Chapter 3

common Network Devices: Routers , Switches and Firewalls

Outlines

4.1- Implement Secure Network Designs

Labs

Lab : Implementing a Secure Network Design

4.- Implement Secure Network Designs

4.1- Implement Secure Switching and Routing

4.2- Implement Secure Wireless Infrastructure

4.3- Implement Load Balancers

4.4- Network Troubleshooting

SECURE NETWORK DESIGNS

- A secure network design provisions the assets and services.
- Weaknesses in the network architecture make it more susceptible to undetected intrusions or to catastrophic service failures.
- Typical weaknesses include:
  - ✓ Single points of failure—a "pinch point" relying on a single hardware server or appliance or network channel.
  - ✓ Lack of documentation and change control—network segments, appliances, and services might be added without proper change control procedures, leading to a lack of visibility into how the network is constituted.
  - ✓ Overdependence on perimeter security—if the network architecture is "**flat**" (that is, if any host can contact any other host), penetrating the network edge gives the attacker freedom of movement.

NETWORK APPLIANCES

- A number of network appliances are involved in provisioning a network architecture:

  - ✓ Switches—forward frames between nodes in a cabled network, Switches work at **layer 2** of the OSI model and make forwarding decisions based on the hardware or Media Access Control (MAC) address of attached nodes, Switches can establish network segments that either map directly to the underlying cabling or to logical segments, created in the switch configuration as virtual LANs (**VLANs**).

  - ✓ Wireless access points—provide a bridge between a cabled network and wireless clients, or stations, Access points work at **layer 2** of the OSI model.

NETWORK APPLIANCES (cont.)

- A number of network appliances are involved in provisioning a network architecture (cont.)

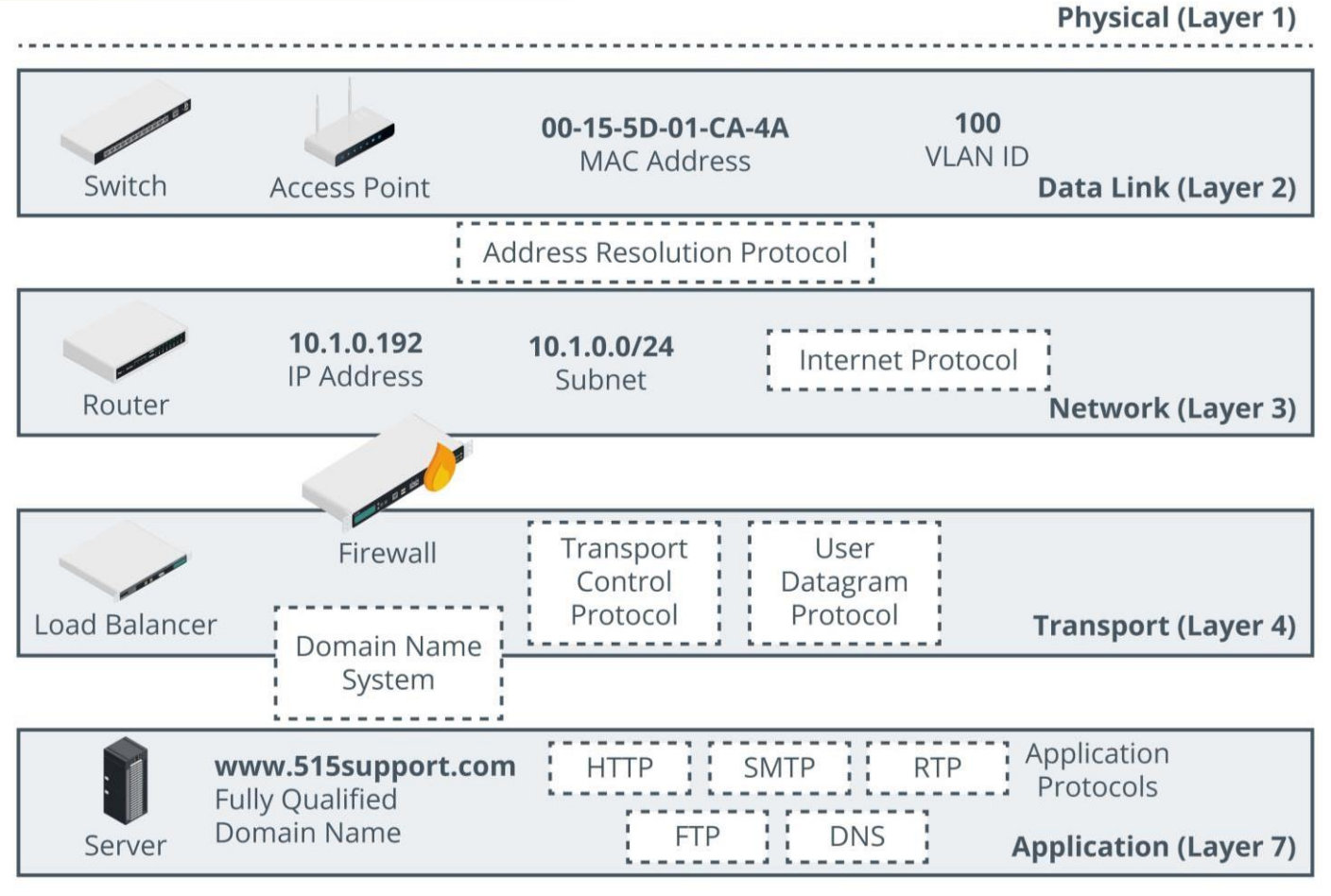
✓ Routers— forward packets around an internetwork, making forwarding decisions based on IP addresses, Routers work at layer 3 of the OSI model, Routers can apply logical IP subnet addresses to segments within a network.

✓ Firewalls— apply an access control list (ACL) to filter traffic passing in or out of a network

- segment, Firewalls can work at layer 3 of the OSI model or higher.

✓ Load balancers—distribute traffic between network segments or servers to optimize performance, Load balancers can work at layer 4 of the OSI model or higher.

NETWORK APPLIANCES (cont.)



ROUTING AND SWITCHING PROTOCOLS

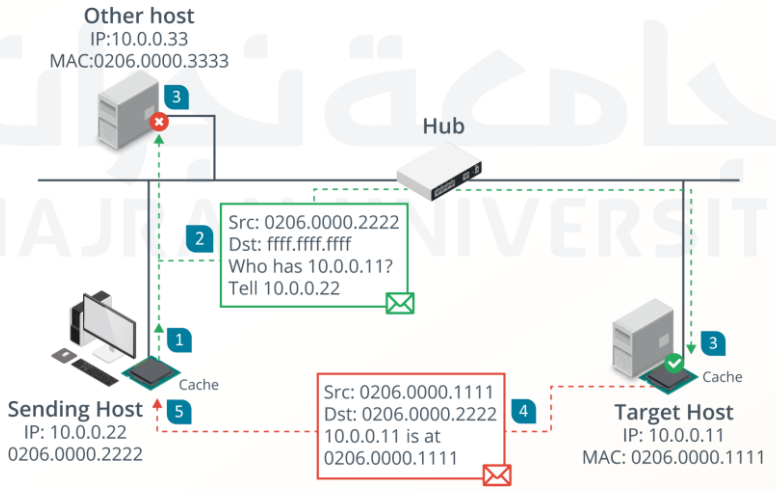
- The basic function of a network is to forward traffic from one node to another.
- A number of routing and switching protocols are used to implement forwarding.
- The forwarding function takes place at two different layers:
  - ✓ Layer 2 forwarding occurs between nodes on the same local network segment that are all in the same broadcast domain, At layer 2, a broadcast domain is either all the nodes connected to the same physical unmanaged switch, or all the nodes within a virtual LAN (VLAN) configured on one or more managed switches, At layer 2, each node is identified by the network interface's hardware or **Media Access Control (MAC) address**, A MAC address is a 48-bit value written in hexadecimal notation, such as 00-15-5D-F4-83-48.

ROUTING AND SWITCHING PROTOCOLS (cont.)

- The forwarding function takes place at two different layers (cont.)
  - Layer 3 forwarding, or routing, occurs between both logically and physically defined networks, A single network divided into multiple logical broadcast domains is said to be subnetted, Multiple networks joined by routers form an internetwork, At layer 3, nodes are identified by an Internet Protocol (IP) address. ✓

ROUTING AND SWITCHING PROTOCOLS (cont.)

- Address Resolution Protocol (ARP)
  - ✓ The Address Resolution Protocol (ARP) maps a network interface's hardware (MAC) address to an IP address.
  - ✓ Normally a device that needs to send a packet to an IP address but does not know the receiving device's MAC address broadcasts an ARP Request packet, and the device with the matching IP responds with an ARP Reply.



ROUTING AND SWITCHING PROTOCOLS (cont.)

- Internet Protocol (IP)
  - ✓ IP provides the addressing mechanism for logical networks and subnets.
  - ✓ A **32-bit IPv4** address is written in dotted decimal notation, with either a network suffix or subnet mask to divide the address into network ID and host ID portions.
  - ✓ For example, in the IP address **172.16.1.101/16**, the /16 suffix indicates that the first half of the address (172.16.0.0) is the network ID, while the remainder uniquely identifies a host on that network.
  - ✓ This /16 suffix can also be written as a subnet mask in the form **255.255.0.0.**
  - ✓ Networks also use **128-bit IPv6** addressing.
  - ✓ IPv6 addresses are written using hex notation in the general format: **2001:db8::abc:0:def0:1234**.
  - ✓ In IPv6, the last 64-bits are fixed as the host's interface ID. The first 64-bits contain network information in a set hierarchy.

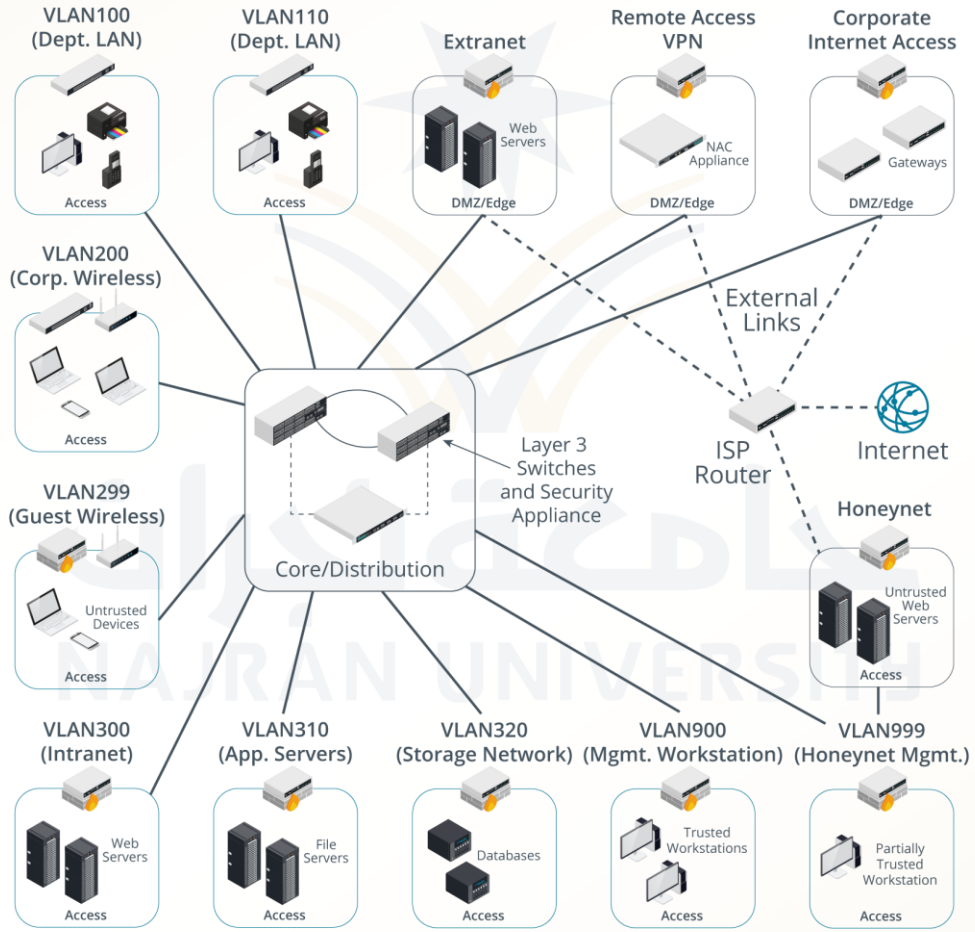
NETWORK TOPOLOGY AND ZONES

- A **topology** is a description of how a computer network is physically or logically organized.
- The logical and physical network topology should be analyzed to identify points of vulnerability and to ensure that the goals of confidentiality, integrity, and availability are met by the design.
- The main building block of a security topology is the **zone**.
- A **zone** is an area of the network where the security configuration is the same for all hosts within it.
- Traffic between zones should be strictly controlled using a security device, typically a firewall.

NETWORK TOPOLOGY AND ZONES (cont.)

- Dividing a campus network or data center into zones implies that each zone has a different security configuration.
- The main zones are as follows:
  - ✓ Intranet (private network)—this is a network of trusted hosts owned and controlled by the organization, Within the intranet, there may be sub-zones for different host groups, such as servers, employee workstations, VoIP handsets, and management workstations.
  - ✓ Extranet—this is a network of semi-trusted hosts, typically representing business partners,
    - suppliers, or customers, Hosts must authenticate to join the extranet.
  - ✓ Internet/guest—this is a zone permitting anonymous access (or perhaps a mix of anonymous and authenticated access) by untrusted hosts over the Internet.

NETWORK TOPOLOGY AND ZONES (cont.)

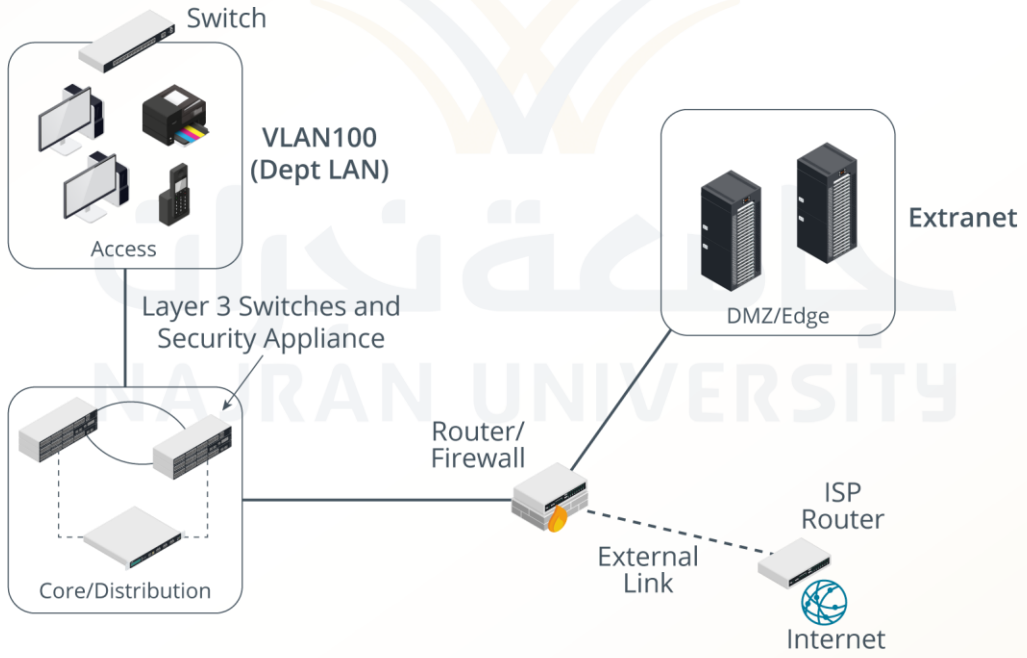


DEMILITARIZED ZONES (DMZ)

- A **DMZ** is also referred to as a perimeter or edge network.
- The basic principle of a DMZ is that traffic cannot pass directly through it.
- A **DMZ** enables external clients to access data on private systems, such as web servers, without compromising the security of the internal network as a whole.
- If communication is required between hosts on either side of a DMZ, a host within the DMZ acts as a **proxy**.
- For example, if an intranet host requests a connection with a web server on the Internet, a proxy in the DMZ takes the request and checks it.
- If the request is valid, it retransmits it to the destination.
- External hosts have no idea about what (if anything) is behind the DMZ.

DEMILITARIZED ZONES (DMZ) (cont.)

- A **DMZ** can be established using one **router/firewall** appliance with three network interfaces.
- One interface is the public one, another is the DMZ, and the third connects to the
- LAN.



Network Troubleshooting
Understanding and Resolving Network Issues

Introduction to Network Troubleshooting Content:
Definition of network troubleshooting Importance of effective troubleshooting in network management Common network issues (e.g., connectivity problems, slow performance)
Visual: Image or graphic representing network problems (e.g., network diagram with issues highlighted)

Network Troubleshooting
Understanding and Resolving Network Issues

troubleshooting Methodology Content:
Step 1: Identify the problem
Step 2: Establish a theory of probable cause
Step 3: Test the theory
Step 4: Establish a plan of action
Step 5: Implement the solution
Step 6: Verify functionality
Step 7: Document findings

Network Troubleshooting
Understanding and Resolving Network Issues

Common Network Problems Content:

- Connection Issues (e.g., no connectivity, intermittent connectivity)
- Slow Network Performance
- Network Configuration Errors
- Hardware Failures

Network Troubleshooting
Understanding and Resolving Network Issues

Troubleshooting Tools Content:

- Ping: Check connectivity to a device
- Traceroute: Analyze the path data takes to reach a destination
- IP Configuration Tools: ipconfig (Windows) / ipconfig (Linux)Network Analyzers: Wireshark for monitoring network traffic

Using Ping and Traceroute Content:
Explanation of how to use the ping
command Syntax: ping [IP address or hostname]
Explanation of how to use the traceroute command
Syntax: tracert [IP address or hostname] (Windows) / traceroute [IP address or hostname] (Linux)What the results indicate

Network Troubleshooting
Understanding and Resolving Network Issues

Network Configuration Issues Content:

- Common configuration errors (e.g., incorrect IP addressing, subletting errors)
- Checking device configurations (routers, switches, firewalls)

Troubleshooting Slow Network Performance Content:

- Possible causes (e.g., bandwidth saturation, hardware limitations, interference)
- Steps to diagnose and address performance issues
- Visual: Graph showing bandwidth usage over time

What is the primary purpose of a firewall in a network design?
A) To improve network speed
B) To create a backup of data
C) To monitor and control incoming and outgoing network traffic
D) To provide wireless connectivity

Answer: C) To monitor and control incoming and outgoing network traffic

Which of the following is a best practice for implementing secure network designs?
A) Use default passwords on all devices
B) Segregate networks using VLANs
C) Allow all traffic through the firewall by default
D) Disable all security features for easier access
Answer: B) Segregate networks using VLANs

Which of the following security measures helps protect against unauthorized access to a network?
A) Regular software updates
B) Network segmentation
C) Both A and B
D) None of the above
Answer: C) Both A and B

What is a DMZ (Demilitarized Zone) in network design?

A) A network segment that is isolated from all other networks

B) A buffer zone between an internal network and the outside world, allowing access to certain services while protecting the internal network

C) A zone that contains all network devices with default settings

D) A zone dedicated solely to user access logs

Answer: B) A buffer zone between an internal network and the outside world, allowing access to certain services while protecting the internal network