and cost of security.

Network design models

- This model is built by connecting various components. In order to secure network we need to use access control mechanism such as firewall. Firewalls and authentication system is used to control traffic of the network.
- In networking, firewalls and authentication systems are used for controlling traffic movement around the network. They are also used to segregate traffic of differing sensitivity levels and using monitoring systems to detect unauthorized activities in the network.

Designing an appropriate network

- The first phase in the life of a network - designing the network - involves making decisions about the type of network that best suits the needs of your organization. Some of the planning decisions you make will involve network hardware; for example:
  - Number of host machines your network can support.
  - Type of network media to use : Ethernet, token ring, FDDI, and so on.

- Network topology; that is, the physical layout and connections of the network hardware.
- Types of hosts the network will support: standalone and dataless.
- Based on these factors, you can determine the size of your local-area network.

– The overall network design must also provide the ability to grow and support future network requirements. By getting involved early in the development cycle, engineers can suggest more secure designs and topologies and additionally can assure the project team that they have a clear understanding of the security considerations and capabilities.

– In addition, they can ensure that new projects are more compatible with the existing corporate infrastructure.

The cost of security

In order to deploy Security control mechanisms we have expenses of purchasing hardware, installation and deployment. While deciding on exact details of redundancy and security controls for a given system or network, it is very important to take a count of negative scenarios in which a security breach, to get the idea of the corporation's costs for each occurrence. This risk-model approach helps management to determine the value of the various security control mechanisms.

Syllabus Topic : Performance

3.1.2 Performance

Q. 3.1.3 Explain secure network design with its various aspects. (Ref. Secs. 3.1, 3.1.1, 3.1.2) **(5 Marks)**

– The network will play a huge role in meeting the performance requirements of an organization. Networks are getting faster and faster, evolving from 10 megabit to 100 megabit to gigabit speeds, with 10GE (Gigabit Ethernet) commonly deployed and 40 GE, 100 GE and InfiniBand technologies available today.

– When determining the appropriate network technology, it must be ensured that it can meet the bandwidth requirements projected for three to five years in the future, if not then expensive replacements or upgrades may be required.

– Applications and networks which has very low tolerance for latency, those supporting video and voice streaming, which needs higher performance network connections and

hardware. This creates a problematic situation with applications that move data in large chunks.

– The legacy Cisco Hierarchical Internetworking model is a common design implemented in large-scale networks today, although many new types of purposed designs have been developed that support emerging technologies like class fabrics, lossless Ethernet, layer two bridging with trill or IEEE 802.1aqand other data center centric technologies.

– The three-tier hierarchy still applies to campus networks, but no longer to data centers. The Cisco three-tier model is derived from the Public Switched Telephone Network (PSTN) model, which is in use for much of the world's telephone infrastructure.

– The Cisco Hierarchical Internetworking model, depicted in Fig. 3.1.1, uses three main layers commonly referred to as the core, distribution and access layers:

– In the Three Tier Architecture, the Core Layer is the one ***coordinating everything***. It has only one, simple purpose : connecting all the distribution layers together.

– In large enterprises, where you have several distribution switches, the core layer is also known as **Backbone**.

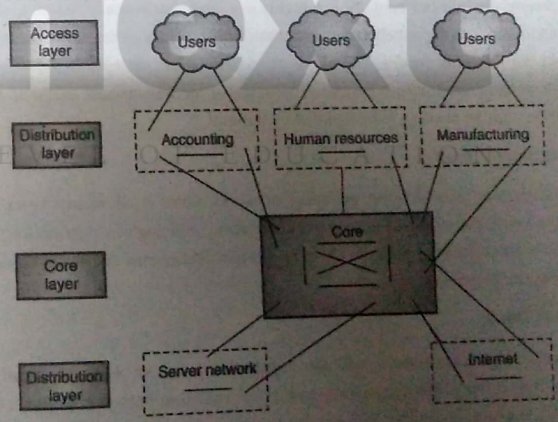


Fig. 3.1.1 : The Cisco hierarchical internetworking model

– Distribution layer is present between the core and the access layer. This layer is used to aggregate access-layer traffic for transmission into and out of the core.

- The Access Layer is the one ***closer to the users***. In fact, at this layer we find the users themselves and the access-layer switches. The main purpose of this layer is to physically connect users to the network. In other words, there is just a cable between end-user PCs and access-layer switches.
- At this layer we apply **network-access policies**. These are the security policies we want to ***enforce*** in order to allow access to the network.
- The network is highly segmented, a single network failure at the access or distribution layers does not affect the entire network. Many modern data center architectures and "cloud" designs do not employ a three-tier model, instead favoring a clustered switching, class fabric, or collapsed two-tier approach that offers higher performance and lower cost but also brings special security considerations.

The following are two-tier network fundamentals (three-tier terminology is used for comparative purposes) :

Core (Tier 1)

The core of the two-tier network is a highly available, horizontally scalable element used for transit and moving data between different areas or zones in the network, much like the core in the three-tier model. The major difference is that the core in a two-tier network doesn't analyze the traffic completely, as much of the host-to-host traffic transits across the fabric without needing to be handled by the core.

Distribution (Tier 2)

The distribution layer in some collapsed networks either is eliminated completely or is combined with the access layer as part of the fabric. Although a "distribution" layer may literally exist, it does not logically exist, as it is part of the same switch fabric or switching cluster as the access switching.

Access (Tier 3)

- The access layer is collapsed into the distribution layer, so while physically separate devices may provide the aggregation and access function, both can be part of the same layer-two domain employing 802.1aq for bridging. These combined layers offer active connectivity across multiple switches via clustering for high availability and performance. This "fabric" introduces a new dimension for security, as server-to-server, server-to-storage and virtual host communication which can be fused together.
- Since the data center network is becoming flatter, faster and much larger, designing the security components to support the goals of the network is more important than ever.

Since virtualization is commonplace and shared server/storage platforms almost always exist underneath, ensure that adequate time is spent designing the networks and topologies to allow security components to "plug in" to the fabric which maintains the integrity of data communications between intended hosts but does not compromise the performance of the data center platform.

- Techniques like VM fencing, virtual appliance firewalls, hypervisor protection and segregation of security zones by service type are common approaches to ensuring adequate controls are in place to enforce the security plan.

Syllabus Topic : Availability

3.1.3 Availability

Q. 3.1.4 Explain network availability. (Ref. Sec. 3.1.3) (5 Marks)

- Network availability means resources should be available to users whenever it's needed. The opposite of availability is denial of services where users cannot use any resource whenever it's needed.
- Business availability has forced some organizations to construct duplicate data centers that perform real-time mirroring of systems and data to provide failover and reduce the risk of a natural disaster or terrorist attack destroying their only data center.
- Depending on the specific business and risk factors, redundancy often increases both cost and complexity. Determining the right level of availability and redundancy is an important design element, which is best influenced by a balance between business requirements and resource availability.
- Fig. 3.1.2 shows a full high-availability network segment without a single hardware point of failure (which in this example uses Cisco's Hot Standby Router Protocol [HSRP], which is a built-in protocol for switching routes if a router or interface goes down).
- A true high-availability design will incorporate redundant hardware components at the switch, network, firewall and application levels. When eliminating failure points, it must be ensured to consider all possible components.
- Today's high-availability designs have reached a high level of sophistication in modern data centers and network and computing architectures, from the facility itself down to the application running in front of the end user.

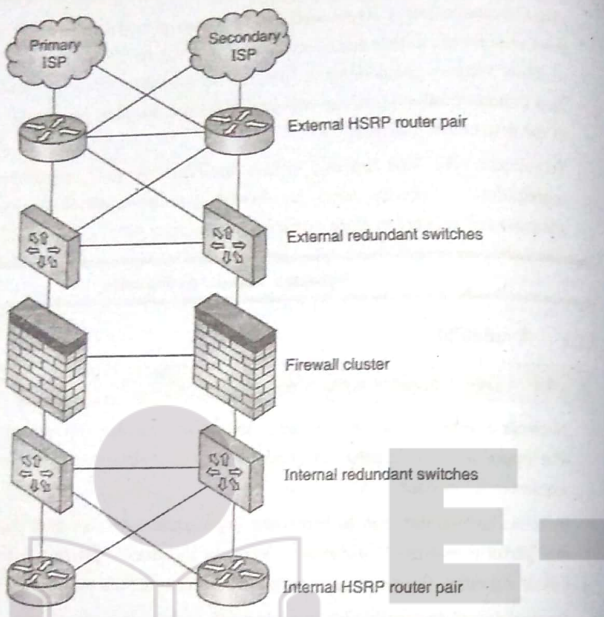


Fig. 3.1.2 : A full High-availability network design

- Load balancers also play an important role in maintaining the availability and performance of network-based services. Today's application delivery technologies are being used for both security and availability.
- In some cases, organizations have gotten rid of their web tier completely and host it directly on Application Delivery Controllers (ADCs), which provide optimized application and network performance.

Syllabus Topic : Security

3.1.4 Security

Q. 3.1.5 Explain network security. (Ref. Sec. 3.1.4) (5 Marks)

- Elements that are present on a network performs different functions and contains data of differing security requirements.
- Some devices contain highly sensitive information that could damage an organization if disseminated to unauthorized individuals, such as payroll records, internal memorandums, customer lists and even internal job-costing documents.
- Other devices have more exposure due to their location on the network.
- For example, internal file servers will be protected differently than publicly available web servers. When designing and implementing security in network and system architectures, it is helpful to identify critical security controls and understand the consequences of a failure in those controls.
- For example, firewalls protect hosts by limiting what services users can connect to on a given system.
- Firewall is a hardware or software device used to keep undesirables electronically out of a network the same way that locked doors and secured server racks keep undesirables physically away from a network.
- A firewall filters traffic crossing it (both inbound and outbound) based on rules established by the firewall administrator. In this way, it acts as a sort of digital traffic cop, allowing some (or all) of the systems on the internal network to communicate with some of the systems on the Internet, but only if the communications comply with the defined rule set.
- Flaws, such as a buffer overflows, can allow an attacker to turn a vulnerable server into a conduit through the firewall.
- Once through the firewall, the attacker can mount attacks against infrastructure behind the protection of the firewall. In addition to the best practice of segmenting the traffic, using the advanced inspection capabilities and application-layer gateways of current-generation firewalls can help protect segmented networks by ensuring that traffic being sent as a particular service over a particular port is in fact well-formed traffic for that service.
- In addition to securing individual elements on the network, it is important to secure the network as a whole. The network perimeter consists of all the external-most points of the internal network and is a definable inner boundary within the electronic security perimeter. Perimeter security is only as strong as its weakest link.

3.1.4.1 Wireless Impact on the Perimeter

- Network perimeter security is only useful if it is able to prevent an authorised user from accessing it and getting connected to internal networks. In order to connect they just need laptop and wireless card so with the help of IP address on the network.

- Signals which are coming through wireless access points degrades quickly while passing through walls and over distance, more powerful and specialized directional antennas which picks up signals at significant distances.
- These antennas, called Yagi antennas, can pick up wireless signals at distances approaching one mile.
- While commercial Yagi antennas can be costly, inexpensive ones can be built at home out of an empty potato chip can and some wire. And Yagi antennas are not the only type that can be used for long-range Wi-Fi; there are also backfire and other types of relatively small but powerful antennas that can be used in this fashion.
- Network design must also factor in the impact of the explosion of mobile devices into the wireless network, the ways in which the wireless design needs to support and accommodate many more varieties of devices and how that in turn is forcing the advancement of technologies like mobile device fingerprinting and identity management.
- The sheer volume of mobile devices has created significant security challenges and unanticipated risks for the wireless network, creating a new dynamic that has expanded the network beyond traditional boundaries.

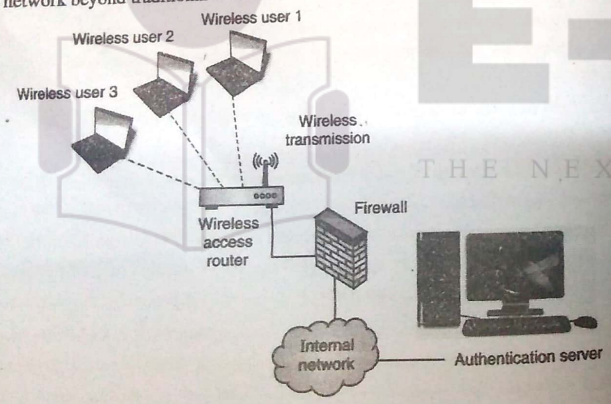


Fig. 3.1.3 : Wireless deployment through a VPN server

3.1.4.2 Remote Access Considerations

- While some corporations still maintain dial-up access as a backup or secondary solution, remote access is now generally provided via a VPN solution. This type of VPN, which connects remotely located people to the organization's network, is a remote access VPN

(as distinguished from a site-to-site or LAN-to-LAN VPN, which connects two networks together).

- Remote-access VPNs allow secure access to corporate resources by establishing an encrypted tunnel across the Internet. The ubiquity of the Internet, combined with today's VPN technologies, allows organizations to cost-effectively and securely extend the reach of their networks to anyone, anyplace, anytime.
- VPNs have become the logical solution for remote-access connectivity for the following reasons :
  - Provides secure communications with access rights tailored to individual users, such as employees, contractors, or partners.
  - Enhances productivity by extending corporate network and applications.
  - Reduces communications costs and increases flexibility.
- Most major firewall and VPN vendors include firewalling functionality in their clients. While a hijacked VPN tunnel may seem like a remote possibility, it has happened. In October of 2000, sensitive Microsoft internal systems were accessed.
- Anytime, anyplace network access gives employees great flexibility regarding when and where they perform their job functions. VPNs accommodate "day extenders", employees who desire network access from home after hours and weekends to perform business functions such as answering e-mail or using networked applications.
- Using VPN technology, employees can essentially take their office wherever they go, thus improving response times and enabling work without interruptions present in an office environment.
- VPNs also provide a secure solution for providing limited network access to non-employees, such as contractors or business partners. With VPNs, contractor and partner network access can be limited to the specific servers, Web pages, or files they are allowed access to, thus extending them the network access they need to contribute to business productivity without compromising network security.
- Posture validation, which is a feature of many remote access VPN products, is a technique for checking the security software and configuration of remote systems before they are allowed to connect to the network.
- It's a good way to reduce the risk of unsecure, infected, or compromised systems spreading risks onto the organization's network.

3.1.4.3 Internal Security Practices

Q. 3.1.6 Explain internal security practice in detail. Hence explain extranet, intranet, DMZ. (Ref. Secs. 3.1.4.3, 3.1.4.4) **(5 Marks)**

- Organizations that deploy firewalls strictly around the perimeter of their network leave themselves vulnerable to internally initiated attacks, which are statistically the most common threats today.
- Internal controls, such as firewalls and early detection systems (IDS, IPS and SIEM), should be located at strategic points within the internal network to provide additional security for particularly sensitive resources such as research networks, repositories containing intellectual property and human resource and payroll databases.

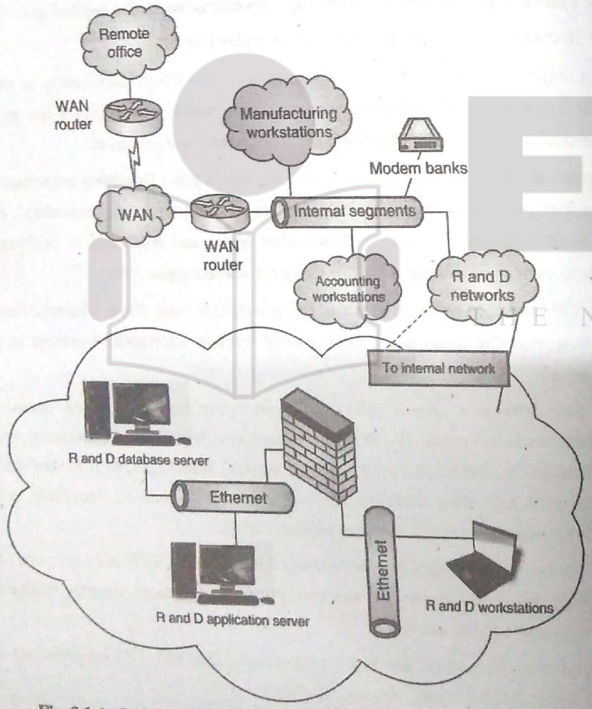


Fig. 3.1.4 : Internal firewalls can be used to increase internal security

- Dedicated internal firewalls, as well as the ability to place access control lists on internal network devices, can slow the spread of a virus.
- When designing internal network zones, if there is no reason for two particular networks to communicate, explicitly configure the network to block traffic between those networks and log any attempts that hosts make to communicate between them.
- With modern VoIP networks, this can be a challenge as VoIP streams are typically endpoint to endpoint, but consider only allowing the traffic you know to be legitimate between any two networks.
- A common technique used by hackers is to target an area of the network that is less secure and then work their way in slowly via "jumping" from one part of the network to another. If all of the internal networks are wide open, there is little hope of detecting, much less preventing and this type of threat vector.

3.1.4.4 Intranets, Extranets and DMZs

Q. 3.1.7 Explain internal security practice in detail. Hence explain extranet, intranet, DMZ. (Ref. Secs. 3.1.4.3, 3.1.4.4) **(5 Marks)**

Extranet

An extranet is defined as the network that restricts access to company files and folders from unknown people and permits only partners, vendors and suppliers who are authorized to do so.

Intranet

Intranet is a network that is not available to outside world, only those who are granted can access this network for data sharing and viewing purposes. various types of firewalls helps to control access between the Intranet and Internet to permit access to the Intranet only to people who are members of the same company or organization.

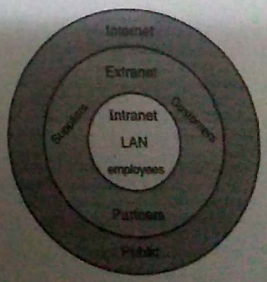


Fig. 3.1.5 : Intranet and Extranet

DMZ networks and screened subnets

- An organization may want to provide public Internet access to certain systems. For example, for an organization to receive Internet e-mail, the e-mail server must be made available to the Internet.
- These systems are deployed on a dedicated subnet, commonly referred to as a DeMilitarized Zone (DMZ) or screened subnet, separate from internal systems. These systems are publicly accessible and hence they can possibly come under attack from malicious users.
- To keep these systems protected, they are kept on a segregated network, a successful attack against these systems still leaves a firewall between the successful attacker and more sensitive internal resources.

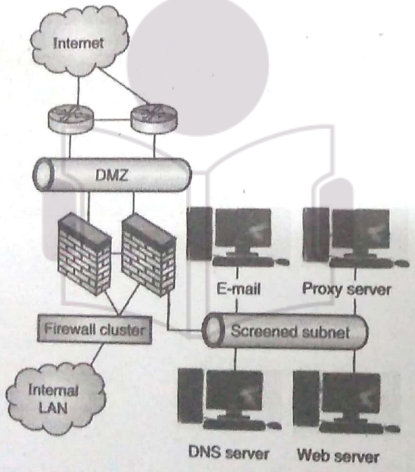


Fig. 3.1.6 : A Demilitarized Zone (DMZ) configuration

The ***presentation*** layer consists of a web server that interacts with end users, accepting input, sending that input to the application layer for processing and returning the output back to the end user.

The ***application*** layer contains the logic necessary for processing those queries and extracting the data that is stored in a database housed on a separate database server.

- Other services that aren't directly supporting the application but provide other functions can be further segregated into a fourth DMZ subnet.

3.1.4.5 Outbound Filtering

Outbound filtering of network traffic is as important as securing the inbound access to the network.

Syllabus Topic : Network Device Security

3.2 Network Device Security

Q. 3.2.1 Explain network device security with respect to router and switches. (Ref. Sec. 3.2) **(5 Marks)**

- Properly configured routers and switches increases the security of the network. These devices can be configured to limit network traffic or to protect themselves against attacks.
- Traditionally, routers and switches have been managed by using a Command-Line Interface (CLI), but interfaces have evolved over time toward graphical configuration solutions. CLIs are still available, but ***web User Interfaces*** *(web UIs)* have become ubiquitous and are the most commonly used configuration tools these days.
- Additional functionality has converged into "all-in-one" devices such as ***Unified Threat Management*** *(UTM)* platforms (firewalls combined with network antivirus, web filtering, application network communication control, IPS, and other network-oriented security functions, often bundled into switches both large and consumer sized).
- Having a web server and additional software running on the devices that control everything else in the environment increases complexity in terms of security. Paying special attention to securing the device interface and feature set will help ensure that network devices are having appropriate protection.

Syllabus Topic : Switch and Router Basics

3.2.1 Switch and Router Basics

- Internetworking protocol that is in use today is known as ***Transmission Control Protocol/Internet Protocol version 4 (TCP/IP or IPv4)***, although *IPv6* is on the horizon and is deployed in some carrier networks today.

- TCP/IP provides all the necessary components and mechanisms to transmit data between two computers over a network.
- TCP/IP is actually a suite of protocols and applications that have discrete functions that map to the ***Open Systems Interconnection (OSI) model***, sometimes referred to as the *OSI stack*. To achieve network device security, understanding TCP/IP functions at the second and third layers of the OSI model, commonly known as the data-link layer and network layer, respectively is important.

MAC Addresses, IP Addresses, and ARP

- Each device on a network actually has two network-related addresses: a layer two (Data-Link layer) address known as the ***Media Access Control (MAC) address*** (also known as the ***hardware address*** or ***physical address***), and a layer three (Network layer) address known as the ***IP address***.
- MAC addresses are 48-bit hexadecimal numbers that are uniquely assigned to each hardware network interface by the manufacturer, or virtually created by a hypervisor in a virtualized environment from a set range of addresses (different hypervisors have different methods for generating these).
- Some networking protocols also generate and use virtual MAC addresses for high availability features, such as ***Hot Standby Router Protocol (HSRP)*** or ***High-Availability (HA)***clusters that maintain one active virtual device no matter which piece of hardware has assumed the active role.
- Each hardware manufacturer has been assigned a range of MAC addresses to use, and each MAC address that has ever been assigned to a physical ***Network Interface Card (NIC)*** is globally unique because it allows the underlying communication protocols to select the right system for network communications (although virtual MAC addresses may be used in more than one place, because the algorithms used to generate them are similar and can start with the same reference values, as long as the same two MACs do not appear on the same network segment, they will work).
- IPv4 addresses are 32-bit numbers assigned by network administrator that allow for the creation of logical and ordered addressing on a local network. IPv6 addresses are 128-bit, but, like IPv4, each IP address must be unique on a given network.
- To send traffic, a device must have the destination device's IP address as well as a MAC address. Knowing the destination device's host name, the sending device can obtain the destination device's IP address using protocols such as ***Domain Name Service (DNS)***.

- To resolve a MAC address, the host uses the ***Address Resolution Protocol (ARP)***, which functions by sending a broadcast message to the network that basically says, "Who has 192.168.10.10, tell 192.168.10.100." If a host receives that broadcast and knows the answer, it responds with the MAC address : "ARP 192.168.10.10 is at ab:cd:ef:19:A0:C2."
- First three octets of MAC address are ***Organizationally Unique Identifier (OUI)*** for the manufacture of this router. Here are the OUI for some well-known manufacturers : Dell : 00-14-22, Nortel : 00-04-DC, Cisco : 00-40-96, Belk in: 00-30-BD.
- No authentication or verification is done for any ARP replies that are received. This facilitates an attack known as ***ARP poisoning***.
- ARP poisoning is one of the most effective and hard-to-defend attack techniques still in widespread use today. An attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets.
- This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination.
- As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user. For traffic destined to nonlocal segments, the MAC address of the local router is used.
- MAC addresses are really only relevant for devices that are locally connected, not those that require packets to travel through layer three devices, such as routers.

3.2.1.2 TCP/IP

Q. 3.2.2 Explain security aspects in TCP/IP protocol suite and OSI model (Ref. Sec. 3.2.1.2) **(5 Marks)**

TCP/IP model layers

- Each layer of the TCP/IP has a particular function to perform and each layer is completely separate from the layer(s) next to it.
- The communication process that takes place, at its simplest between two computers, is that the data moves from layer 4 to 3 to 2 then to 1 and the information sent arrives at the second system and moves from 1 to 2 to 3 and then finally to layer 4.

Application layer

- The application layer is concerned with providing network services to applications. There are many application network processes and protocols that work at this layer, including Hyper Text Transfer Protocol (HTTP), Simple Mail Transport Protocol (SMTP) and File Transfer Protocol (FTP).
- At this layer sockets and port numbers are used to differentiate the path and sessions which applications operate. Most application layer protocols, especially on the server side, have specially allocated port numbers, e.g. HTTP = 80 and SMTP = 25, and FTP = 20 (Control), 21 (Data).

Transport layer

- This layer is concerned with the transmission of the data. The two main protocols that operate at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is regarded as being the reliable transmission protocol and it guarantees that the proper data transfer will take place.
- UDP is not as complex as TCP and as such is not designed to be reliable or guarantee data delivery. UDP is generally thought of as being a best effort data delivery, i.e. once the data is sent, UDP will not carry out any checks to see that it has safely arrived.

The Internet layer

This is the layer that contains the packet construct that will be transmitted. This takes the form of the Internet Protocol (IP) which describes a packet that contains a source IP Address, destination IP Address and the actual data to be delivered.

Network access layer

This is the lowest level of the TCP/IP protocol stack and functions carried out here include encapsulation of IP packets into frames for transmission, mapping IP addresses to physical hardware addresses (MAC Addresses) and the use of protocols for the physical transmission of data.

Note : TCP/IP is actually a suite of protocols sometimes referred to as the Internet Protocol Suite.

(a) Brief overview of the OSI layer

- The OSI model uses a seven-layer structure to represent the transmission of data from an application residing on one computer to an application residing on another computer.

- TCP/IP does not strictly follow the seven-layer OSI model, having integrated the upper OSI layers into a single application layer.
- Fig. 3.2.1 shows a graphical representation of the OSI reference model and its relationship to the TCP/IP implementation.
- Table 3.2.1 highlights the functions performed by each layer of the OSI reference model.

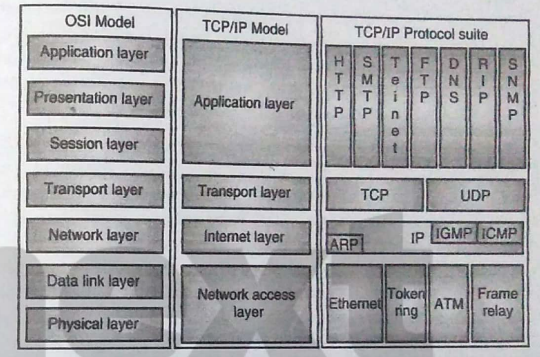


Fig. 3.2.1 : The OSI reference model and the TCP/IP model

Table 3.2.1 : Functionalities of the OSI seven layer model

Layers	OSI Model	Functions
Layer seven	Application layer	Provides the protocol (Commonly accepted and published language Syntax and functions) for applications to access networked services. The most well-known application-layer protocols in use today are HTTP (which presents data to a web browser or other application that "tunnels" through the protocol), along with SMTP, POPS and IMAP (for sending and receiving e-mail on mobile devices).
Layer six	Presentation layer	Used to convert application data into acceptable and compatible formats for transmission. At this layer, data is encoded and encrypted. For example, audio, video or image files transferred

Layers	OSI Model	Functions
		between systems might use MP3, MPEG4 or GIF encoding. Data compression (for example, with a Lempel-Ziv algorithm commonly used in Zip type file archiving) is also done at this layer. Network encryption is done at this layer as well.
Layer five	Session layer	Provides mechanisms for two hosts to maintain a network connection, or session, across network. As long as a session is established, two hosts can continue to send data back and forth. This concept is important in the next chapter on firewalls, in the context maintaining a session once it has been properly validated and accepted by the firewall policy configuration. NetBIOS is often classified as a session-layer protocol and is SQL.
Layer four	Transport layer	Connects the upper OSI layers (five through seven) to the lower layers (one through three). The transport layer differentiates each application by assigning it a port number. These port numbers are familiar to most people in the context of "port 80" (for HTTP) or "port 53" (for DNS). Firewalls make access control decisions based on these port numbers TCP and UDP are the two most common transport-layer protocols. The main difference between the two is that TCP provides additional services, such as ordered and reliable delivery, that UDP is described as being connectionless. TCP is used when an application must ensure that every packet is received, such as when transferring files. UDP is most appropriate when the resending of data is not needed or is not useful (especially over unreliable connection), such as with streaming video or voice applications.
Layer three	Network layer	Provides a unique address to every host on the network. Layer three also provides a means to connect layer one and two networks together using routers. IP is the most common layer three protocol in use worldwide. IP addresses are examples of layer three objects. IP (version 4) addresses consist of four groups of numbers between 0 and 255 like 192.168.0.1 or 10.1.55.223.
Layer two	Data-link layer	Composed of two different sublayers : Media Access Control (MAC) and Logical Link Control (LLC). The MAC is used to manage the sending of electrical signals across the physical medium with other hosts on the local segment. The LLC

Layers	OSI Model	Functions
		provides flow control, error checking and synchronization. MAC addresses are 12 hexadecimal digits (usually grouped in pairs for easy readability) like 20-10-7a-3c-94-c7 or ccaf:78:bb:73:1d.
Layer one	Physical layer	Used to define and control electrical signals over the physical media Ethernet is a commonly recognized example.

b) Ports and TCP/IP

- A number assigned to user sessions and server applications in an IP network. Port numbers, which are standardized by the Internet Assigned Numbers Authority (IANA), reside in the header area of the packet being transmitted and thus identify the purpose of the packet (Web, email, voice call, video call, etc.).
- Destination Ports Are Server Applications Destination ports may be "well-known ports" (0-1023) for the major Internet applications, such as Web and email. For example, all port 80 packets (HTTP packets) are directed to and processed by a Web server.
- User "registered ports" (1024-49151) are assigned to applications that are mostly vendor specific, such as Skype and BitTorrent. See well-known port, port forwarding and opening a port.Connecting on any other port would result in an error unless the web server had been configured to listen on that non-default port and respond to the requests. If an administrator chose to have the web server use port 81, they would have to inform all their users to specifically connect on port 81 (usually done in a browser by specifying the port at the end of the URL, for example: *www.mywebpage.com:81*).

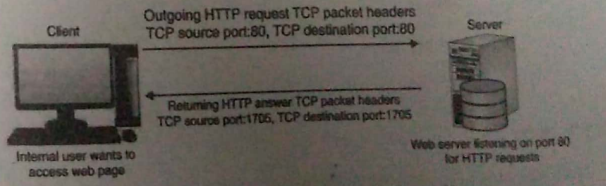


Fig. 3.2.2 : HTTP uses well-known TCP port 80

- Fig. 3.2.2 shows how port numbers are used within TCP/IP packets. Source ports are necessary for the TCP/IP stack to connect the data received from the network to the application process that is requesting it.

- The application service/port combination creates a "socket" that the client and server use to communicate. The list of TCP port numbers and the applications they are associated with is available in RFC 1700, "Assigned Numbers."
- Table 3.2.2 lists some of the well-known services and their assigned ports.

Table 3.2.2 : Well-known TCP and UDP port numbers

Service	Protocol	Port
FTP FTP-data	TCP	21 20
SSH	TCP	22
Telnet	TCP	23
SMTP	TCP	25
DNS (zone transfer)	TCP	53
DNS (queries)	UDP	53
HTTP	TCP	80
NetBIOS	TCP UDP	137-139, 445
POP3	TCP	110
IMAP	TCP	145
SNMP	UDP/TCP	161
SNMP Traps	UDP	162
HTTPS	TCP	443

3.2.1.3 Hubs

- Hubs were used to connect more than two networking devices together. Hubs operates at first layer (Physical layer) of OSI model. They transmitted packets between devices connected to them, and they functioned by retransmitting each and every packet received on one port out through all of its other ports without storing or remembering any information about the hosts connected to them.

- Unlike a network switch or router, a network hub has no routing tables or intelligence on where to send information and broadcasts all network traffic across each port. This created scalability problems for legacy half-duplex Ethernet networks, because as the number of connected devices and volume of network communications increased, collisions became more frequent, degrading performance.
- A collision occurs when two devices transmit a packet onto the network at almost the exact same moment, causing them to overlap and thus mangling them. When this happens, each device must detect the collision and then retransmit their packet in its entirety. As more devices are attached to the same hub, and more hubs are interconnected, the chance that two nodes transmit at the same time increases, and collisions became more frequent.
- As the size of the network increases, the distance and time a packet is in transit over the network also increases, making collisions even more likely. Thus, it is necessary to keep the size of such networks very small to achieve acceptable levels of performance.
- Most modern hubs offer 100-Mbps full-duplex or gigabit connectivity (there are no half-duplex connections in gigabit networks the Gigabit Ethernet standard is always full duplex) to address the collision issue, and actually do perform some type of switching, but having all information broadcast to multiple ports can be a security risk and cause bottlenecks. In the past, network hubs were popular because they were cheaper than a switch or router. Today, switches do not cost much more than a hub and are a much better solution for any network.

3.2.1.4 Switches

- Switches are the evolved descendants of the network hub. A switch is a hardware device that filters and forwards network packets. From a network operation perspective, switches are layer two (Data-link layer) devices and routers are layer three (Network layer) devices (referring to their level of operation in the OSI stack), though as technology advances, switches are being built with capabilities at all seven layers of the OSI model.
- Switches were developed to overcome the historical performance shortcomings of hubs. Switches are more intelligent devices that learn the various MAC addresses of connected devices and transmit packets only to the devices they are specifically addressed to.
- Since each packet is not rebroadcast to every connected device, the likelihood that two packets will collide is significantly reduced.

- Switches provide a security benefit by reducing the ability to monitor or sniff another workstation's traffic. With a hub, every workstation would see all traffic on that hub; with a switch, every workstation sees only its own traffic.
- A switched network cannot absolutely eliminate the ability to sniff traffic. An attacker can trick a local network segment into sending it another device's traffic with an attack known as ***ARP poisoning***. ARP poisoning works by forging replies to ARP broadcasts.
- For example, suppose malicious workstation Attacker wishes to monitor the traffic of workstation Victim, another host on the local switched network segment. To accomplish this, Attacker would broadcast an ARP packet onto the network containing Victim's IP address but Attacker's MAC address.
- Any workstation that receives this broadcast would update its ARP tables and thereafter would send all of Victim's traffic to Attacker. This ARP packet is commonly called a *gratuitous ARP* and is used to announce a new workstation attaching to the network.
- To avoid alerting Victim that something is wrong, Attacker would immediately forward any packets received for Victim to Victim. Otherwise Victim would soon wonder why network communications weren't working. The most severe form of this attack is where the Victim is the local router interface.
- In this situation, Attacker would receive and monitor all traffic entering and leaving the local segment. While ARP poisoning attacks appear complicated, there are several tools available that automate the attack process, such as Ettercap.
- A network's exposure to ARP poisoning attacks can be reduced by segregating sensitive hosts between layer three devices or by using ***Virtual LAN (VLAN)*** functionality on switches. For highly sensitive hosts, administrators can statically define important MAC entries, such as the default gateway.
- Statically defined MAC entries will take precedence over MAC entries that are learned via ARP. Statically defining ARP entries carries a high administrative burden and does not scale well, but can protect small networks that require high security.

3.2.1.5 Routers

Routers operate at layer three, the network layer of the OSI model, designed to receive, analyze and forward incoming packets to another network and hence also known as 'Internetworking' device.

- The dominant layer three protocol in use today is Internet Protocol Version 4 (IPv4). Routers are primarily used to move traffic between different networks, as well as between different sections of the same network.
- Routers learn the locations of various networks in two different ways : dynamically via routing protocols and manually via administratively defined static routes. Networks usually use a combination of the two to achieve reliable connectivity between all necessary networks.
- Static routes are required when a network can't or shouldn't be directly learned via a routing protocol. For example, to ensure that they aren't tricked into routing traffic to an attacker, firewalls typically do not run routing protocols. If a firewall is not informing the network of any networks behind it, those routes must be statically added to a network router and propagated. Additionally, static routes can be added for any interconnected network that cannot or does not communicate with the routing protocols on the network.
- Cisco router, issue the following command :

```
Router(config-router)#passive-interface FastEthernet0/0
Router(config)#access-list 1 permit 192.168.10.0
Router(config)#access-list 2 permit 192.168.20.0
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.10.0
Router(config-router)#distribute-list 1 in
Router(config-router)#network 192.168.20.0
Router(config-router)#distribute-list 2 out
```

Routing protocols

There are several routes that a packet can travel from the source network to the ultimate destination network. Routing protocols implements some mechanism to choose a best route for a packet to travel. There are two main types of layer three routing protocols: distance-vector protocols and link-state protocols. The main difference between the two types is in the way they calculate the most efficient path to the ultimate destination network.

a) ***Distance-vector protocols*** are better suited for smaller networks (less than 15 routers), and require less CPU power on the devices that run them. Distance-vector protocols maintain tables of distances to other networks. The metric (cost) is distance, which is measured in terms of *hops*, with each additional router that a packet must pass through

being considered a hop. The most popular distance-vector protocol is the Routing Information Protocol (RIP).

b) ***Link-state protocols*** were developed to address the specific needs of larger networks. Link-state protocols use several different metrics to determine the best route to another network, and they maintain maps of the entire network that enable them to determine alternative and parallel routing paths to remote networks. Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) are examples of link-state protocols. Link-state protocols perform metric calculation and maintain databases of the entire network topology, and require significantly more CPU and memory capability than distance-vector protocols. As router hardware has evolved and more functions have been handled in silicon, such as in Cisco's Content Addressable Memory (CAM) and Ternary Content Addressable Memory(TCAM), a type of memory used by Cisco devices, even low-end routers can generally handle link-state routing (although many still have a limit on the number of routes they can handle).

Syllabus Topic : Network Hardening

3.2.2 Network Hardening

Q. 3.2.3 Explain network hardening in detail. (Ref. Secs. 3.2.2, 3.2.2.1, 3.2.2.2, 3.2.2.3, 3.2.2.4, 3.2.2.5) **(5 Marks)**

- Hardening is disabling of unwanted services and enabling of required services which require as per company standard policies and it is require for reducing security threats. Many would say it's all that but for SECURITY HARDENING there is allot more to consider in today's workplace mil, government, or private sector.
- It starts with complex passwords that are long and use special characters that are very hard to crack using cracking tools.
- A standing corporate policy (benchmarks) should be formalized and security audits would sweep the network to measure and identify any vulnerabilities based on advisories from organizations like SANS and Cisco. The network devices IOS should be regularly patched and 3DES or better encryption IOS using trusted root and subordinate certificates (from a trusted CA) should be used for access. Local accounts would be removed and network intrusion monitoring and prevention would be implemented on the device and the network. The device admin access could be restricted to changes from only one IP or AAA server.

- Think of it like a wrapper around everything based on polices where the goal is to try to block rouge hackers from gaining control to the devices even if it's only passive and not malicious intent.
- For example they don't want the switch but the data that passes through it and it's proprietary value. This has to be measured and proven in Network Hardening Reports. This work never ends, it runs in loops of maintenance and change and configuration control management "process".
- There are process when a team member leaves to change all the passwords or every 30 days to change all the passwords and they cannot be reused for a few years.

3.2.2.1 Patching

Q. 3.2.4 Explain network hardening in detail. (Ref. Secs. 3.2.2, 3.2.2.1, 3.2.2.2, 3.2.2.3, 3.2.2.4, 3.2.2.5) **(5 Marks)**

- Network devices such as routers and switches perform various functions like connecting, routing, filtering, forwarding, etc. The internal software of those network devices can have bugs as any other software. To correct those bugs, manufacturers create and publish code also known as patches or hot fixes.
- The act of updating the firmware of network devices is called patching. Patches and updates released by the product vendor should be applied in a timely manner.
- Quick identification of potential problems and installation of patches to address newly discovered security vulnerabilities can make the difference between a minor inconvenience and a major security incident. By subscribing to vendor's e-mail notification services user will receive timely notification of such vulnerabilities. After patching, the network device can work better or be more secure.

3.2.2.2 Switch Security Practices

Q. 3.2.5 Explain network hardening in detail. (Ref. Secs. 3.2.2, 3.2.2.1, 3.2.2.2, 3.2.2.3, 3.2.2.4, 3.2.2.5) **(5 Marks)**

- Network nodes are not directly aware that switches handle the traffic they send and receive; effectively making switches the silent workhorse of a network. Other than sometimes offering an administrative interface, layer two switches do not maintain layer three IP addresses, so hosts cannot send traffic to them directly. The primary attack against a switch is the ARP poisoning attack.

- Switches can also be used to create ***Virtual Local Area Networks (VLANs)***, layer two broadcast domains that are used to further segment LANs. ARP broadcasts are sent between all hosts within the same VLAN. To communicate with a host that is not in a VLAN, a switch must pass the host's packets through a layer three device and route them to the appropriate VLAN.
- Although there are some very specific exceptions to this rule for applications such as multicast (search the Web for "Multicast VLAN Registration" for details), in general, VLAN boundaries are helpful for containing and managing network segmentation, in addition to creating a foundation for applying differing levels of security to different networks based on the specific security needs.

3.2.2.3 Access Control Lists

Q. 3.2.6 Explain network hardening in detail. **(5 Marks)**
(Ref. Secs. 3.2.2, 3.2.2.1, 3.2.2.2, 3.2.2.3, 3.2.2.4, 3.2.2.5)

- Routers have the ability to perform IP packet filtering, an *Access Control Lists (ACLs)* can be configured to permit or deny TCP, UDP, or other types of traffic based on the source or destination address, or both, as well as on other criteria such as the TCP or UDP port numbers contained in a packet. While firewalls are capable of more in-depth payload inspection, strategically placed router ACLs can significantly increase network security.
- For example, ACLs can be used on edge or border routers to drop obviously unwanted traffic (such as RFC 1918 traffic originating from a source on the Internet), removing the burden from the border firewalls. ACLs can also be used on WAN links to drop broadcast and other unnecessary traffic, thus reducing bandwidth usage.
- ACLs are often used to protect the router itself, and for other more advanced functions. It is a best practice to use an ACL to allow only the management stations or hosts on a network used by administrative staff authorized to log in to the network devices to connect to the administrative services (such as Telnet, SSH, or HTTP) on a router. Many vendors have unique functionality embedded in the ACL engines within their devices. Not all ACLs are created equal; it is a good practice to understand a vendor's implementation and use of ACLs within its technology, as some specific features may be more or less desirable to networks performing different functions. A simple ACL in a Cisco router could be implemented with the following commands:

```
router(config)#access-list 11 deny tcp any anyeq 23
router(config)#access-list 11 deny tcp host 10.10.0.1 any eq www
```



```
router(config)#access-list 11 permit ip any any
```

- Telnet uses TCP, port 23. This configuration shows that all TCP traffic for port 23 is blocked, also disallow HTTP sessions with a source address of10.10.0.1 to all destinations. The last line of the ACL permits all other traffic.
- To enforce this ACL, it must be applied to an interface with the access-group command :

```
router(configYif)#ip access-group 11 in
```

3.2.2.4 Disabling Unused Services

Q. 3.2.7 Explain network hardening in detail. **(5 Marks)**
(Ref. Secs. 3.2.2, 3.2.2.1, 3.2.2.2, 3.2.2.3, 3.2.2.4, 3.2.2.5)

As with general-purpose operations, routers run services that are not required for the process of routing packets. Taking steps to disable and protect such services can increase the overall security of the network.

(a) Proxy ARP
(b) Network Discovery Protocols
(c) Other Extraneous Services

➜ a) Proxy ARP

- Proxy ARP allows one host to respond to ARP requests on behalf of the real host. This is commonly used on a firewall that is proxying traffic for protected hosts.
- Cisco routers have Proxy ARP enabled by default, and this may allow an attacker to mount an ARP poisoning attack against a host that is not on the local subnet or VLAN.

➜ b) Network discovery protocols

- There are several automatic discovery protocols, some of which are vendor specific, such as Cisco Discovery Protocol (CDP), others of which are open standard, such as Link Layer Discovery Protocol - Media Endpoint Devices (LLDP-MED).
- These protocols provide some level of convenience for administering networks, but they also present the opportunity for anyone sniffing the network to learn a significant amount of information about the network topology. If these protocols are not actively used, they should be disabled and if they are used, careful attention should be paid to securing them as much as possible.

➜ **c) Other extraneous services**

All routers provide a number of services that can be disabled if they are not needed. The following is a list of example services, depending on network requirement an administrator can disable them or secure them from unauthorized access or use.

(i) Diagnostic Services	(ii) BOOTP Server
(iii) TFTP Server	(iv) Finger Server
(v) Web Server	

➜ **i) Diagnostic Services**

- Most routers have a number of diagnostic services enabled for certain UDP and TCP services, including echo, charged (intended for testing, debugging, and measurement purposes), and discard. These services should be disabled when not in use for troubleshooting or testing.
- Certain debug functions are particularly resource intensive, and an attacker could create a Denial of Service (DoS) condition simply by accessing a compromised router and turning on a debug process that consumes all of the available resources on the device.
- An administrator could also inadvertently create an outage in the same manner. Different vendors have different approaches to how much resources on a router these functions are allowed to use at any given time, including some with adjustable thresholds. These functions can be used for customised network configuration.

➜ **ii) BOOTP Server**

Routers can be used to provide DHCP addresses to clients through the BOOTP service. For Small Office/Home Office (SOHO) and residential setups, the router frequently is the DHCP server, but for enterprise, it is less common. If not in use, can be disabled.

➜ **iii) TFTP Server**

Trivial File Transfer Protocol (TFTP) is a simple protocol used for transferring files. TFTP uses the User Datagram Protocol (UDP) to transport data from one end to another. TFTP is mostly used to read and write files/mail to or from a remote server.

➜ **iv) Finger Server**

The finger service can be queried to see who is logged in to the router and from where. Disabling this service can protect user's information leakage.

➜ **v) Web Server**

Many vendors provide a web server for making configuration changes. If the router will not be managed in this manner, the web server can be disabled.

- These services and several others pose security risks to the normal operation of the router while they are running.
- Different equipment manufacturers will have a variety of services that can potentially run on their devices, and it is important to understand what these are and which are really needed for operation.
- The best practice recommendation is to turn off the services until they are needed.

3.2.2.5 Administrative Practices

Q. 3.2.8 Explain network hardening in detail. (Ref. Secs. 3.2.2, 3.2.2.1, 3.2.2.2, 3.2.2.3, 3.2.2.4, 3.2.2.5) (5 Marks)

- Routers have a number of methods by which they can be managed. A command-line interface is accessible directly from a console or remotely via either Telnet or the Secure SHell protocol (SSH). SSH is recommended, as Telnet is sent over the network in clear text. Additionally, a web interface can be accessed via a browser, or the router can be monitored and managed via the Simple Network Management Protocol (SNMP).
- Some routers that allow user to download the configuration and manipulate it, compile it, and test that it is compatible and correct prior to uploading to the device. Securing each of these management protocols is of paramount importance, so they cannot be abused by attackers.
- Another important step when hardening network devices is to configure a banner that is displayed whenever a connection is established as part of the login process, often called a login banner or Message-Of-The-Day (MOTD) banner. The banner doesn't include any important information that may identify the device type or the operating system on the device, also it is a good practice to include in the banner a warning message regarding unauthorized use of the device.
- This ensures that an individual cannot argue that they didn't know that their use was unauthorized. It is a good idea not to include details such as the physical location of the device or the name of the organization it belongs to. There is no good reason to offer a potential attacker any details that they could use for malevolent purposes or to support another component of an attack, such as social engineering.

a) Remote Command Line

- Telnet is a very old command-line protocol for remote connections. A weakness of the Telnet connectivity protocol is that it does not protect communications while they are in transit over the network (it does not use any data encryption). As a more secure alternative, most routers support the Secure SHell (SSH) protocol. SSH provides the same interface and access as Telnet, but it encrypts all communications. Failure to encrypt administrative connections to network routers may allow an attacker to capture sensitive information, such as passwords and configuration parameters, while they are in transit over the network.
- To enable SSH, it is necessary to configure host and domain names on the router, generate an encryption key, configure accounts, and set required SSH parameters. The commands to complete the configuration vary on a per-device basis.
- By default, many network devices maintain one password to access the device and a second password to access configuration commands, commonly called "privileged" or "enable" access. Even if this is not the default behavior, it can usually be configured. This is not true in all cases, depending on the manufacturer, the default account setup and how accounts are handled and permissioned may vary.
- To provide granular authorization and full accountability, individual user accounts can and should be created, although not necessarily locally on the device; the approach and decision to use named accounts on a per-individual basis is much more important than where the accounts are created and stored. Even if individual or generic local accounts will be used, different passwords for any default accounts can be set.
- Morden network devices today use a commodity operating system, typically some flavor of Unix, where account information such as passwords are stored as a hashed value or in an encrypted file.
- Determining the type of encryption and methods used for locally stored passwords is relevant and should be understood prior to deploying devices into production, if for no other reason than to understand what a password recovery procedure might involve.
- It is entirely conceivable that being able to recover a password on a device could prove in valuable such as in a scenario where an attacker finds a way to lock an administrator out of a critical piece of infrastructure, which can sometimes be done without actually gaining access to the device (for example, too many failed attempts from a certain account).

b) Centralizing Account Management (AAA)

- Most network devices can be configured to authenticate against a central account repository via Authentication, Authorization, and Accounting (AAA). This helps remove usernames and passwords from local configurations (although having a backup local account with a more complex password is a best practice, when it is reserved only for emergencies).
- *Authentication* is the component that determines if an incoming connection is allowed, a*uthorization* determines what level of access or privilege the authenticated account is allowed, and *accounting* keeps track of everything that the authenticated and authorized account does.
- Using the AAA methodology for device access is a best practice and can fully support auditability, an important consideration when trying to unravel what may have happened with too many hands in the cookie jar.
- While AAA is the mechanism, it is also critical to have a strong methodology around administrative device account creation and use policy.
- Requiring that administrators have a separate account specifically for administrative purposes will help protect critical network equipment, some additional features can be configured such as more frequent password rotation for admin accounts or more stringent password complexity requirements.
- The only tangible downside to the approach (besides the overhead of maintaining one or more systems that perform the AAA functionality) is that if one of these elevated privilege accounts is compromised, an attacker would have access to things they may not have otherwise. However, this is less risky than using the same local username and password on all devices, because once the breach is discovered, the accounts can be disabled from a single place.
- The two most common protocols used for these access devices to perform device-level AAA communication are RADIUS and TACACS (now TACACS+). RADIUS is documented in RFC 2865, while TACACS+ is a Cisco-developed protocol. A newer protocol, *Diameter*, currently underdevelopment at IEEE, is aimed at replacing RADIUS. Defined in RFC 3588, Diameter will eventually become the newer AAA framework, with more advanced functionality than RADIUS or TACACS+ but essentially intended to solve the same basic problem. Because of its more advanced functionality and security, TACACS+ has been adopted or licensed for use by a variety of different equipment manufacturers and is currently the most common AAA protocol.
- These AAA protocols constitute part of a framework and can achieve the same goal that is securing AAA communication between an authenticator and endpoint. In

addition to devices that use RADIUS and TACACS+, there are some devices that can directly query an LDAP or X.500 directory, but it is most common to find RADIUS or TACACS+ in use for communicating with network devices, even if some sort of directory like LDAP or Active Directory is the actual back-end database (many of the access control server products can map groups to an LDAP directory). Using the granular controls and variables offered by these protocols, administrative control can be finely tuned for specific needs.

- Authentication to a network device should not rely completely on a remote authentication server. If the server can be down or unavailable, no one could log in. Therefore, keeping a local backup account is a good precautionary measure. Beyond simply authenticating access to the router, it is good practice to limit the locations from which such connections can be initiated.
- For example, denying Telnetor SSH sessions to the border routers from external networks, or to core routers from the entire internal network if not needed.
- ACLs are packet filters that will either accept or deny packets based on the packet's layer three header information, and can be employed to control the access management to the device itself.

c) Simple Network Management Protocol (SNMP)

- Network devices can also be monitored and managed via Simple Network Management Protocol (SNMP), which provides a centralized mechanism for monitoring and configuration. SNMP can be used to monitor such things as link operation, port status and statistics, and CPU load via *Management Information Base Object Identifiers (MIBOIDs)*, a structured format database that describes objects within a device that can be monitored or managed by SNMP or another management protocol.
- As SNMP has evolved as a tool, and its capabilities have expanded, its security has improved. The first version, SNMPv1, was originally released in 1988, with a little consideration for the security of the protocol itself. A "community string" similar to a password for a built-in account was used for authenticating the protocol (with a well-known default value that was rarely changed), and all other protections were left to the configuration of the device.
- Also, depending on the configuration within the device, the community string could be used as Read-Only[RO] or Read-Write [RW], the second option offering a tempting vehicle for malicious intent by providing access to change, not just read, device settings.

- SNMPv2 addressed many of the issues with SNMPv1, including performance, but added significant complexity. The most common flavour of SNMPv2 in use in the field is SNMPv2c.SNMPv3, the current version, doesn't change the protocol functionally but adds the capability of encryption, message integrity, and authentication of traffic.
- SNMP can be a powerful tool to alert personnel to detected problems by sending traps to configured consoles. *Traps* are unsolicited messages that a device will send when a configured threshold is exceeded or a failure occurs. SNMP consoles can be used to proactively monitor network devices and generate alerts if connectivity is lost or if other defined threshold conditions are violated. SNMP is the most prolific approach in use today for monitoring networks.
- Protecting SNMP communications can be done by configuring an ACL on each device to control which stations are allowed to query the device via SNMP, and what they are allowed to do. RW SNMP should be used only if there is specific functionality or automation that requires read-write access. Otherwise, for node managers that are only gathering statistics, use RO.
- The SNMPv1 has significant security risks. SNMPv1 traffic, including authentication credentials, is not encrypted. Authentication consists of a community string, sent in clear text over the network, and many implementations did not change the default strings from "public" for read access and "private" for write access.

3.2.2.6 Internet Control Message Protocol (ICMP)

Q. 3.2.9 Explain security related to ICMP. (Ref. Sec. 3.2.2.6) (5 Marks)

- The Internet Control Message Protocol (ICMP) provides a mechanism for reporting TCP/IP communication problems, as well as utilities for testing IP layer connectivity. ICMP is not a transport protocol that sends data between systems rather it is use to generate error messages to the source IP address when network problems prevent delivery of IP packets.
- ICMP is not used regularly in end-user applications, it is used by network administrators to troubleshoot Internet connections in diagnostic utilities including ping and trace route. However, ICMP can also be used to glean important information regarding network topologies and available host services.
- ICMP was originally defined by RFC 792, but has since been updated by several other RFCs and is currently described by RFC 4884. Many different types of ICMP communications are defined, and are commonly referred to as messages. The following relevant ICMP functions present various risks when used for malicious purposes.

a) ECHO and traceroute

- Echo requests and replies, more commonly known as *pings*, which is used to determine if another host is available and reachable across the network or not. This does not guarantee that there are no other barriers or restrictions in place, but it does at least demonstrate reachability.
- While there are many cases where reachability exists but ping does not work (on some networks routers have been configured to drop ICMP messages), it is a basic tool used by systems and network administrators to very quickly determine if a particular host is up or down.
- An attacker can use ping to scan publicly accessible networks to identify available hosts, though more experienced attackers avoid ping and use more stealthy methods of host identification. Another use of ICMP echo and echo reply has been to create covert channels through firewalls that allow malicious traffic to pass through unchecked, under the assumption that nothing bad can be contained in an ICMP packet. ICMP echo requests and replies should be dropped at the network perimeter.
- Trace route is not itself an ICMP message type, but rather a method that frequently employs ICMP messages. It is also used to troubleshoot network-layer connectivity by mapping the network path between the source and destination hosts. Trace route is useful in pinpointing where along the network path any connectivity troubles are occurring.
- Trace route works by sending out consecutive packets with the Time To Live (TTL) field incremented by one each time. When a network device routes a packet, it always decreases the

b) Unreachable messages

- Type 3 ICMP message is Destination Unreachable message. A router returns an ICMP Type 3 message when it cannot forward a packet when destination is unreachable. There are over 15 different types of codes they are given in following Table 3.2.3.

Table 3.2.3 : ICMP Unreachable message code types

Code	Message	Description
0	Network unreachable	The router does not have a route to the specified network.
1	Host unreachable	The host on the destination network does not respond to ARP.

Code	Message	Description
2	Protocol unreachable	The layer four protocol specified is not supported through the router.
3	Port unreachable	The layer four protocol cannot contact a higher layer protocol specified in the packet.
4	Fragmentation needed	The size of the packet exceeds the maximum size allowed on the segment, but the packet's *DO NOT FRAGMENT* bit is set.
5	Source route failed	The next hop specified by the source route option is not available.
9 and 13	Communication	
Administratively prohibited	A router has been configured to drop such communications to the destination host or network.	

- There is an important consequence to dropping all Destination Unreachable messages. Code 4, Fragmentation Needed, is a very important message for proper network operation and disruptions can occur if hosts cannot be informed that the packets they are sending through the network exceed the Maximum Transmission Unit (MTU) of that network.

c) Directed broadcasts

- The first and last IP addresses of any given network are treated as being special. These addresses are known as the network address and the broadcast address, respectively.
- Sending a packet to either of these addresses is similar to sending an individual packet to each host on that network. Thus, someone who sends a single ping to the broadcast address on a subnet with 100 hosts could receive 100 replies.
- This functionality can cause the ***bandwidth amplification attacks***. Examples of tools that use this attack are known as smurf and fraggle.
- Ina ***smurf attack***, the attacker sends ICMP traffic to the broadcast address of a number of large networks, inserting the source address of the victim. This is done so that the ICMP replies are sent to the victim and not the attacker.

- In a fraggle attack, the attacker also sends packets to large broadcast addresses in order to create a large number of responses, but this attack uses UDP ECHO packets instead of ICMP ECHO packets.
- The end result is the same. These UDP packets will generate responses from each system that is reachable and answering in the network range, and it can be more effective due to the behavior of certain services that use the UDP protocol.
- Modern firewalls can detect and defend against these types of attacks, but often rely on being configured to do so. Defending against these types of exploits should be a basic component of any firewall setup.

d) Redirects

- Redirect message occurs when a host sends a datagram (or packet) to its gateway (destination of this datagram is a different network), which in turn forwards the same datagram to the next gateway (next hop) and this second gateway is on the same network as the host.
- The second gateway will generate this ICMP message and send it to the host from which the datagram originated.

3.2.2.7 Anti-Spoofing and Source Routing

Q. 3.2.10 Explain security related to antispoofing. (Ref. Sec. 3.2.2.7) (5 Marks)

- IP address spoofing is the creation of IP packets with a false source IP address, for the purpose of hiding the identity of the sender. Address spoofing is an attempt to slip through external defenses by masquerading as an internal host, and internal packets should obviously not be arriving inbound on border routers.
- Dropping such packets protects the network against such attacks, and border routers can be used to drop inbound packets containing source IP addresses matching the internal network. Routers should also drop packets containing source addresses matching RFC 1918 private IP addresses and broadcast packets.
- In addition to spoofed packets, routers should be configured to drop packets that contain source routing information. Source routing is used to dictate the path that a packet should take through a network. Such information could be used to route traffic around known filters or to cause a denial of service situation by forcing large amounts of traffic through a single router, overloading it.

3.2.2.8 Logging

Q.3.2.11 Explain security related to logging. (Ref. Sec. 3.2.2.8) (5 Marks)

- Routers are able to login formation related to ACL activity as well as system-related information. Syslog can become a critical component for troubleshooting something that happened on a network, or for performing forensics.
- While the logging host itself needs to be managed, an exercise to determine the right duration of archival logs should be performed when deploying a network; 30 or 60 days worth of logs is common, although in some cases they are needed for longer.
- Determining the right logging level (known as a facility, different levels of which dictate the verbosity and severity of the incident required to trigger a log action or trap) and for how long you will keep those logs gives you a window of time into the past, allowing a look back at what was going on in different places around the network at a given point in time.

3.3 Firewalls

Q.3.3.1 Describe about firewalls. (Ref. Sec. 3.3) (5 Marks)

- Firewalls have been one of the most popular and important tools used to secure networks. The basic function of a firewall is to monitors and controls incoming and outgoing network traffic based on predetermined security rules for the purposes of preventing unauthorized access between computer networks.
- In computer networks, applications running internally and externally on servers and workstations (and sometimes on other network devices or appliances) generates network traffic.
- Thus, managing a network traffic via firewalls is application communication management on layers one through seven of the OSI stack. Applications are what firewalls are really all about.
- Firewall is not just a network appliance it is one of the tools which can be implemented as both hardware and software, or a combination of both and it is used for managing the behaviour of applications.

Syllabus Topic : Overview

3.3.1 Overview of Firewalls

- Firewalls are the first line of defense between the internal network and untrusted networks like the Internet. First concern before applying any type of protection is to understand what is really needs to protected to achieve the right level of protection for an environment.

- First introduced conceptually in the late 1980s in a whitepaper from Digital Equipment Corporation, "firewalls" provided a then new and important function to the rapidly growing networks of the day.
- Before dedicated hardware was commercially available, router-based access control lists were used to provide basic protection and segregation for networks. However, they proved to be inadequate as emerging malware and hacking techniques rapidly developed. Consequently, firewalls evolved over time so their functionality moved up the OSI stack from layer three to layer seven.

Syllabus Topic : The Evolution of Firewalls

3.3.1.1 The Evolution of Firewalls

- First-generation firewalls were simply permit/deny engines for layer three (network) traffic, working much like a purposed access control list appliance. Originally, first-generation firewalls were primarily used as header-based packet filters, capable of understanding source and destination information up to OSI layer four (transport: ports). Second-generation firewalls were able to keep track of active network sessions, putting their functionality effectively at layer four. These were referred to as ***stateful firewalls*** or, less commonly, ***circuit gateways***.
- When an IP address (for example, a laptop) connected to another IP address (a web server) on a specific TCP or UDP port, the firewall would enter these identifying characteristics into a table in its memory. This allowed the firewall to keep track of network sessions, which could give it the capability to block ***Man-In-The-Middle (MITM)*** attacks from other IP addresses.
- The third generation of firewalls focused on application layer (layer seven) protection. These "application firewalls" were able to decode data inside network traffic streams for certain well-defined, preconfigured applications such as HTTP (the language of the web), DNS (the protocol for IP address lookups), and older, person-to-computer protocols such as FTP (the data transfer) and Telnet (remote assess).
- Today's current generation of firewalls (commonly termed the fourth generation), have the intelligence and capability to look inside packet payloads and understand how applications function. As silicon has increased in speed, advanced router-based firewalls exist today that can provide IP inspection as a software component of a multipurpose router, although they do not provide the speed or sophistication of today's industrial-strength firewalling solutions.

- Fourth-generation firewalls can run application-layer gateways, which are specifically designed to understand how a particular application should function and how its traffic should be constructed and patterned (traffic that conforms predictably to an application's well-defined communication protocol is referred to as "well formed").
- There are fifth generation firewalls, which are internal to hosts and protect the operating system kernel and some sixth-generation firewalls have been described (meta firewalls), but most network appliances fall into the generally accepted fourth-generation firewall definition.
- Some manufacturers call their devices "next-generation firewalls" or "zone-based firewalls," and these essentially function under the same guiding principles of the fourth-generation designs.

3.3.1.2 Application Control

- Firewalls have always been intended to handle application traffic. Some applications are authorized, and some aren't. For example, web traffic outbound to Internet web sites is commonly permitted, while some types of peer-to-peer software are not.
- On those applications that are allowed, certain behaviours are allowed within the application and others aren't. For instance, a system on internet is only allowing are mote access to certain systems, but the file-sharing capabilities for those systems might be restricted.
- First- and second-generation firewalls could restrict simple applications that functioned on well-known ports. Back then, applications were well behaved, communicating on assigned ports that were well documented, so they were easy to control.
- But application developers did not always want to be subject to control, so they devised a simple but effective way to get through the firewall use port 80. This is known as "tunnelling" or "circumventing." Since web traffic uses the HTTP protocol over TCP port 80, it had to be allowed to pass through the firewall unrestricted.
- The third-generation firewall, an Application firewalls observe the contents of the HTTP traffic traversing port 80, and determine whether it consisted of web site to browser requests and responses, or something else tunnelling through from an application on a local workstation to a remote server.
- This provided a basic ability to block applications that were prohibited by security policies, but it didn't usually help with controlling application behaviour (such as allowing voice but not video, or transfer of document files but not photos and movies). Security administrators were concerned about different types of software that could violate security policies, following are some of those security policies :

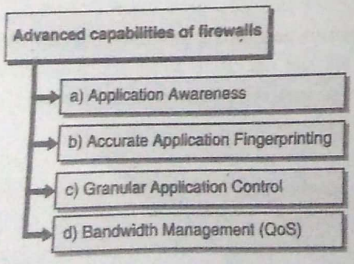
- **Peer-to-peer file sharing :** Direct system-to-system communication from an inside workstation to another one on the Internet that could leak confidential documents, or expose the organization to liability from music and movie copyright violations.
- **Browser-based file sharing :** Web sites that provide Internet file storage via a web browser, which allow trusted people inside an organization's network to copy files outside the security administrator's area of control.
- **Web mail :** Mail services with the capability to add file attachments to messages, providing a path to theft and leakage of confidential materials.
- **Internet proxies and circumventors :** Services running on the Internet or on local workstations explicitly designed to bypass security controls like web filtering.
- **Remote access :** Remote administration tools, usually used by system administrators to support internal systems from the Internet, which could be abused by Internet attackers.

– None of these were easy to control using application-aware firewalls, which could really only block broad categories of applications from functioning, or the Internet addresses they needed to connect to, but never with 100 percent effectiveness. That's where fourth-generation firewalls come in. These devices have advanced heuristic application detection and behaviour management capabilities. Circumventing network security controls by using allowed ports isn't effective any more. Until application developers come up with a new way to circumvent the firewall, the security administrator is back in control.

3.3.1.3 Must-Have Firewall Features

– Today's firewalls are expected to do much more than simply block traffic based on the outward appearance of the traffic (such as IP address and the TCP or UDP port).

– As applications have become increasingly complex and adaptive, the firewall has become more sophisticated in an attempt to control those applications. Some of the advanced capabilities of firewalls are as follows :



➜ **a) Application awareness**

The firewall must be able to process and interpret traffic at least from OSI layers three through seven. At layer three, it should be able to filter by IP address; at layer four by port; at layer five by network sessions; at layer six by data type, and, most significantly, at layers even to properly manage the communications between applications.

➜ **b) Accurate application fingerprinting**

The firewall should be able to correctly identify applications, not just based on their outward appearance, but by the internal contents of their network communications as well. Correct application identification is necessary to ensure that all applications are properly covered by the firewall policy configuration.

➜ **c) Granular application control**

Along with allowing or denying the communication among applications, the firewall also needs to be able to identify and characterize the features of applications so they can be managed appropriately. File transfer, desktop sharing, voice and video, and in-application games are examples of potentially unwanted features that the firewall should be able to control.

➜ **d) Quality of Service (QoS)**

The Quality of Service (QoS) of preferred applications, which might include Voice over IP (VoIP) for example, can be managed through the firewall based on real-time network bandwidth availability. If a sporting event is broadcast live via streaming video on a popular web site, firewall should be able to proactively limit or block access so all those people who want to watch it don't bring down your network. The firewall should integrate with other network devices to ensure the highest possible availability for the most critical services.

Syllabus Topic : Core Firewall Functions

3.3.2 Core Firewall Functions

Q. 3.3.2 Explain core firewall functions. (Ref. Sec. 3.3.2) (5 Marks)

Firewalls are ideally situated for performing certain functions in addition to controlling application communication. These include Network Address Translation (NAT), which is the process of converting one IP address to another, and logging of traffic.

3.3.2.1 Network Address Translation (NAT)

- **Network Address Translation** (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.
- The primary version of TCP/IP used on the Internet is version 4 (IPv4). Version 4 of TCP/IP was created with an address space of 32 bits divided into four octets, mathematically providing approximately four billion addresses. As internet is growing so fast, this address space is not sufficient.
- In order to conserve IPv4 addresses, RFC 1918 specifies blocks of addresses that will never be used on the Internet. These network ranges are referred to as "private" networks and are identified in Table 3.3.1. This allows organizations to use these blocks for their own corporate networks without worrying about conflicting with an Internet network.

Table 3.3.1 : Private Addresses Specified in RFC 1918

Address	Mask	Range
10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

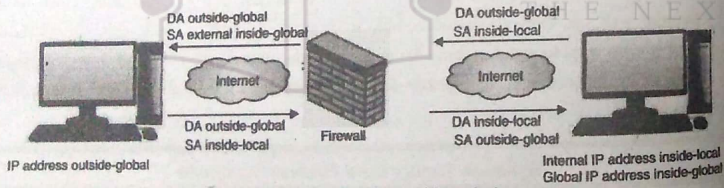


Fig. 3.3.1 : Network Address Translation

- A NAT (Network Address Translation or Network Address Translator) is the virtualization of Internet Protocol (IP) addresses. NAT helps improve security and decrease the number of IP addresses an organization needs.
- Once the packet crosses the firewall and is translated, the addresses will be called the host's ***global addresses***. These terms, as depicted in Fig. 3.3.1, the following sections to

describe the various types and nuances of NAT. The abbreviations "DA" and "SA" refer to "destination address" and "source address" respectively.

a) Static NAT

- A static NAT configuration always results in the same address translation. The host is defined with one local address and a corresponding global address in a 1:1 relationship, and they don't change.
- The static NAT translation rewrites the source and destination IP addresses as required for each packet as it travels through the firewall. No other part of the packet is affected. This is typically used for internal servers that need to be reachable from the Internet reliably on an IP address that doesn't change. See Fig. 3.3.2.

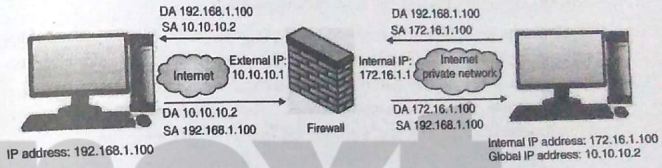


Fig. 3.3.2 : NAT replacing global terms with actual IP addresses

- Due to this simple approach, most protocols will be able to traverse static NAT without problems. The most common use of static NAT is to provide Internet access to a trusted host inside the firewall perimeter, or inbound access to a specific host, such as a web server that needs to be accessible via a public IP address.

b) Dynamic NAT

- Dynamic network address translation (Dynamic NAT) is a technique in which multiple public Internet Protocol (IP) addresses are mapped and used with an internal or private IP address.
- It allows a user to connect a local computer, server or networking device to an external network or Internet group with an unregistered private IP address that has a group of available public IP addresses.
- This address can then be reused by a different host.
- One advantage of dynamic NAT over static NAT is that it provides a constantly changing set of IP addresses from the perspective of an Internet-based attacker, which makes targeting individual systems difficult. The limitation of dynamic NAT

is that it limits on the number of concurrent users on the inside who can access external resources simultaneously.

- The firewall will simply run out of global addresses and not be able to assign new ones until the idle timers start freeing up global addresses.

c) Port Address Translation

- ***Port Address Translation*** (PAT), is an extension to NAT that permits multiple devices on a Local Area Network (LAN) to be mapped to a single public IP address. This is done by modifying the communication port addresses in addition to the source and destination IP addresses. The goal of PAT is to conserve IP addresses.
- Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router.
- When Computer A logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This gives Computer a unique address. If Computer B logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.
- Thus, the firewall can use a single IP address for multiple communications by tracking which ports are associated with which sessions. For example, the sending host initiates a web connection on source port1705.
- When the packet traverses the firewall, in addition to replacing the source IP address, the firewall translates the source port to port 4500 and creates an entry in a mapping table for use in translating future packets. When the firewall receives a packet back for destination port4500, it will know how to translate the response properly. Using this system, thousands of sessions can be PATed behind a single IP address simultaneously.

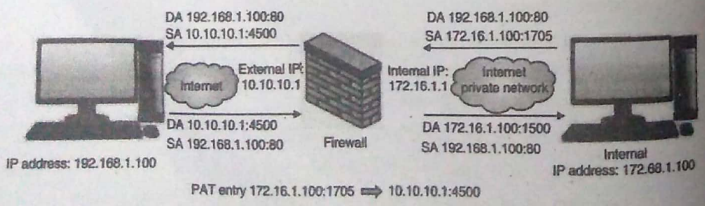


Fig. 3.3.3 : An example of Port Address Translation

- PAT provides an increased level of security because it cannot be used for incoming connections.

3.3.2.2 Auditing and Logging

- Firewalls are excellent auditors. Attack attempts will leave evidence in logs, and if network administrators are watching systems diligently, attacks can be detected before they are successful. Therefore, it is important that system activity be logged and monitored.
- Firewalls should record system events that are both successful and unsuccessful. Since this can generate a huge volume of log traffic, the logs are best sent to a Security Information and Event Management (SIEM) system that can filter, analyze, and perform heuristic behaviour detection to help the network and security administrators.

Syllabus Topic : Additional Firewall Capabilities

3.3.3 Additional Firewall Capabilities

Q. 3.3.3 Discuss about some additional security feature of firewall. (Ref. Sec. 3.3.3) (5 Marks)

Modern firewalls can do more than manage application communications and behaviors; they can also assist in other areas of network quality and performance.

3.3.3.1 Application and Website Malware Execution Blocking

- An older version of viruses required a user to click on some disguised link or button to execute. If the end users were sophisticated enough to recognize the virus writer's tricks, these viruses wouldn't get very far.
- Modern malware can execute and spread itself without the intervention of end users. Through automatic, browser-based execution of code (via ActiveX or Java, for example), simply opening a web page can activate a virus. Adobe PDF files can also transmit malware, due to their extensive underlying application framework. Firewalls with advanced anti-malware capability should be able to detect the seinvisible malware vectors and stop them in their tracks. They should also be able to block the communication to a Command and Control (CnC) server once malware successfully implants itself on a victim system and tries to reach back to its controller for instructions.

3.3.3.2 Antivirus

- Firewalls that are sophisticated enough to detect malware can (and should) block it on the network. Worms that try to propagate and spread themselves automatically on the network, and malware that tries to "phone home," can be stopped by the firewall, confining their each.
- Malware control solutions should be layered, and the firewall can form an important component of a network-based malware blocking capability to complement your organization's endpoint antivirus software.

3.3.3.3 Intrusion Detection and Intrusion Prevention

- Intrusion detection and prevention are two broad terms describing application security practices used to mitigate attacks and block new threats.
- Intrusion detection is a reactive measure that identifies and mitigates on going attacks using an intrusion detection system. It's able to weed out existing malware (e.g., Trojans, backdoors, root its) and detect social engineering (e.g., man in the middle, phishing) assaults that manipulate users into revealing sensitive information.
- Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents to the system more secure. Firewalls can provide IDS and IPS capabilities at the network perimeter, which can be a useful addition or substitution for standard purpose-built intrusion detection and prevention systems, especially in a layered strategy.

3.3.3.4 Web Content (URL) Filtering and Caching

- The firewall is optimally positioned on the network to filter access to web sites (between an organization's internal networks and the Internet). A separate URL filtering system or service can be implemented, or a built-in capability of firewall can be used.
- Today's firewalls are demonstrating web content filtering capabilities that rival those of purpose-built systems, so users may be able to save money by doing the filtering on the firewall especially if it doesn't cost extra.

3.3.3.5 E-Mail (Spam) Filtering

A modern firewall can also subtract the spam from e-mail messages before they get delivered to a mail server. User can sign up for an external service or buy a purpose-built spam filter instead, but with a firewall that includes this capability, provides users an additional option.

3.3.3.6 Enhance Network Performance

- Firewalls need to be able to run at wire speed fast enough to avoid bottle necking application traffic. They should be able to perform all the functions that have been enabled without impacting performance. In addition, firewalls should be able to allocate network bandwidth to the most critical applications to ensure QoS, without sacrificing filtering functionality.
- As firewall features continue to become more sophisticated, the underlying hardware needs to keep up. If a network has a low tolerance for performance impact, firewall platforms that are built for speed can be used to enhance network performance.

Syllabus Topic : Firewall Design

3.3.4 Firewall Design

Q. 3.3.4 Describe the firewall design for achieving security measures. (Ref. Sec. 3.3.4) **(5 Marks)**

- Firewalls may be software based or, more commonly, purpose-built appliances. Sometimes the firewalling functions are actually provided by a collection of several different devices.
- The specific features of the firewall platform and the design of the network where the firewall lives are key components of securing a network.
- To be effective, firewalls must be placed in the right locations on the network, and configured effectively. Best practices of firewall designing are as follows :

a) All communications must pass through the firewall. The effectiveness of the firewall is greatly reduced if an alternative network routing path is available; unauthorized traffic can be sent through a different network path, bypassing the control of the firewall. Assuming the firewall as lock on organisation's front door. It can be the best lock in the world, but if the back door is unlocked, intruders don't have to break the lock on the front door they can go around it. The door lock is relied upon to prevent unauthorized access through the door, and a firewall is similarly relied upon to prevent access to a network.

b) The firewall permits only traffic that is anthorized. If the firewall cannot be relied upon to differentiate between authorized and unauthorized traffic, or if it is configured to permit dangerous or unneeded communications, its usefulness is also diminished.

c) In a failure or overload situation, a firewall must always fail into a "deny" or closed state, under the principle that it is better to interrupt communications than to leave systems unprotected.

d) The firewall must be designed and configured to resist attacks upon itself. Because the firewall is relied upon to stop attacks, and nothing else is deployed to protect the firewall itself against such attacks, it must be hardened and capable of resisting attacks directly upon itself.

3.3.4.1 Firewall Strengths and Weaknesses

A firewall is just one component of an overall security architecture. Its strengths and weaknesses should be taken into consideration when designing network security.

☞ **Firewall strengths**

Consider the following firewall strengths when designing network security :

- Firewalls are excellent at enforcing security policies. They should be configured to restrict communications to what management has determined and agreed with the business to be acceptable.
- Firewalls are used to restrict access to specific services.
- Firewalls are transparent on the network no software is needed on end-user workstations.
- Firewalls can provide auditing. Given plenty of disk space or remote logging capabilities they can log interesting traffic that passes through them.
- Firewalls can alert appropriate people of specified events.

☞ **Firewall weaknesses**

You must also consider the following firewall weaknesses when designing network security :

- Firewalls are only as effective as the rules they are configured to enforce. An overly permissive rule set will diminish the effectiveness of the firewall.
- Firewalls cannot stop social engineering attacks or an authorized user intentionally using their access for malicious purposes.
- Firewalls cannot enforce security policies that are absent or undefined.
- Firewalls cannot stop attacks if the traffic does not pass through them.

3.3.4.2 Firewall Placement

A firewall is usually located at the network perimeter, directly between the network and any external connections. However, additional firewall systems can be located inside the

network perimeter to provide more specific protection to particular hosts with higher security requirements.

3.3.4.3 Firewall Configuration

Following best practices can be implemented while building a rule set on a firewall :

- Building rules from most to least specific. Most firewalls process their rule sets from top to bottom and stop processing once a match is made. Putting more specific rules on top prevents a general rule from hiding a specific rule further down the rule set.
- Configure all firewalls to drop "impossible" or "unroutable" packets from the Internet such as those from an outside interface with source addresses matching the internal network, RFC 1918 "private" IP addresses, and broadcast packets. None of these would be expected from the Internet, so if they are seen, they represent unwanted traffic such as that produced by attackers.

Syllabus Topics : Radio Frequency Security Basics

3.4 Radio Frequency Security

Q. 3.4.1 Explain in brief radio frequency security. (Ref. Sec. 3.4) (5 Marks)

- The popularity of IoT and all the devices getting connected wirelessly is imminent in today's life. The majority of these devices will communicate with each other wirelessly using radio protocols (frequency range ~ 3 kHz to 300 GHz). IoT devices use different Radio protocols such as ZigBee, RFID, Bluetooth etc. for communication.
- If we go back in time, many vulnerabilities have been found and exploited in IoT devices using some sort of radio communication. So, for pen testing IoT devices we need to have a strong foundation of various radio protocols, how they communicate and different modulation schemes they use for communication. Thus, analyzing radio communication is of utmost importance from a security point of view and cannot be taken for granted.

3.5 Data-Link Layer

- The data link layer is the protocol layer in a program that handles the moving of data into and out of a physical link in a network. The data link layer is Layer 2 in the Open Systems Interconnection (OSI) architecture model for a set of telecommunication protocols. Data bits are encoded, decoded and organized in the data link layer, before they are transported

as frames between two adjacent nodes on the same LAN or WAN. The data link layer also determines how devices recover from collisions that may occur when nodes attempt to send frames at the same time.

- The data link layer is the protocol layer in a program that handles the moving of data into and out of a physical link in a network. The data link layer is Layer 2 in the Open Systems Interconnection (OSI) architecture model for a set of telecommunication protocols. Data bits are encoded, decoded and organized in the data link layer, before they are transported as frames between two adjacent nodes on the same LAN or WAN. The data link layer also determines how devices recover from collisions that may occur when nodes attempt to send frames at the same time.

Q. 3.5.1 How to Prepare your WLAN for the 802.11ax Standard ? (Ref. Sec. 3.5) (5 Marks)

- Currently planned for release in 2019, the 802.11ax standard offers 10 Gbps speeds –up to 40% faster than Wave 2 802.11ac. Find out how this will be a game changer, and why anyone with skin in the game should start educating themselves now.
- The data link layer has two sublayers : the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer.
- As described by the IEEE-802 LAN specification, the role of the LLC sublayer is to control data flow among various applications and services, as well as provide acknowledgement and error notification mechanisms. The LLC sublayer can then talk to a number of IEEE 802 MAC sublayers, which control access to the physical media for transport. It is also responsible for the physical addressing of frames. Two common MAC layer types include Ethernet and 802.11 wireless specifications.

Syllabus Topics : Data- Link Layer Wireless Security Features

3.5.1 Data-Link Layer Features

Q. 3.5.2 Give features of data link layer. (Ref. Sec. 3.5.1) (5 Marks)

The data link layer has three main functions :

1. It handles problems that occur as a result of bit transmission errors.
2. It ensures data flows at a pace that doesn't overwhelm sending and receiving devices.
3. It permits the transmission of data to Layer 3, the network layer, where it is addressed and routed.

Syllabus Topics : Data- Link Layer Wireless Security Flaws

3.5.2 Data-Link Layer Flaws

Q. 3.5.3 Explain flaws of data link layer. (Ref. Sec. 3.5.2) (5 Marks)

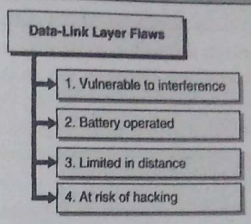


Fig. 3.5.1 : Data-Link Layer Flaws

➜ **1. Vulnerable to interference**

Though very uncommon, wireless security systems are susceptible to interference—just like Wi-Fi randomly disconnects or cellphones can't find signals. Whether the interference is electromagnetic through remote controls or power lines, or structural through walls or metal filing cabinets, there are several things can cause a sensor's radio frequency communication to fail.

➜ **2. Battery operated**

Wireless systems often run on batteries, so you must periodically check the battery life of the sensors and devices.

➜ **3. Limited in distance**

Wireless system devices have sensor limitations, so they're best for small- to medium-sized homes. Their open-air range is generally up to 500 feet.

➜ **4. At risk of hacking**

Burglars can hack into wireless security systems, jamming the signals so the alarm won't set off. Carefully review the security of the wireless system you want to purchase. Some wireless systems fail to encrypt or authenticate signals sent from the access point sensors - like on windows - to the main control panel. If you use a wireless system, enable encryption on your router and protect your Wi-Fi with a strong password.

Syllabus Topics : Threats

3.5.3 Network Security : Common Threats

Q. 3.5.4 What are the threats of data link layer. Explain in detail. (5 Marks)
(Ref. Sec. 3.5.3)

- It will be good if the networks are built and managed by understanding everything. The problem is that there are users who are familiar and who stole the data, embarrass the company and will confuse everything. It needs little effort to fight against with the threats on the computers and networks. The vulnerability will make the threat as reality and helps to mitigate that threats are discussed below. It includes wireless network security, threats and mitigation techniques which helps perform better.
- Nowadays, due to its popularity and wide range of advantage the wireless plays important role everywhere from large organizations to individual personal use computer and networks. Here listed below are some of the threats which are specific to the wireless networks to recognize and to mitigate the threats.

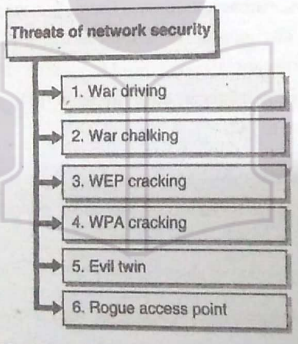


Fig. 3.5.2 : Threats of network security

1. War driving

The war driving is an act of searching for the wireless network in the moving vehicles with the help of the PDA or portable computer. It introduce with the earliest of the wireless network because it was more popular among many organizations are also setting this wireless network that they really did not know to secure it. To keep the wireless network more secure, implement the measures which needed for the wireless network.

2. War chalking

In the year 2002, a group of people developed the series of symbol which indicates that a network was nearby as well as whether it was unsecure, secure, protected by the WEP. They marked the symbols onto the street sign or wall to indicate the network location. This method has gone away and the people started using Wi-Fi when it need and various cell phones are looking for it.

3. WEP cracking

The wireless network, which is protected by the WEP is not secure as per today's technology. All the attackers have to determine a WEP key and it can be done in a fraction of a second. Once the attacker determined the key, then he can get into the system and also monitor the traffic or can take the administrator's role and change the settings.

4. WPA cracking

The WPA is the one which uses the security mechanism is known as temporal key integrity protocol. There are ways that the experienced and determined attacker can also decrypt the incoming traffic to the computers using WPA with the TKIP. It is not a secure option anymore and make use of the WPA2 with the AES for the secure network.

5. Evil twin

- An evil twin is the bogus type Wi-Fi connection which fools users that believing that it is the legitimate connections to phishing attacks as well as exploitation of the data transaction purposes. These kinds of attacks are more common, it is necessary to aware of it and guard against it. It will affect it professionally and personally.
- Protect computer or network against the evil twin attacks by learning about such attacks. Make use of the VPN with TLS or SSL to ensure that the all passwords, emails and all sensitive information are encrypted while transmission. It is better to avoid sending highly sensitive and important information through wireless networks, which is not 100 % safe.

6. Rogue access point

- The rogue access point is the wireless access point which installed without explicit permission of a network administration team. It creates the potential for the man in the middle attack where the security of a network has breached.
- To avoid the installation of the rogue access points, monitors the network for the newly installed access point with the help of wireless intrusion prevention system that will detect changes in a radio spectrum which indicate the new access point is operational and

installed. Most of these systems will take automatic countermeasures by identifying a rogue and redirecting the traffic away from that.

Syllabus Topics : Mitigation

3.5.4 Mitigation Techniques

Q. 3.5.5 Write short note on mitigation techniques. (Ref. Sec. 3.5.4) **(5 Marks)**

Take a deep look to protect against the threats. The mitigate techniques and methods are mainly depends upon the type of threats. Listed below are some of the mitigation techniques:

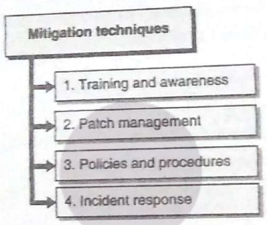


Fig. 3.5.3 : Mitigation techniques

➜ **1. Training and awareness**

It is considered as the most convenient and comfortable form of security. User training is considered as the least expensive and most effective mitigation techniques. It is the best way to keep the users from making mistakes that will lead to a success of the social engineering attack is educating how to handle them. It is important to know the procedures, protocols and policies for the security of a network. Or else training users give a real advantage of the relatively low cost.

➜ **2. Patch management**

- When an application or an operating system is released, it is not perfect from the security perspective. Then after the release, updates and security patches are released on the ongoing basis, which can add to a software to make them more secure or provide it more functionality.
- The windows update systems which are installed in the latest servers and clients can be configured to install as well as download the patches automatically from the site. The

windows server update services to download the patches to servers and then test it before applying to the bulk of the clients on the network.

➜ **3. Policies and procedures**

The security procedures and policies must be outlined clearly in writing in the organization. It should define acceptable behaviors on networks and organization computers. Who uses the computers has to read the procedures and policies and also sign the form for agreeing it.

➜ **4. Incident response**

- When the intruder has enacted an attack on the network, then the first instinct gets the user back to work regardless of what that takes. It makes a more sense in the short run, but in case of long run it might be a wrong move. The reinstall software which is damaged by the attack, then this re-installation may cover the track of an attacker and prevent it from prosecuting and finding it.
- It is essential to understand the security threats which affect the networks. And be familiar with the affecting networks like DoS attacks, worms, viruses, smurf, social engineering and man in the middle attacks. It is necessary to learn each type of these attacks operates and how to secure it.
- Additionally, understand the mitigation techniques such as incident response, procedure and policies, patch management and training and awareness.
- Understand efficient and effective method of protecting against the social engineering threats and also other network weaknesses. Understand the security patches must be used to update the applications and operating systems.

3.5.6 WLAN security

- First-generation wireless networking placed you between a rock and a hard place. Should you cave in and deploy a WLAN, despite well-documented protocol vulnerabilities and rampant threats? Or should you try to ban wireless, despite its business advantages and the unnerving suspicion that rogue access points (APs) will crop up anyway?
- It's no longer a no-win, either/or choice. Recent improvements in wireless protocols and infrastructure technologies make "WLAN security" a realistic goal, not a laughable oxymoron.
- "We've been forced to take [wireless] security more seriously than a lot of campuses have," says Col. Donald Welch, associate dean for information and education technology

at the U.S. Military Academy at West Point. The academy recently installed a WLAN security suite and plans to offer campus-wide wireless connectivity by fall.

- As West Point and thousands of other organizations are now discovering, WLANs can be made secure if you're smart about how you integrate wireless with your wired enterprise, leverage your existing security tools and select the right security technologies--from basic 802.11 security to VPNs to solutions based on the new generation of wireless authentication/encryption protocols. As with any technology, the trick then is to monitor your network's health to keep it safe.

Syllabus Topics : Wireless Vulnerabilities

3.5.7 Threats and Vulnerabilities

Q. 3.5.6 Explain in brief vulnerabilities. (Ref. Sec. 3.5.7) (5 Marks)

- The perils awaiting unprotected WLANs are many. Wireless traffic is easily recorded. Passive eavesdroppers can gather proprietary information, logins, passwords, intranet server addresses, and valid network and station addresses. Intruders can steal Internet bandwidth, transmit spam, or use your network as a springboard to attack others.
- They can capture and modify traffic to masquerade as you, with financial or legal consequences. Even a low-tech attacker can disrupt your business by launching wireless packet floods against your APs, nearby servers, next-hop wired network or Internet uplink.
- Fortunately, these risks are not yet heavily exploited. Jupiter Media Research recently reported that 26 percent of surveyed businesses had experienced at least one type of WLAN attack in the past year.
- However, most of these incidents were problems waiting to happen: rogue APs, stations associating with the wrong AP and war driving. Serious security breaches--like wired network intrusion, theft of confidential data and forgery--were far less common, according to the survey.
- In short, early adopters have been lucky. The cost of downtime and cleanup can be an order of magnitude greater than the cost of prevention. Now is the time to start playing catch-up with WLAN security.

3.5.7.1 Steps to Securing Wireless Networks

- If you don't know what you're defending and why, your security measures are just shots in the dark. It's critical to identify business assets that must be protected and the impact of damage, theft or loss.
- For wireless network security, as with dial-up and DSL, your policy management should define access requirements. Who needs access to what and when? If your company already has a remote access policy for travelers and telecommuters, expand it to incorporate wireless.
- If you have no such policy, create one. Remember to include scenarios that are unique to wireless, like employees at public hot spots (see "Hot Spots Give Security Managers the Chills") or office visitors.
- Consider how wireless changes the rules for office visitors. Few companies offer Ethernet access to visiting customers or business partners. Jacks in public areas are typically disabled or latched to known addresses. But wireless laptops and mobile devices can easily associate with nearby APs or other wireless stations.
- This is both a threat and an opportunity. Security policies should define rules for "walled garden" guest access. For example, you may prohibit peer-to-peer networking while permitting logged guest sessions through specific APs with limited destinations, protocols, duration and bandwidth. If guest access is banned, your policy must state this so that steps can be taken to prevent visitor intrusion.
- Once assets have been identified, enumerate threats and quantify risks. Security is always a balancing act, weighing risk against cost. After this foundation has been established, you can begin to consider WLAN implementation alternatives.

3.5.7.2 Taking Stock

- Before you plot out access point deployment, conduct a site survey using a WLAN discovery tool such as NetStumbler. What you learn might surprise you.
- According to a recent Gartner report, at least one in five companies find APs deployed without IT department permission. Commodity pricing, retail distribution and setup wizards have made it trivial for employees to install rogue APs, which can expose corporate assets to outsiders and interfere with WLAN performance. Find and eliminate rogue APs from the start--or safely incorporate them into your wireless network design.

- Site surveys also turn up unauthorized workstations. Create an inventory of laptops and mobile devices with wireless adapters, documenting user, MAC address and operating system. This will be used to implement WLAN access controls. And you'll find an up-to-date list is essential when WLAN adapters are lost or stolen.
- You may find nearby APs and stations that don't belong to you. Survey public areas (parking lots, hallways, lobbies) just beyond the physical boundaries of your facility, including upstairs and downstairs. Neighboring MAC addresses should be recorded, along with network name (SSID) and channel. This list will be used to avoid cross-channel interference and eliminate false-positive intrusion alerts.
- Consider getting APs with high-grade antennas that produce strong yet tight signals. These provide focused connectivity for your users. At the same time, their narrow focus means the signals are less likely to spill out into the street, where a war driver can capture and exploit it.

Syllabus Topics : Wireless Network Hardening Practices and Recommendations

3.6 Hardening

Q. 3.6.1 Why harden your wireless network? (Ref. Sec. 3.6) (5 Marks)

- In a perfect world you wouldn't need to secure your network because everybody would mind their own business. Unfortunately, we leave in second best world where everyone seem to have something fishy up their sleeves and trust does not come that easily. Ideally, we secure our wireless networks to keep off disgusting freeloaders who use up our bandwidth and slow down internet speeds, all for free.
- More importantly, hardening your wireless network secures your personal information and exempts you from numerous online scams. Lastly, a well-fortified home wireless network secures you from identity theft crimes. You probably are familiar with case of Kostolnik, where his new neighbor Aldorf hacked his WEP encrypted Wi-Fi, uploaded child pornography and sent threatening emails to top politicians included Vice President of US all in the name of Kostolnik.
- Although there is nothing like a 100% secure web, applying the following few tips will go a long way in hardening your home wireless network against potential attacks.

☞ **Tips to enhance your home/work wireless network security**

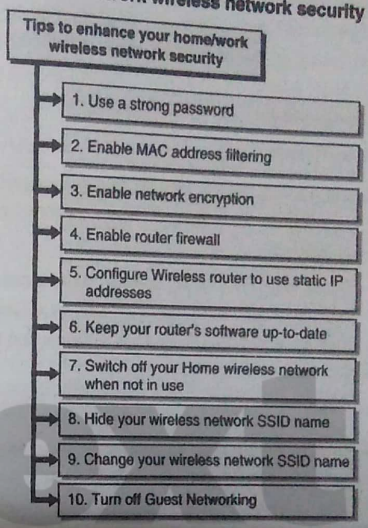


Fig. 3.5.4 : Tips to enhance your home/work wireless network security

➜ **1. Use a strong password**

- It is hard to emphasize the importance of a strong password in all your accounts. Using 654321 or a pet name as your Wi-Fi's password is as good as locking your house - and putting the keys under a flower pot next to your door. Hackers are aggressive people and will do anything to crack your password, so don't make it easy for them.
- For a strong password, use a combination of letters, numbers, and symbol and special characters. Never use a password that is associated with you or your family. Passwords which are based on special events such as anniversaries or Birthdays are as easy to crack as using the word 'password' as your password.

➜ **2. Enable MAC address filtering**

- Normally, your Wi-Fi router keeps a record of the Media Access Control (MAC) Addresses of all devices connected to it. The MAC address or physical address uniquely identifies each internet connecting devices such as Laptops, iPad, Xbox360 etc.

- To secure your wireless network, create a list of the Mac addresses of all your devices and set the router to filter connections based on the list. Devices not on the list are automatically denied access to the network regardless whether the intruder has a legit password or not. The MAC Address of your device can be found in a label affixed to it, or simply, read the addresses when all your devices are logged on.

➜ **3. Enable network encryption**

- A strong encryption will beat any hacker anytime. The two encryption protocols used in wireless network are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) security protocols.
- To break into your wireless network, a hacker need to find and exploit any vulnerabilities in WEP or WP2. WEP protected Wi-Fi are generally weak and easy to crack. On contrary, Wi-Fi protected Access (WPA1/2) protocol is strong and the best encryption to use in your wireless networks.

➜ **4. Enable router firewall**

- Having a personal firewall for all your devices is an easy way to block unwanted incoming and outgoing connections. A good firewall will notify you when someone tries to connect to your wireless network.
- All major operating systems come with pre-installed firewall, all you need is to activate it. Most wireless routers also have a firewall feature. Go to your router's setting and activate the firewall.

➜ **5. Configure Wireless router to use static IP addresses**

- Most internet providers use DHCP technology to generate a new IP address for your device every time you connect to the internet. While these dynamic IP addresses may have numerous advantage they also have some setbacks that could give the attacker a undeserving edge.
- For instance, an attacker could get a valid IP address from your router's DHCP pool making it easy for him to attack your network. We recommend configuring your router to use a fixed IP address for your devices. Your chosen static IP address should be within the Standard private IP address range e.g. 172.16.0.0 through 172.31.255.255.

➜ **6. Keep your router's software up-to-date**

- Proverbially, old is gold but in the IT world or in matters to do with network security. Outdated software have numerous vulnerabilities that could be exploited by attackers to

gain access into your network. Worse still, most outdated software are out of commercial support implying their developers no longer release patches for new security holes.

- To be on the safe side, ensure your wireless router is running on the latest software by having a firmware upgrade from time to time. Check for new firmware releases on your software's developer websites.

➜ **7. Switch off your Home wireless network when not in use**

Switching off your router during extended hours of non-use gives you several advantages. First it reduces the attackers contact hours with your wireless network which reduces the possibility of being hacked. Secondly, it cuts on power bills and reduces the chances of damaging your network gear due to power surges or overheating.

➜ **8. Hide your wireless network SSID name**

- This is simply preventing your wireless network from broadcasting into the neighborhood. The fact that your Wi-Fi appears on your neighbours "available networks list" is enough motivation for them to hack it especially when their Wi-Fi is down.
- Hiding your SSID is not itself a security measure because hackers can still detect it using one of the many wireless hacking tool we discussed in our previous article.

➜ **9. Change your wireless network SSID name**

- Normally, your wireless router is shipped using a default SSID name and password. The default name could be something like the manufacturer name such as Cisco or Netgear. While there may be no harm in using the default name, it could give the hacker important leads such as your router's manufacturer.
- Changing your router's SSID name and password to something unique denies the hacker any clue about your router. It also makes it easy for you to identify your Wi-Fi in a list of many networks using the same SSID name. As a rule of thumbs, never use an SSID name that could be identified with you or your family.

➜ **10. Turn off Guest Networking**

- If you are not careful, some wireless routers have the Guest access feature enabled by default. This allows anyone to access your wireless network without requiring a security key. Enabling guest access could be a good thing for a coffee shop but dangerous for a home or office wireless network.
- To stay safe, go to your router setting and turn off the Guest access option (if you find it). Alternatively, set a strong password for guest access to be used only by your guests.

Syllabus Topics : Wireless Intrusion Detection and Prevention

3.7 Wireless Intrusion Detection and Prevention System

3.7.1 WIDS (Wireless Intrusion Detection System)

Q. 3.7.1 Write a short note on Wireless Intrusion Detection System (WIDS). (Ref. Sec. 3.7.1) **(5 Marks)**

- WIDS is actually a broader concept than catching break-in attempts. It also includes verifying the access points that are on the network, identifying any that shouldn't be there or have security issues, and detecting attacks on APs/clients.
- A well-run network has an inventory of all authorized devices. This lets a network scan and identify any rogue devices. "Rogue" here means simply that the device wasn't approved, not necessarily that it's hostile. Network sniffing tools will probe all IP addresses and identify authorized and unauthorized ones.
- Network monitoring over TCP/IP doesn't always reveal which devices have Wi-Fi capability, and it won't catch relays that aren't directly on the network, so over-the-air sniffing is necessary as well. Such sniffing will identify any APs within range and check if they have weak security.
- Then we come to intrusion detection in the narrower sense. Intrusion attempts include password guessing, WPS breach attempts, and packet flooding. Detection methods are like the ones used in standard intrusion detection systems, except that they operate at all network layers from 1 (physical) up and include the special risks of wireless access. Regular intrusion detection operates on Layer 3 and higher.
- Fingerprinting in a more sophisticated WIDS can be done at multiple layers. For example, at the physical/MAC layer it make sure the modulation scheme is standards-compliant and not trying to exploit idiosyncrasies in chipsets. In addition, it can perform fine-grained analysis and comparison of capabilities advertised by an AP that a user commonly has no view into.

3.7.2 WIPS (Wireless Intrusion Prevention System)

Q. 3.7.2 Write a short note on Wireless Intrusion Prevention System (WIPS). (Ref. Sec. 3.7.2) **(5 Marks)**

- A Wireless Intrusion Prevention System (WIPS) is a dedicated security device or integrated software application that monitors a wireless LAN network's radio spectrum for rogue access points and other wireless threats.
- A WIPS compares the MAC addresses of all wireless access points on a network against the known signatures of pre-authorized, known wireless access points and alerts an administrator when a discrepancy is found. To circumvent MAC address spoofing, some higher-end WIPS are able to analyze the unique radio frequency signatures that wireless devices generate and block unknown radio fingerprints.
- The PCI Security Standards Council recommends the use of WIPS to automate wireless network scanning. In addition to providing a layer of security for wireless LANS, WIPS are also useful for monitoring network performance and discovering access points with configuration errors.
- There are three basic ways to deploy a WIPS. The first, primarily found at the lower-end of the market, is known as time slicing or time sharing. In this type of deployment, the wireless access point does double duty, providing network traffic with wireless connectivity while periodically scanning for rogue access points.
- In the second approach, which is known as integrated WIPS, a sensor that is built into the authorized access point continually scans radio frequencies, looking for unauthorized access points.
- In the third approach, which is known as WIPS overlay, sensors are deployed throughout a building to monitor radio frequencies. The sensors forward the data they collect to a centralized server for further analysis, action and log archiving. This approach is more expensive because it requires dedicated hardware, but it is also thought to be most effective.
- WIPS overlay hardware resembles a rack server and the associated sensors resemble Wi-Fi access points. Most WIPS overlay systems share the same fundamental components:
  - **Sensors :** monitor the radio spectrum and forward logs back to a central management server.
  - **Management server :** receives information captured by the sensors and take appropriate defense actions based on this information.
  - **Database server :** stores and organizes the information captured by the sensors.
  - **Console :** provides an interface for administrators to set up and manage the WIPS.

3.8 Exam Pack (Review Questions)

Syllabus Topic : Secure Network Design, Introduction to Secure Network Design

Q. 1 Explain secure network design with its various aspects. (Refer Sections 3.1, 3.1.1, 3.1.2) **(5 Marks)**

Syllabus Topic : Availability

Q. 2 Explain network availability. (Refer Section 3.1.3) **(5 Marks)**

Syllabus Topic : Security

Q. 3 Explain network security. (Refer Section 3.1.4) **(5 Marks)**

Q. 4 Explain internal security practice in detail. Hence explain extranet, intranet, DMZ. (Refer Sections 3.1.4.3, 3.1.4.4) **(5 Marks)**

Syllabus Topic : Network Device Security

Q. 5 Explain network device security with respect to router and switches. (Refer Section 3.2) **(5 Marks)**

Syllabus Topic : Switch and Router Basics

Q. 6 Explain security aspects in TCP/IP protocol suite and OSI model. (Refer Section 3.2.1.2) **(5 Marks)**

Syllabus Topic : Network Hardening

Q. 7 Explain network hardening in detail. (Refer Sections 3.2.2, 3.2.2.1, 3.2.2.2, 3.2.2.3, 3.2.2.4, 3.2.2.5) **(5 Marks)**

Q. 8 Explain security related to ICMP. (Refer Section 3.2.2.6) **(5 Marks)**

Q. 9 Explain security related to antispoofing. (Refer Section 3.2.2.7) **(5 Marks)**

Q. 10 Explain security related to logging. (Refer Section 3.2.2.8) **(5 Marks)**

Q. 11 Describe about firewalls. (Refer Section 3.3) **(5 Marks)**

Syllabus Topic : Core Firewall Functions

Q. 12 Explain core firewall functions. (Refer Section 3.3.2) **(5 Marks)**

Syllabus Topic : Additional Firewall Capabilities

Q. 13 Discuss about some additional security feature of firewall. (Refer Section 3.3.3) **(5 Marks)**

Syllabus Topic : Firewall Design

Q. 14 Describe the firewall design for achieving security measures (Refer Section 3.3.4) **(5 Marks)**

Syllabus Topics : Radio Frequency Security Basics

Q. 15 Explain in brief radio frequency security. (Refer Section 3.4) **(5 Marks)**

Syllabus Topics : Data- Link Layer Wireless Security Features

Q. 16 Give features of data link layer. (Refer Section 3.5.1) **(5 Marks)**

Q. 17 How to prepare your WLAN for the 802.11ax standard ? (Refer Section 3.5) **(5 Marks)**

Syllabus Topics : Data- Link Layer Wireless Security Flaws

Q. 18 Explain flaws of data link layer. (Refer Section 3.5.2) **(5 Marks)**

Syllabus Topics : Threats

Q. 19 What are the threats of data link layer ? Explain in detail. (Refer Section 3.5.3) **(5 Marks)**

Syllabus Topics : Mitigation

Q. 20 Write short note on mitigation techniques. (Refer Section 3.5.4) **(5 Marks)**

Syllabus Topics : Wireless Vulnerabilities

Q. 21 Explain in brief vulnerabilities. (Refer Section 3.5.7) **(5 Marks)**

Syllabus Topics : Wireless Network Hardening Practices and Recommendations

Q. 22 Why harden your wireless network? (Refer Section 3.6) **(5 Marks)**

Syllabus Topics : Wireless Intrusion Detection and Prevention

Q. 23 Write a short note on Wireless Intrusion Detection System (WIDS). (Refer Section 3.7.1) **(5 Marks)**

Q. 24 Write a short note on Wireless Intrusion Prevention System (WIPS) . (Refer Section 3.7.2) **(5 Marks)**

Chapter Ends...

□□□