Computer Networks

# Communications in a Connected World

## Network Types

### Local Networks

* Small home networks connect a few computers to eachother and to the internet
* SOHO networks allow computers in a home or remote office to connect to a corporate network
* Medium to large networks can have many locations with thousands of interconnected hosts

E.g.: schools, corporations

* ‘The Internet’ = a network of networks that connects hundreds of millions of computers world-wide

### Mobile devices

* Smart phones
* Tablets
* Smart watch
* Smart glasses

### Connected Home Devices

* Smart home devices
  + Security system
  + Climate control
  + Lighting
  + …
* Household appliances
  + Refrigerators
  + Ovens
  + Dishwashers
* Smart TV
* Gaming consoles

### Other Connected Devices

* Smart cars
  + Can connect to internet:
    - Maps
    - Audio
    - Video
    - Info about destination
* Connected sensors
  + Temperature, humidity, …
* Medical devices
  + Pacemakers, insulin pumps, …

## Data Transmission

### Types of Personal Data

* Volunteered data
  + Created and explicitly shared by individuals
    - Video files, pictures, text, audio,…
    - E.g.: social network profiles
* Observed data
  + Captured by recording the actions of individuals
    - E.g.: location data using cell phones
* Inferred data
  + Based on analysis of volunteered or observed data
    - E.g.: credit score

### The Bit

* Bit = Binary Digit
* Each bit: 2 values
  + 0 or 1
* 8 bits = byte
  + ASCII: Each character = 1 byte = 8 bits
    - E.g.: A = 01000001

9 = 00111001

# = 00100011

### Common Methods of Data Transmission

* Electrical signals
  + Transmission achieved by representing data as electrical pulses on copper wire
* Optical signals
  + Transmission achieved by converting electrical signals into light pulses
* Wireless signals
  + Transmission achieved by using infrared, microwave, or radio waves through the air

## Bandwidth an Throughput

### Bandwidth

* The capacity of a medium o carry data
* Digital bandwidth measures the amount of data that CAN flow from one place to another in a given amount of time
* Measured in number of bits/s

Background pattern

Description automatically generated

### Throughput

* Throughput measures the amount of data that ACTUALLY flows from one place to another in a given amount of time
* Due to a number of factors: throughput ≠ bandwidth
  + Amount of data being sent and received
  + Type of data being transmitted
  + Latency created by number of network devices between source and destination
* Latency: the amount of time, including delays, for data to travel from one point to another

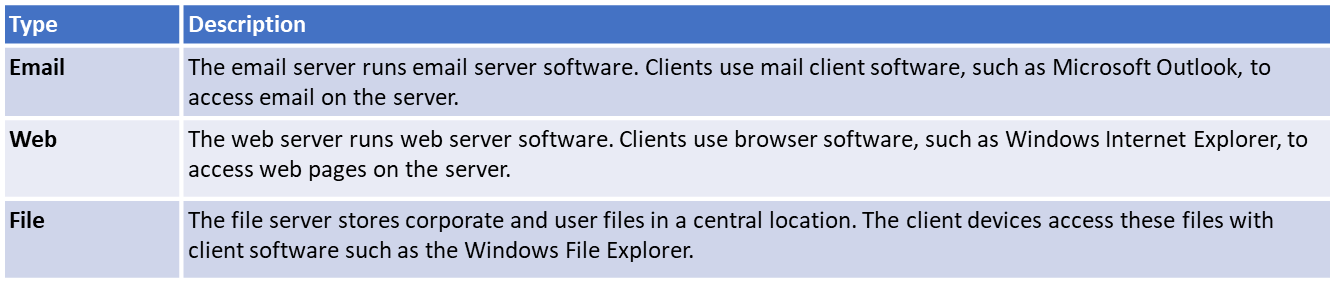
## Clients and Servers

### Clients and Server Roles

* Clients are computer hosts that have software installed that enables the hosts to request and display information obtained from the server
* Servers are hosts that have software installed which enable them to provide information, like email or web pages, to other hosts on the network

Icon

Description automatically generated



### Peer-to-Peer Networks

* In small businesses and homes, many computers function as the servers and clients on the network
  + = P2P network
  + Simplest P2P: consist of 2 directly connected computers
* Advantages
  + Easy to set up
  + Less complex than other networks
  + Lower cost because network devices
  + Can be used for simple tasks such as transferring files and sharing printers
* Disadvantages
  + No central administration
  + Not as secure
  + Not scalable
  + All devices may act as both client and server which can slow performance

### Peer-to-Peer Applications

* A P2P application allows a device to act as both client an server within the same communication
* Diagram

  Description automatically generatedEach end device must provide a user interface and run a background service

### Multiple Roles in the Network

* A computer with server software can provide services to one or many clients simultaneously
* Single computer can run multiple types of server software
  + E.g.: file server, web server, email server

## Network components

### Network infrastructure

* The network infrastructure contains 3 categories of hardware components
  + End devices
  + Intermediate devices
  + Network media

Graphical user interface, application

Description automatically generated

### End devices

* = Hosts
* Form an interface between users and underlying communication network
* E.g.:
  + Computers
  + Network printers
  + Telephones
  + Security cameras
  + Mobile devices

# Online Connections

## Wireless Networks

### Mobile Telephones

* Most mobile phones can be connected to many different types of networks simultaneously
* Use radio waves to transmit voice signals to antennas
* = cell phones (geographical area with individual antenna = cell)

### Cell Phone Network

* 3G, 4G, 4G-LTE, 5G = enhanced cell phone networks optimized for fast data transmission
  + “G” = generation

### Other Wireless Networks

* GPS
* Wi-Fi
* Bluetooth
* NFC (Near Field Communications)

## Local Network Connections

### LAN Components

* Many components ca be part of a Local Area Network (LAN)
  + E.g.: PC’s, servers, networking devices, cabling, …
* 4 main categories
  + **Hosts**
    - Can send and receive user traffic
    - ‘Host’: generic name for most end-user devices
    - Has IP address
    - E.g.: PC’s, network attached printers
  + **Peripherals**
    - Do not communicate directly on the network
    - Rely on their connected host to perform all network operations
    - E.g.: cameras, scanners, locally attached printers
  + **Network devices**
    - Connect other devices, mainly hosts
    - Move and control network traffic
    - E.g.: hubs, switches, routers
  + **Network media**
    - Provides connection between hosts and network devices
    - Can be wired (fibreoptic, copper)
    - Can be wireless (Wi-Fi)

### End Device Addressing

* To be physically connected, end-user device needs:
  + Network Interface Card (NIC)
  + OS configuration to participate in network
* 3 parts to IP configuration
  + **IP address**
    - Identifies the host on the network
  + **Subnet Mask**
    - Identifies the network on which host is connected
  + **Default Gateway**
    - Identifies networking device the host uses to access a different network

### Manual and Automatic Address Assignment

* **Manual configuration**
  + Network administrator enters required values
  + IP address = static address (must be unique on the network)
* **Automatic configuration**
  + = Dynamic Host Configuration Protocol = DHCP

## Network Documentation

### Device Names and Address Planning

* Use of logical device naming simplifies network management + easier troubleshooting

### Network Topologies and Representations

* **Physical topology** shows where wiring is installed and locations of networking devices that connect to hosts
* **Logical Topology** shows relevant network config. Information

Diagram

Description automatically generatedDiagram

Description automatically generated

**Logical Topology**

**Physical Topology**

# Explore Networks with Packet Tracer

* Packet tracer niet te kennen (I think)

# Build a Simple Network

## Network media types

### Three Media Types

* Metal wires within cables
  + Data encoded into electrical pulses
* Glass or plastic within cables = fibreoptic
  + Data encoded into light pulses
* Wireless transmission
  + Data encoded via modulation of specific frequencies of electromagnetic waves

### Common Network Cables

* Twisted-Pair cable
  + Ethernet: generally twisted-pair
* Coaxial cable
  + One of the earliest network cabling types
  + High-freq. transmission line
* Fibre-Optic cable
  + Glass or plastic

## Ethernet Cabling

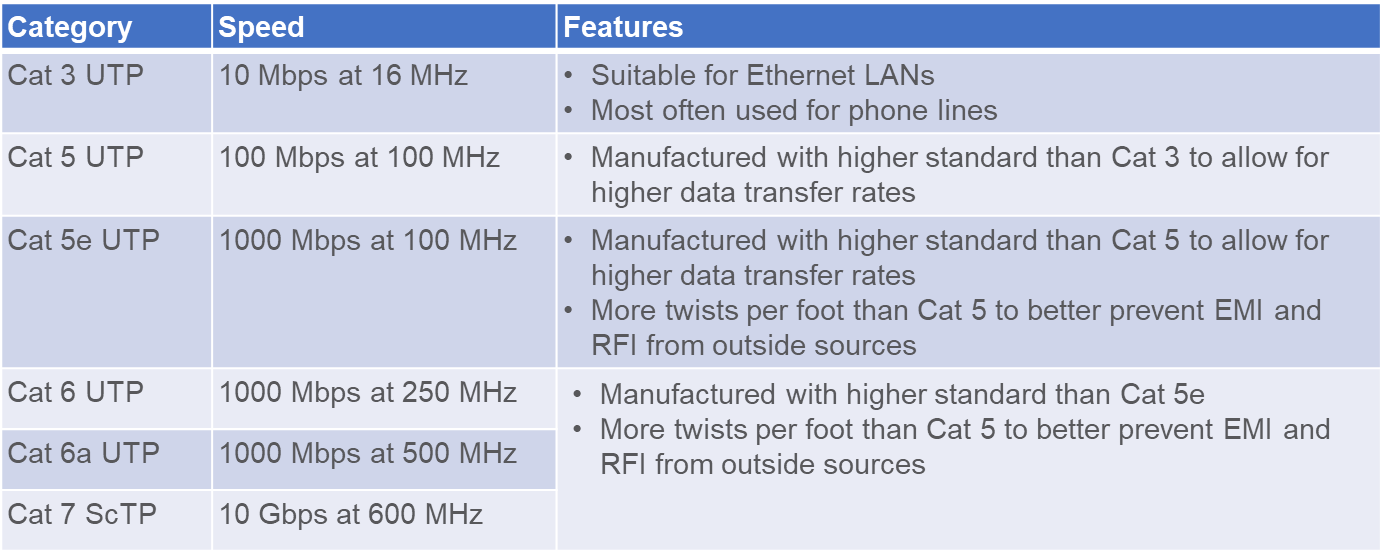
### Twisted-Pair Cables

* Networks in most homes and schools: twisted-pair
* Inexpensive, very widely available
* Ethernet patch cables = copper twisted-pair: twisted together, housed in protective jacket
* Pulses of electricity
* Sensitive to EMI (Electromagnetic Interference)
* Crosstalk: interference in cables that are bundles together for long lengths
* Interference can cause problems

1. Diagram

   Description automatically generatedPure digital signal is transmitted
2. Interference signal on medium
3. Digital signal is corrupted by interference signal
4. Receiving computer reads a changed signal

* 2 types of TP
  + UTP (unshielded)
    - Most common type in NA
    - 4 pairs of twisted cable
    - Each pair: colour
  + STP (shielded)
    - Almost exclusively in EU
    - Immune to EMI and RFI
    - Expensive, not as flexible
* Many diff. categories of UTP



## Coaxial and Fibre-Optic Cabling

### Cable TV and Satellite Cables

* Coax carries data in electrical signal form
  + Provides shielding
  + Can carry more data than UTP
  + Used by TV companies
  + Addition of cable modem: data, internet, tv and telephone over same cable
  + BNC or F-series connector
  + Outer jacket = insulator against EMI & RFI
  + Single centre conductor: Cu or Al
  + Metallic braid helps shielding

### Fibre-Optic Cables

* Light pulses
* Immune to EMI & RFI
* Different parts:
  + **Jacket:** typically PVC
  + **Strengthening material:** surrounds buffer, prevents stretching
  + **Buffer:** shields core and cladding from damage
  + **Cladding:** acts like a mirror, slightly diff. than core material
  + **Core:** light transmission element at centre of cable

## Twisted-Pair Operation

### TP Wiring Schemes

* Colour coding of wire in UTP: depends on standard
* Diff. standards = diff. purposes
  + 2 standards widely implemented (TIA/EIA organization)

Diagram

Description automatically generated with medium confidence

### TP Transmit and Receive Pairs

* Ethernet NIC’s and the ports on networking devices are designed to send data over UTP cables
* Specific pins on connector are associated with transmit or receive function
* Interfaces on each device are designated to transmit and receive data on designated wires within the cable
* When 2 unlike devices are directly connected
  + Important that transmit and receive function on each end of cable are reversed

Diagram

Description automatically generated

## Verify Connectivity

### Using Ping Command

* Host that sends message across internet must have IP address
* Ping utility can be used to test end-to-end connectivity between IP address of sending host and destination host
* Measures time it takes test message to make round trip
* If test message does not work; ping cannot determine where problem lies
* E.g.: ping 192.168.30.1 or ping [www.cisco.com](http://www.cisco.com)

### Traceroute Command

* Traceroute utility traces the route a message takes from source to destination
* Individual networks through which it travels = hops
* Displays each hop
* If problem occurs: can determine where message was lost or delayed
* tracert

# Communication Principles

## The Rules

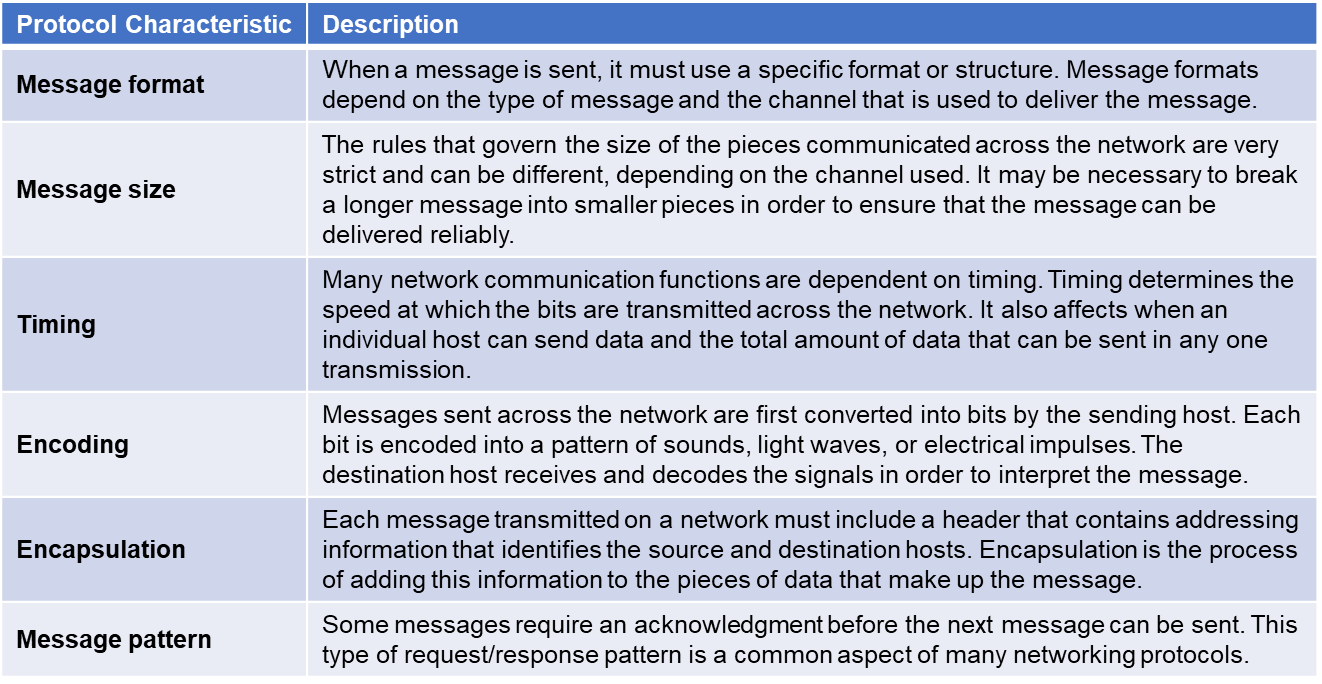
### The Three Elements

* The primary purpose of any network is to provide us with a method to communicate and share info
* All communication begins with a message that must be sent from one individual device to another
* All communication methods have three elements in common
  + **Source**: people or electronic devices that need to communicate a message to other individuals or devices
  + **Destination**: the destination receives and interprets the message
  + **Transmission medium**: provides the pathway over which the message can travel form source to destination

### Communication Protocols

* Protocols / Rules to follow for message to be successfully delivered and understood
  + Identified sender & receiver
  + Agreed upon method of communication
  + Common language and grammar
  + Speed and timing of delivery
  + Confirmation or acknowledgement requirements

### Why Protocols Matter



## Communication Standards

### The Internet and Standards

* A standard is a set of rules that determines how something must be done
* Networking and internet standards ensure that all devices connecting to the network implement the same set of rules or protocols in the same manner
* Using standards, it is possible for different types of devices to send information to each other over the internet
  + E.g.: the way in which an email is formatted, forwarded and received by all devices I done according to a standard:
    - If one person sends an email via a personal computer, another person can use a mobile phone to receive and read the email as long as the mobile phone uses the same standards as the personal computer

### Network Standards Organizations

* An internet standard is the end result of a comprehensive cycle of discussion, problem solving, and testing
* They’re developed, published and maintained by a variety of organisations
* When a new standard is proposed, each stage of the development and approval process is recorded in a number of Request for Comments (RFC) document
* Logo, company name

  Description automatically generatedOther organizations:

## Network Communication Models

### The Protocol Stack

* Successful communication between hosts requires interaction between a number of protocols
* The protocols are implemented in soft-/hardware installed on each host and networking device
* Chart

  Description automatically generatedInteraction between diff. protocols on a device can be illustrated as a protocol stack ↘
* A stack illustrates the protocols as a layered hierarchy with each

higher-level protocol depending on the services of the one below

* The separation of functions enables each layer to operate

independently of others

* **Hypertext Transfer Protocol (HTTP)**
  + Governs the way a web server and web client interact
  + HTTP defines the content and formatting of the requests and

responses that are exchanged between client and server

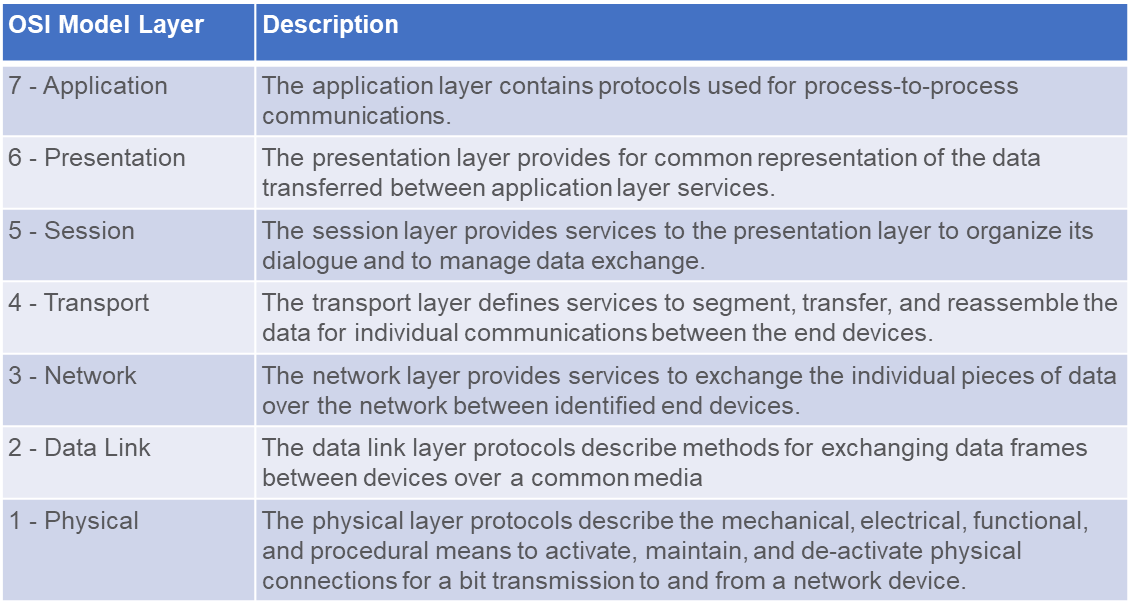
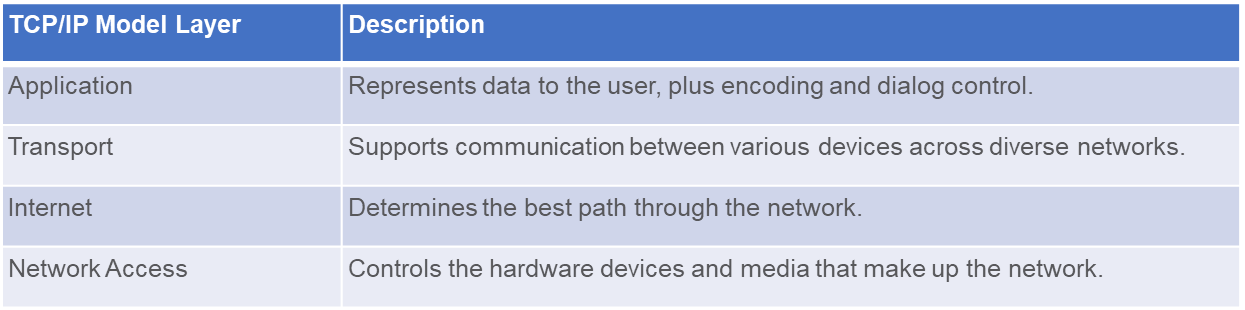
* **Transmission Control Protocol (TCP)**
  + Manages the individual conversations
  + Responsible for guaranteeing the reliable delivery of the information and managing flow control between end devices
* **Internet Protocol (IP)**
  + Responsible for delivering messages form the sender to the receiver
  + Used by routers to forward the messages across multiple networks
* **Ethernet**
  + Responsible for the delivery of messages form one NIC to another NIC on the same LAN

### The TCP/IP Model

* Layered model that depicts the operation of the protocols occurring within each layer, as well as the interaction with the layers above and below it

### The OSI Reference Model

|  |
| --- |
| Hybrid Model Layer |
| **Application**  E.g.:  - network aware applications  - email  - web browsers  - file transfer |
| **Transport**  E.g.:  - video and voice streaming  - firewall filtering lists |
| **Network**  E.g.:  - Ip addressing  - routing |
| **Data** **Link**  E.g.:  - NIC’s  - network switching  - WAN |
| **Physical**  E.g.:  - Physical medium  - hubs and repeaters |



Because the OSI model as well as the TCP/IP model are bullshit, we’ll be using the Hybrid Model Layer

## Ethernet

### The Rise of Ethernet

Graphical user interface

Description automatically generated with low confidence

* Each technology standard is assigned a number that refers to the committee that is responsible for approving and maintaining it
* The committee for Ethernet standards = 802.3
* Each version has an associated standard, e.g.: 802.3 100BASE-T
  + 100: speed in Mbps
  + BASE: baseband transmission
  + T: TP cabling standards

### The Ethernet MAC Address

* MAC address is the physical address of every Ethernet Network Interface
* In theory, it is unique worldwide
* 00-00-00-X0-X0-X0 or 00:00:00:X0:X0:X0
  + Can be split into the first and the last 3 couples (2 groups of 6 characters)
  + The first 3 bytes (6 characters or 3 couples) give away the manufacturer
* If 2 MAC addresses are the same = doesn’t work
* In reality, not all MAC addresses are unique
  + As long as they are not within the same subnet, there is no problem
* There is no central register with all MAC addresses
* Identifies each source and destination host on the network

# Network Design and the Access Layer

## Encapsulation and the Ethernet Frame

### Encapsulation

* Each message is encapsulated into a specific format (frame) that includes the source and destination
* For communication on an IP network, the format is very specific and includes a source and destination address

### Ethernet Frame

* On an ethernet network, messages are put into a frame or Layer protocol data units (PDU’s)

Application, table

Description automatically generated

## Hierarchical Network Design

### Physical and Logical Addresses

* Both a physical address and logical IP address are needed for a device to communicate on an Ethernet Network
  + Physical address = MAC address (friends in bar metaphor: national registration number)
    - Does not change
    - Burned into the NIC
  + Logical Address = IP address (friends bar metaphor: nickname)
    - Can change and is commonly assigned by network admin
    - Two parts: network and host

Diagram

Description automatically generated

### Benefits of Hierarchical Design

* A hierarchical, layered design provides:
  + Increased efficiency
  + Optimization of function
  + Increased speed
  + A way in which to scale the network without impacting the performance of existing ones
* Three Layers:
  + **Access layer**
    - Provides connections to hosts in local Ethernet network
  + **Distribution layer**
    - Interconnects smaller local networks
  + **Core layer**
    - Provides a high-speed connection between distribution layer devices

Diagram

Description automatically generated

## The Access Layer

### Access Layer Devices

* Provides access so hosts can join a network
* In wired network, each host connects to an access layer network device (such as a switch)

Diagram

Description automatically generatedDiagram

Description automatically generated

### Ethernet Hubs

* Only 1 message can be sent through simultaneously
* Hubs take signals from one port and sends the message out all of the other ports

### Diagram Description automatically generated Ethernet Switches

* An access layer device
  + Builds MAC address table
  + Uses that table to send the message to a specific port

### The MAC Address Table

* Switch builds MAC address table by examining a frame as

it comes into the switch

* Switch adds the source MAC address of the device connected

to the port through which the frame came in on

* Switch forwards frame out to specific port when destination

MAC address is in MAC address table

* Forwards a frame out to all hosts except source when destination MAC address isn’t in table

## Broadcast Containment

### Ethernet Broadcasts in the Local Network

* Broadcast message is used to contact every other device on the local network
* Ethernet broadcast is all 1s in the destination MAC address

### Broadcast domains

* Diagram, engineering drawing

  Description automatically generatedThe area through which a broadcast message can travel
* Each local Ethernet network is a broadcast domain
* Routers are used to divide the network into multiple broadcast domains

### Access Layer Communication

* In order to send info from a device on an Ethernet network
  + Must supply own source MAC and IP + destination MAC and IP
* ARP (Address Resolution Protocol) is used to discover MAC of device on

the same local network

### ARP

* Uses 3 steps to discover and store MAC of a host on local network when only IPv4 is known
  + Sending host creates and sends a frame addressed to a broadcast MAC
    - Contained within the frame is a message with the IPv4 of the destination host
  + Each host on the network receives the broadcast frame and compares the IPv4 to its own
    - The host with the matching IP will send its own MAC back to the original sending host
  + Sending host receives the message and stores the MAC and IPv4 in an ARP table

Diagram

Description automatically generatedDiagram

Description automatically generated

# IP Addressing

## A picture containing text Description automatically generatedIPv4 address

* 32-bit = 4 byte
* 232 addresses possible

## IPv6 address

* 128-bit = 16 byte
* 2128 addresses possible

## IPv4 subnetting

* Private IP addresses:

Table

Description automatically generated

* Address not private = public
* Home routers: usually 192.168.0.1
* NAT (Network Address Translation)
* Classful network design ≠ scalable
* Replaced by CIDR (Classless Inter-Domain Routing Variable-Length Subnet Masking)
  + E.g.: 172.23.9.15/16
  + 2 major addresses can be deducted:
    - Network Address = start of subnet
    - Broadcast Address = end of subnet
      * These cannot be used for a host
* Deducting the NA
  + Binary “and” between IPa and SN

**172.23.9.15/16**

1010 1100 . 0001 0111 . 0000 1001 . 0000 1111 => 172.23.8.15

1111 1111 . 1111 1111 . 0000 0000 . 0000 0000 => /16

1010 1100 . 0001 0111 . 0000 0000 . 0000 0000 => NA = 172.23.0.0

Network bits Host bits

**172.23.9.15/23**

1010 1100 . 0001 0111 . 0000 1001 . 0000 1111 => 172.23.9.15

1111 1111 . 1111 1111 . 1111 1110 . 0000 0000 => /16

1010 1100 . 0001 0111 . 0000 1000 . 0000 0000 => NA = 172.23.8.0

Network bits Host bits

* Deducting broadcast address
  + = network address, but the host bits are all 1’s

**172.23.9.15/16**

1010 1100 . 0001 0111 . 0000 1001 . 0000 1111 => 172.23.8.15

1111 1111 . 1111 1111 . 0000 0000 . 0000 0000 => /16

1010 1100 . 0001 0111 . 0000 0000 . 0000 0000 => NA = 172.23.0.0

1010 1100 . 0001 0111 . 1111 1111 . 1111 1111 => BA = 172.23.255.255

**172.23.9.15/23**

1010 1100 . 0001 0111 . 0000 1001 . 0000 1111 => 172.23.9.15

1111 1111 . 1111 1111 . 1111 1110 . 0000 0000 => /16

1010 1100 . 0001 0111 . 0000 1000 . 0000 0000 => NA = 172.23.8.0

1010 1100 . 0001 0111 . 0000 1001 . 1111 1111 => BA = 172.23.9.255

* Extra deductions we can make
  + E.g.: 192.168.0.101/24
  + Class: C
  + Private / Public: Private
  + Classful mask /24 or 255.255.255.0
  + # hosts / subnet 32-24 (network bits) = 8 host bits

28 = 256 – 2 = 254 hosts (network and broadcast address)

* + E.g.: 172.123.9.15/23
  + Class: B
  + Private / Public: Public
  + Classful mask: /16 or 255.255.0.0
  + # hosts / subnet 32-23 = 9

29-2 = 510 hosts

* + # subnets in classful

network 23-16 = 7

27 = 128 subnets

# Routing Between Networks

## The Need for Routing

### Criteria for Dividing the Local Network

* Diagram

  Description automatically generatedBroadcast containment

Routers in the distribution layer can limit broadcasts to the local network where they need to be heard. Although broadcasts are necessary, too many hosts connected on the same local network can generate excessive broadcast traffic and slow down the network

* Diagram

  Description automatically generatedSecurity

Routers in the distribution layer can separate and protect certain groups of computers where confidential information resides. Routers can also hide the addresses of internal computers from the outside world to help prevent attacks, and control who can get into or out of the local network.

* Diagram

  Description automatically generatedLocations

Routers in the distribution layer can be used to interconnect local networks at various locations of an organization that are geographically separated.

* Diagram

  Description automatically generatedLogical Grouping

Routers in the distribution layer can be used to logically group users, such as departments within a company, who have common needs or for access to resources.

### Now We Need Routing

* Switch examines MAC addresses.

A picture containing chart

Description automatically generated

* Router examines IP addresses

Chart

Description automatically generated with low confidence

## The Routing Table

### Path Selection

* Each router interface connects to a different network.
* A routing table contains information for how to reach local and remote networks.
* The destination IP address is used and compared with the networks in the routing table to determine the interface to forward the packet out of.

Diagram

Description automatically generated

* Routers do not forward broadcast messages

Diagram

Description automatically generated

### Packet Forwarding

* The destination MAC address is used to forward the packet to either the router if the destination IP address is for a different network or a specific network device on the local network.
* The ARP table shows a mapping of IP address to MAC address.

Diagram

Description automatically generated

### Routing Table Entries

* A routing table contains network addresses and the best path to reach a network.
* Two ways routes can be added to a routing table
  + Dynamically learned from other routers
  + Manually entered by a network administrator
* A default route is the router interface used when forwarding packets to a destination that is not in the routing table.
* If a packet is destined for a network that is not in the routing table and no default route exists, the packet will be dropped.

Diagram

Description automatically generated

Graphical user interface

Description automatically generated with low confidence

### The Default Gateway

* When a host sends a message to a device on the same network, it forwards the message directly and uses ARP to discover the MAC address.
* When a host sends a message to a device on a remote network, the hosts uses the MAC address of the router as the destination, but still has the IP address of the remote host as the Layer 3 destination.
* It is very important that each host has the correct default gateway that is the IP address of the router on the same network.

Diagram

Description automatically generatedTable

Description automatically generated

## Create a LAN

### Local Area Networks

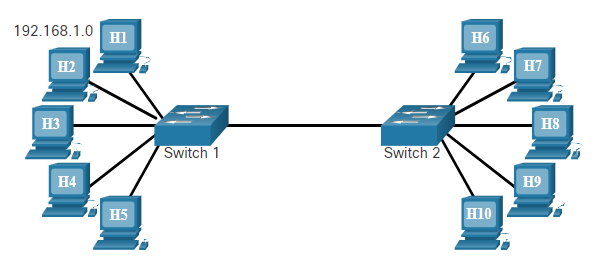
* LANs are under one administrative control
* LANs are usually either wired Ethernet or wireless

**3 LANs**

Diagram

Description automatically generated

### Local and Remote Network Segments

Advantages of a single local segment:

* Appropriate for simpler networks
* Less complexity and lower network cost
* Allows devices to be “seen” by other devices
* Faster data transfer – more direct communication
* Ease of device access

Disadvantages of a single local segment

* All hosts are in one broadcast domain which causes more traffic on the segment and may slow network performance
* Harder to implement QoS (Quality of Service)
* Harder to implement security

Diagram

Description automatically generatedAdvantages of having hosts on a remote segment:

* More appropriate for larger, more complex networks
* Splits up broadcast domains and decreases traffic
* Can improve performance on each segment
* Makes machines invisible to those on other local network segments
* Can provide increased security
* Can improve network organization

Disadvantages of having hosts on a remote segment:

* Requires the use of routing (distribution layer)
* Router can slow traffic between segments
* More complexity and expense (requires a router)

# The Internet Protocol

## Purpose of the IPv4 Address

### The IPv4 Address

* Is a logical network address that identifies a particular host
  + Must be properly configured and unique within the LAN
* Is assigned to the network interface connection for a host such as a workstation, server, network printer or IP phone
* Router interfaces that provide to an IP network will also have an IPv4 address
* Every packet sent across the internet has a source and destination IPv4 address
  + Required by networking devices to ensure the information gets to the destination and any replies are returned to the source

## Binary Conversion of an IPv4 Address

### IPv4 Addressing

* Series of 32 binary bits (0/1)
  + Grouped into 4 8-bit octets called ‘bytes’
* One decimal per byte
* Quad Dotted Decimal: 192.168.1.5 (4 groups of decimal numbers separated by dots)

### Binary to Decimal

A picture containing chart

Description automatically generated

## The IPv4 Address Structure

### Networks and Hosts

* The logical 32-bit IPv4 address is hierarchical and made up of 2 parts: network and host.
  + e.g.: 192.168.5.11/24 (-/24 = subnet mask: 255.255.255.0)
  + network: 192.168.5
  + host: .11
* routers only need to know how to reach eat network, rather than needing to know the location of each individual host.
* Multiple logical networks can exist on one physical network, if the network portion of the network host is different
  + Hosts with the same network number in their IPv4 addresses will be able to communicate with each other, but will not be able to communicate with the other hosts without the use of routing.

E.g.: 1 physical network, 2 logical IPv4 networks

Diagram

Description automatically generated

### Logical AND

* One of three basic binary operations used in digital logic and is used in determining the network address
* It is the comparison of 2 bits that produce the results shown in the following:
  + 1 AND 1 = 1
  + 0 AND 1 = 0
  + 1 AND 0 = 0
  + 0 AND 0 = 0
* To identify the network address of an IPv4 host, the IPv4 address is logically ANDed, bit by bit, with the subnet mask.

E.g.: IPv4 address: 192.168.0.241 subnet mask: 255.255.255.0

1100 0000 . 1010 1000 . 0000 0000 . 1111 0001 (IP)

1111 1111 . 1111 1111 . 1111 1111 . 0000 0000 (SM)

1100 0000 . 1010 1000 . 0000 0000 . 0000 0000 (Network address = 192.168.0.0)

### Calculate Whether the Destination is Local or Remote

* Subnet mask tells you which portion of an IPv4 is the network and which is the host
* When a host sends a packet, it compares its subnet mask to its own IPv4 and the destination IPv4
  + If the network bits match, they are on the same network = local
  + If the network bits don’t match, they aren’t on the same network.
    - The host forwards the packet to the local router interface to be sent to the other network

### Calculate the Number of Hosts

## Classful IPv4 Addressing

|  |  |  |
| --- | --- | --- |
| Class A | 0.0.0.0/8 – 127.0.0.0/8 | SM: 255.0.0.0 (+16mill hosts) |
| Class B | 128.0.0.0/16 – 191.255.0.0/16 | SM: 255.255.0.0 (+-65k hosts) |
| Class C | 192.0.0.0/24 – 223.255.255.0/24 | SM: 255.255.255.0 (254 hosts) |

## Public and Private IPv4 addresses

|  |  |
| --- | --- |
| Class A | 10.0.0.0/8 – 10.255.255.255 |
| Class B | 172.16.0.0/12 – 172.31.255.255 |
| Class C | 192.168.0.0/16 – 192.168.255.255 |

* Most organizations use private IPv4 addresses for their internal hosts
  + They must be translated to a public address to be routable in the internet
* NAT (Network Address Translation) is used to translate between private and public addresses
  + Usually done on the router that connects the internal network to the ISP’s (Internet Service Provider) network

Diagram

Description automatically generated

### Assignment of IPv4 Addresses

* For a company or organization to support network hosts that are accessible from the internet, it must have a block of public addresses assigned
* Public addresses are regulated and allocated to each organization separately. They must be unique and not repeated in their use across the world
* Both IPv4 and IPv6 addresses are managed by the IANA (Internet Assigned Numbers Authority)
  + IANA manages and allocates blocks of IP addresses to the Regional Internet Registries (RIR’s)
  + RIR’s are in turn responsible for providing address blocks to organisations and smaller ISP’s

## Unicast, Broadcast and Multicast Addresses

### Unicast Transmission

* Used for normal host-to-host communication in both a client/server and peer-to-peer network
* Unicast packets use the address of the destination device as the destination address and can be routed through an internetwork
  + During the encapsulation process, the source host uses its IPv4 address as the source address and the IPv4 address of the destination host as the destination address
  + Regardless of whether the destination specified a packet as a unicast, broadcast or multicast; the source address of any packet is always the unicast address of the originating host

### Broadcast transmission

* Broadcast packets are sent to all hosts in the network using a broadcast address
  + Contains a destination IPv4 with a 1’s in the host portion
    - All hosts on that local network (broadcast domain) will receive and look at the packet
    - When a host receives a broadcast packet, it processes the packet as it would one addressed to its unicast address
* Broadcast may be directed or limited
  + Directed: Sent to all hosts on a specific network
  + Limited: Sent to 255.255.255.255
* By default, routers do not forward broadcasts
  + Routers can eliminate excessive broadcast traffic by subdividing networks into separate broadcast domains

### Multicast Transmission

* Reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a multicast group
* IPv4 has reserved the 224.0.0.0 – 239.255.255.255 addresses as a multicast range
  + IPv4 multicast range addresses are reserved for multicasting on the local network only
    - a router connected to the local network will not forward them further
* hosts that receive multicast data are called multicast clients
  + They use services requested by a client program to subscribe to the multicast group
  + Each multicast group is represented by a single IPv4 multicast destination address

# Dynamic Addressing with DHCP

## Static and Dynamic Addressing

### Static IPv4 Address Assignment

* IPv4 addresses can be assigned either statically or dynamically
* With a static assignment, the host IPv4 address must be configured manually, together with the subnet mask, default gateway and DNS server address
* Static addresses are typically assigned for printers, servers, and other networking devices that need to retain a fixed IP address to provide services

### Dynamic IPv4 Address Assignment

* IPv4 addresses can be dynamically assigned to end devices through an application protocol known as Dynamic Host Configuration Protocol (DHCP)
* DHCP automatically assigns addressing information such as IPv4 address, subnet mask, default gateway and other configuration information
* Benefits:
  + Reduces the burden on network support staff and virtually eliminates entry errors
  + A dynamic IP address is not permanently assigned to a host, but leased for a period of time

### DHCP Servers

* A device can be a DHCP server if it’s running the DHCP service software
* DHCPv4 servers are typically connected to a LAN because it uses broadcast. DHCPv4 servers deployed outside of a LAN will require a relay service
* In a SOHO, a wireless router provides DHCP service to end devices, it is also a DHCP client to get IPv4 address from ISP

Diagram

Description automatically generated

## DHCPv4 Configuration

### DHCPv4 Operation

* When a host is configured using DHCP, it will try to obtain an IPv4 address, SM, DG and DNS from a DHCP
* Process:
  + Client sends DHCPDISCOVER message using broadcast
  + DHCP server responds with a DHCPOFFER message with a set of IPv4 addressing information
  + Client sends DHCPREQUEST message to request the use of the IPv4 addressing information
  + DHCP server responds with DHCPACK message to grant the request

# IPv4 and IPv6 Address Management

## Network Boundaries

### Routers as Gateways

* Routers are used to connect networks
* Each router interface connects to a separate network
* The IPv4 address assigned to the interface is the default gateway address for all hosts connected to that same network
* Hosts commonly get an IPv4 address using DHCP

Diagram

Description automatically generated

### Routers as Boundaries Between Networks

* A wireless router commonly provides IP addressing information for local internal hosts
* A router that connects to the internet commonly gets addressing information using DHCP from the internet provider

## Network Address Translation

### NAT Operation

* NAT is used to convert private IP addresses used within a company to a public address that can be routed on the internet
* One public address can be shared among many private IP addresses through the use of port numbers

Diagram

Description automatically generated

## IPv4 Issues

### Need for IPv6

* While NAT has been used to slow the depletion of IPv4 addresses, NAT creates latency and has limitations
* IoT devices are furthering the need for IPv6 addressing

### IPv4 and IPv6 Coexistence

* Dual stack allows IPv4 and IPv6 to coexist on the same network segment.
* Dual stack devices run both 4 and 6 protocol stack simultaneously.
* Known as native IPv6, this means the customer network has an IPv6 connection to its ISP and is able to access content found on the internet over IPv6

Diagram

Description automatically generated

* Tunnelling is a method of transporting and IPv6 packet over an IPv4 network
* The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data
* IPv4 tunnel between 2 dual stack routers that connect to IPv6-only networks:

Diagram

Description automatically generated

* NAT64 router translating between an IPv6-only and IPv4-only network:

Diagram

Description automatically generated

## IPv6 Features

### Autoconfiguration and Link-Local Addresses

* Stateless Address Autoconfiguration (SLAAC) allows a host to create its own internet-routable IPv6 address without the need for a DHCP server
* Link-local address is used to communicate with devices on the same IPv6 local network

A picture containing diagram

Description automatically generated

### IPv6 Address Representation

* Omit leading zeros in any 16-bit section
  + ODB8 is DB8
  + 0000 is 0
  + 0200 is 200
* Omit any group of consecutive “all zero” segments and insert a double colon (:😊
  + Can only use one ::

Table

Description automatically generated

# Transport Layer Services

## The Client Server Relationship

### Client and Server Interaction

* We use network services available over networks and the internet to communicate with others and to perform routine tasks
* A server is a host running a software application (or server service) that provides services to other hosts (clients)
* There are millions of servers on the internet
  + Clients and servers interact following agreed upon standards and protocols

### Client Requests a Web Page

* A client/server system is illustrated by the interaction between a web client and a web server:
  + A person uses a web browser to access a web server by sending a request, for example requesting a web page
  + The server receives the request and responds by sending the requested web page back to the client
* A web server is usually in a part of the network with other servers called a farm, or within a data center

### URI, URN and URL

* Uniform Resource Name (URN) – identifies only the namespace of the resource without reference to the protocol
* Uniform Resource Locator (URL) – defines the network location of a specific resource on the network

A picture containing diagram

Description automatically generated

* Components in the example URL:
  + Protocol/scheme - HTTPS or other protocols such as FTP, SFTP, mailto, and NNTP
  + Hostname - w​ww.example.com
  + Path and file name - /author/book.html
  + Fragment - #page155

## TCP and UDP

### Protocol Operations

* A web server and a web client use specific protocols and standards in the process of exchanging information to ensure that the messages are received and understood
* The various protocols necessary to deliver a web page function at the four different layers of the TCP/IP model are as follows:
  + Application layer protocol
    - HTTP (Hypertext Transfer Protocol) governs the way a web server and client interact
  + Transport layer protocol
    - TCP (Transmission Control Protocol) ensures that IP packets are sent reliably and any missing packets are resent
  + Internetwork layer protocol
    - IP (Internet Protocol) is the most common internetwork protocol, which is used to identify end hosts and to route packets to destination hosts
  + Network access layer
    - The specific protocol at the network access layer, such as ethernet, depends on the type of media and transmission methods used in the physical network

### Graphical user interface, diagram Description automatically generatedTCP and UDP

* each service has its own application protocols that are implemented in the server and client software
* All the common internet services use IP to address and route messages between source and destination hosts
* The service application decides which transport protocol to use. Transport protocols specify how to manage the transfer of messages between hosts
* The 2 most common transport protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)

### TCP Reliability

* Transmission Control Protocol helps ensure reliable delivery of data packets:
  + TCP breaks up a message into small pieces (segments)
  + Segments are numbered in sequence and passed to the IP process for assembly into packets
  + TCP tracks the number of segments that have been sent
  + If the sender does not receive an acknowledgement within a certain period, it assumes that the segments were lost and retransmits only the missing portion of the message
* On the receiving host, TCP is responsible for reassembling the message segments in order and passing them to the application

### UDP Best Effort Delivery

* In some applications, reliable delivery is not required => UDP
  + UDP is a “best effort” delivery system that does not require acknowledgement of receipt
  + UDP is preferable with applications that use time sensitive technology such as streaming audio and voice over IP (VoIP)
  + Acknowledgment would slow down delivery and retransmissions are undesirable

## Port Numbers

### TCP and UDP Port Numbers

* When a message is delivered using either TCP or UDP, the protocols and services requested are identified by a port number
* A port is a numeric identifier within each segment that is used to keep track of specific coverstations between a client and server
* Every message that a host sends contains both a source and destination port
* Ports are assigned and managed by an organization known as the Internet Corporation for Assigned Names and Numbers (ICANN)
* Ports are broken into 3 categories and range in number from 1 to 65,535:
  + Well-Known Ports
    - Destination ports that are associated with common network applications
    - 1 – 1023
  + Registered Ports
    - Ports that can be used as either source or destination
    - 1024 – 49,151
  + Private Ports
    - Can be used by any application, often as source ports
    - 49,152 – 65,535

### Destination and Source Port Numbers

* The source port number is associated with the originating application on the local sending host
* The destination port number is associated with the destination application on the remote host
  + Source Port
    - Dynamically generated by the sending device to identify a conversation between 2 devices
    - Allows multiple conversations to occur simultaneously
  + Destination Port
    - Client places a destination port number in the segment to tell the destination server what service is being requested
    - Server responds to the request and sends information back to the sending device using the source port

Graphical user interface, website

Description automatically generated

### Socket Pairs

* The source and destination port are placed within the segment PDU
* It is encapsulated within an IP packet which contains the IP of the source and destination
* The combination of source IP and source port number, or destination IP and destination port number is called a **socket**

A picture containing chart

Description automatically generated

* In the example, the socket is used to identify the server and service being requested by the client
* A client socket might look like 192.168.1.5:1099
* The socket on a web server might be 192.168.1.7:80
* Together these 2 sockets form a socket pair
* The source port number acts as a return address for the requesting application

### Netstat Command

* Unexplained TCP connections can pose a major security threat
* On a PC, the command “netstat” lists the protocols in use, the local address and port numbers, the foreign address and port numbers and the connection state

# Application Layer Services

## Network Application Services

### Common Network Application Services

* The most common internet services include internet searches, social media sites, video and audio straming, online shopping sites, email, etc…
  + Each of these relies on protocols from the TCP/IP protocol suite to reliably communicate the information between the clients and the servers

Table

Description automatically generated

## Domain Name System

### Domain Name Translation

* It would be impossible to remember the IP addresses for all of the servers hosting services on the internet
* Instead there is an easier way to locate servers by associating a name with an IP address:
  + DNS names are registered and organized on the internet within specific high-level groups, or domains
    - Some of the most common high-level domains on the internet are .com, .edu, and .net

### DNS Servers

* A DNS server contains a table that associates hostnames in a domain with corresponding IP addresses
* When a client has the name of server, such as a web server, but needs to find the IP address, it sends a request to the DNS server on port 53
* When the DNS server receives the request, it checks its table to determine the IP address associated with that web server
* If the local DNS server does not have an entry for the requested name, it queries another DNS server within the domain

## Web Clients and Servers

### HTTP and HTML

* When a web client receives the IP address of a web server, the client browser uses that IP address and port 80 to request web services
  + This request is sent to the server using the Hypertext Transfer Protocol (HTTP)
  + Requests for secure HTTP are sent to port 443
* When the server receives a port 80 request, the server responds to the client request and sends the web page to the client
  + The information content of a web page is encoded using specialized ‘mark-up’ languages
    - The HyperText Markup Language (HTML) coding tells the browser how to format the web page and what graphics and fonts to use
    - HTML is the most commonly used language

## FTP Clients and Servers

### File Transfer Protocol

* The File Transfer Protocol (FTP) provides an easy method to transfer files from one computer to another
* A host running FTP client software can access FTP server to perform various file management functions, including file uploads and downloads
* The FTP server enables a client to exchange files between devices, it also enables them to manage files remotely by sending file management commands such as delete or rename
* The FTP service uses two different ports to communicate between client and server
  + To begin an FTP session, control connection requests are sent to the server using destination TCP port 21
  + When the session is opened, the server uses TCP port 20

# Security Considerations

## Security Threats

### Types of Threats

* 4 types of threats
  + Information theft
    - Breaking into a computer to obtain confidential information
    - Stolen info can be used or sold for various purposes
    - Solution: backups
  + Data loss and manipulation
    - Breaking into a computer to destroy or alter data records
    - E.g.: data loss:
      * threat actor sends a virus that reformats a computer hard drie
    - E.g.: data manipulation:
      * Breaking into a records system to change info, such as the price of an item
  + Identity theft
    - A form of information theft where personal information is stolen for the purpose of taking over the identity of someone
    - Using this info, a threat actor can obtain legal documents, apply for credit and make unauthorized online purchases
    - Identity theft is a growing problem costing billions of dollars per year
  + Disruption of service
    - Preventing legitimate users from accessing services to which they are entitled
    - E.g.: denial of service (DoS) attacks on servers, network devices or network communications links

### Internal and External Threats

* External:
  + Individuals outside of an organization that do not have authorized access to the computer systems or network
  + External attackers work their way into a network mainly from the internet through wireless links or dialup access servers
* Internal:
  + When someone has authorized access to the network through a user account or has physical access to the network equipment
  + Internal attackers know the internal politics and people, they often know what info is both valuable and vulnerable and how to get to it
  + +- 80% of threats are internal

## Social Engineering Attacks

### Overview of Social Engineering

* One of the easiest ways for an intruder to gain access is by exploiting human behaviour through social engineering
* Social engineering involves various techniques used to deceive internal users into performing specific actions or revealing confidential information
* Through social engineering techniques, an attacker takes advantage of unsuspecting legitimate users to gain access to internal resources and private information, such as blank account numbers or passwords

### Types of Social Engineering Attacks

* Pretexting
  + Typically over the telephone, the attacker typically uses an invented scenario to get the victim to release info or perform an action
  + To be effective, the attacker must be able to establish legitimacy with the intended target or victim
* Phishing
  + In this attack the phisher pretends to represent a legitimate person from another organization
  + The phisher typically contacts the victim via email or text message
* Vishing
  + A newer form of social engineering that uses Voice over IP (VoIP)
  + Unsuspecting users are sent a voicemail instructing them to call a number which appears to be a legitimate phone-banking service
  + The call is then intercepted by a thief
  + Bank account numbers or passwords entered over the phone are stolen

## Malware

### Malicious software

* 3 kinds
  + Viruses
  + Worms
  + Trojan horses

### Spyware

* Spyware, tracking cookies, adware and popups
  + Designed to collect info about users which can be used for advertising, marketing, etc
  + May not damage computer, can still invade privacy
* Spyware = Any program that gathers personal information from your computer without your permission or knowledge.
* Cookies = A form of spyware, but not always bad. They are used to record information about an internet user when they visit websites. May be useful to allow personalization

### Adware and Popups

* Adware = A form of spyware that is used to collect information about a user based on websites the user visits. That information is then used for targeted advertising.
* Pupups = Popups and -unders, are additional advertising windows that display when a website is visited. Not intended to collect information

### Botnets and Zombies

* Malicious bot software infects a host
* Infected, the zombie computer contacts servers managed by the botnet creator
* The servers act as a command and control (C&C) center for an entire network of compromised devices which is called a botnet

## Denial of Service Attacks

### Denial of Service

* DoS
  + Aggressive attacks on an individual computer or groups of computers with the intent to deny services to intended users
  + DoS attacks can target end user systems, servers, routers and network links
  + DoS are relatively simple and can be initiated by an unskilled threat actor
  + Used to flood a network, host or application with traffic to prevent legitimate network traffic from flowing
  + Can disrupt connections between a client and server to prevent access to a service
* SYN (synchronous) flooding
  + A flood of packets with invalid source IP addresses are sent to a server requesting a client connection
  + The server becomes occupied trying to respond to these fake requests
* Ping of death
  + A packet that is greater in size than the maximum allowed by IP (65,535 bytes) is sent to a device
  + This can cause the receiving system to crash

### Distributed Denial of Service

* DDos
  + More sophisticated and potentially damaging form of DoS attack designed to saturate and overwhelm a network with useless data
  + May involve hundreds or thousands of attack points attempting to overwhelm a target simultaneously
    - These may be unsuspecting computers infected by the DDos code
  + Infected systems attack the target site when invoked
  + Group of infected computers = botnet
* Brute force
  + May result in DoS
  + The attacker tries a large number of possible passwords in rapid succession to gain access or crack a code
  + Can cause DoS due to excessive traffic to a specific resource or by locking users out

## Security Tools

* Change the default usernames like admin, administrator, guest,…
* Create passwords that aren’t easy to guess

Table

Description automatically generated with medium confidence

# Configure Network and Device security

## Wireless Security Measures

### Wireless Vulnerabilities

* Wireless networking provides ease and convenience of connecting devices
* Unfortunately, that ease of connectivity and the fact that the information is transmitted through the air also makes the wireless network vulnerable to interception and attacks, such as war-driving
* **War-driving** is the process of driving around and searching for wireless networks, when a wireless network is found, the location of the WLAN is logged and shared
  + When the access to a WLAN is compromised, an attacker can access the network from any location the wireless signal reaches
  + Special security features and implementation methods are required to help protect a WLAN from attacks

### A Comprehensive Security Plan

* Basic Wireless Setting
  + Change the default SSID and disable SSID broadcast
* Wireless Security
  + Set the security profile for each band to use WPA2 Personal
* MAC Address Filtering
  + BULLSHIT
* Port Forwarding
  + Configure the ports that should be forwarded to a specific device, such as a web server in the demilitarized zone
* DMZ (demilitarized zoned)
  + Configure the IPv4 address for the server in the DMZ

### SSID Broadcasts

* One easy way to gain entry to a WLAN is through the network name (SSID)
* By default, wireless routers and access points broadcast SSID’s to all computers within the wireless range
* With SSID broadcast activated, any wireless client can connect to it, if no other security features are configured
* The broadcast feature can be turned off, then the network is no longer made public
* Any client must already know the SSID to join the network
* Note: turning off SSID broadcast alone does not protect the wireless network from experienced threat actors

### Changing Default Settings

* Most wireless access points and routes are preconfigured with settings such as SSID’s, admin passwords and IP addresses, those default settings are well-known
* Changing the default settings on a router will not protect the wireless network by itself
  + E.g.: SSID’s are transmitted in plaintext, even with SSID broadcast turned off, and default values changed, attackers can learn the name of a WLAN through the use of devices that intercept wireless signals
* Other security measures should be implemented

### MAC Address Filtering

* Bullshit

## Implement Wireless Security

### Open Authentication

* Another way to control who can connect to the network is to implement authentication
  + = the process of permitting entry to a network based on a set of credentials
  + Used to verify that the device attempting to connect is trusted
* Most common = username + password
* ­­in a wireless environment, authentication, if enabled, must occur before the client can connect to the WLAN
* Different kinds of authentication
  + PSK
  + EAP
  + SAE
* By default, wireless devices do not require authentication = open authentication
  + Should only be used on public wireless networks ore where authentication will be done by other means

### Authentication and Association

* **Authentication** is to verify that the device which is trying to connect, is trusted
* **Association** is for a client to successfully connect to the AP and carry data communication
* After authentication is enabled, client must pass authentication before it can connect to the AP and join the network
* When authentication is successful, the AP will then check the MAC address against the MAC address table

### Authentication protocols

* Early wireless routers used an encryption protocol known as WEP (Wired Equivalency Protocol), to secure wireless transmissions between clients and AP’s
* WEP uses pre-configured keys to en-/decrypt data. A WEP key is entered as a string of numbers and letters and is generally 64 or 128 bits long (sometimes 256)
* WPA2 = better

## Configure a Firewall

### Firewall Overview

* Prevents undesirable traffic from entering protected areas of the network
* One of the most effective security tools available for protecting internal network users from external threats
* Usually installed between two or more networks and controls the traffic between them, as well as helping to prevent unauthorized access
* Use various techniques for determining what is permitted or denied access to a network

### Firewall Operation

* Can be implemented in software which is to be loaded onto PC’s, networking devices or servers
* May also be hardware devices for the single purpose of protecting areas withing the network
* Can be configured to block multiple individual external devices by IP address, to permit or deny packets matching the range of TCP or UDP ports
* Typically a firewall passes 2 different types of traffic into a network:
  + Responses to traffic that originates from inside the network
  + Traffic that originated from outside the organization that is destined for a port that you have intentionally permitted, such as a server located in the DMZ
* Additionally, they often perform Network Address Translation (NAT)

### The DMZ

* Many home network devices support demilitarized zone capabilities
* DMZ refers to an area of the network that is accessible and controlled for both internal and external users
* It is more secure than the external network but not as secure as the internal network
* With the wireless router, a simple DMZ can be set up that allows an internal server to be accessible by outside hosts
* The server requires a static IP that must be specified in the DMZ configuration
* The wireless router isolates traffic destined to the IP specified
* This traffic is then forwarded only to the switch port where the server is connected

### Port Forwarding

* Way to permit other users to reach devices inside the network through the internet
* A rule-based method of directing traffic between devices on separate networks
* This method of exposing internal devices to the internet is safer than using a DMZ
* When incoming traffic from the internet reaches the router, the firewall in the router determines if the traffic should be forwarded to a certain device based on the port number found with the traffic
* Port numbers are associated with specific services (e.g.: FTP, HTTP, HTTPS, POP3)
* Port forward rules configured in the firewall settings determine which traffic is permitted on to the inside LAN

|  |  |  |
| --- | --- | --- |
| HTTP | 80 | TCP |
| FTP | 21 | TCP |
| Telnet | 23 | TCP |
| SMTP | 25 | TCP |

* Port triggering allows the router to temporarily forward data through inbound TCP or UDP ports to a specific device
* Port triggering can be used to forward data to a computer only when a designated port range is used to make an outbound request
* One usage for port triggering is multiplayer games where a number of TCP and UDP connections could exist between the players while the game is active
* Port triggering should be configured carefully because leaving a large number of ports open to the internet can represent a security risk

# Troubleshoot Common Network Problems

## The Troubleshooting Process

### Structured Troubleshooting Methods

* Bottom-Up (**best method for most people**)
  + Start with the physical layer
  + Work you way up the Hybrid OSI-TCP/IP ladder
* Top-Down
  + Reverse
* Divide-and-Conquer
  + Only applicable if you know what you’re doing
* Follow-the-Path
  + Eliminate links and devices irrelevant to the problem
  + Follow from source to destination
* Substitution
  + Aka swap-the-component
* Comparison
  + Aka spot-the-difference
* Educated Guess
  + Aka shoot-from-the-tip