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

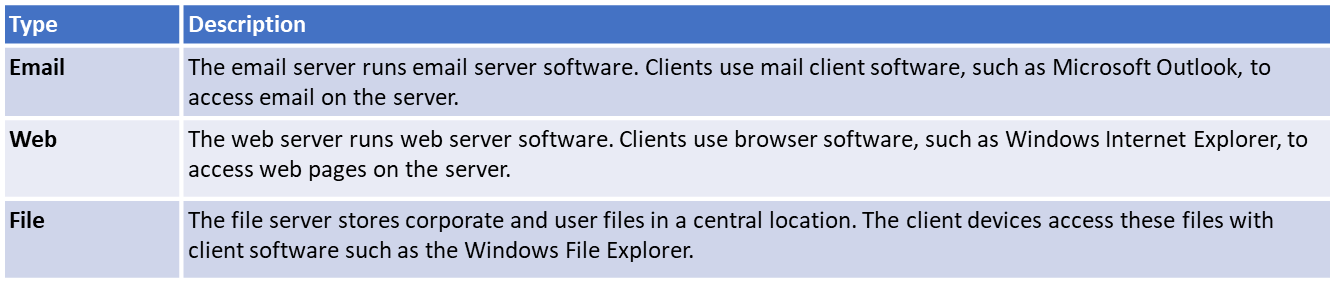
## Clients and Servers

### 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

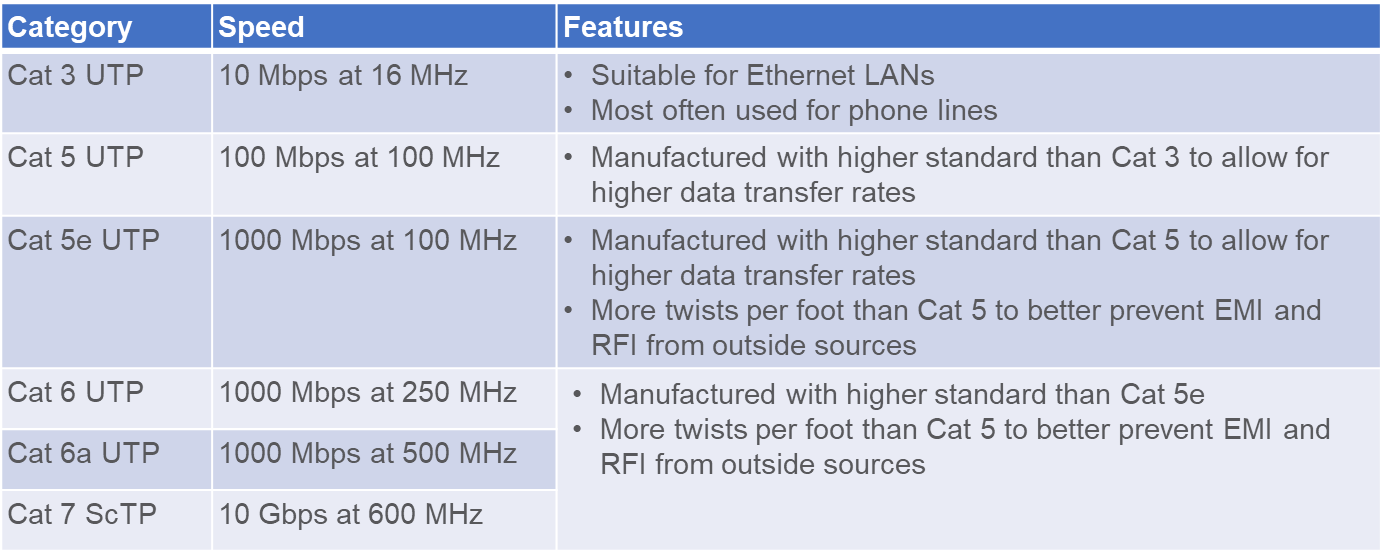
### Twisted-Pair Cables

* 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

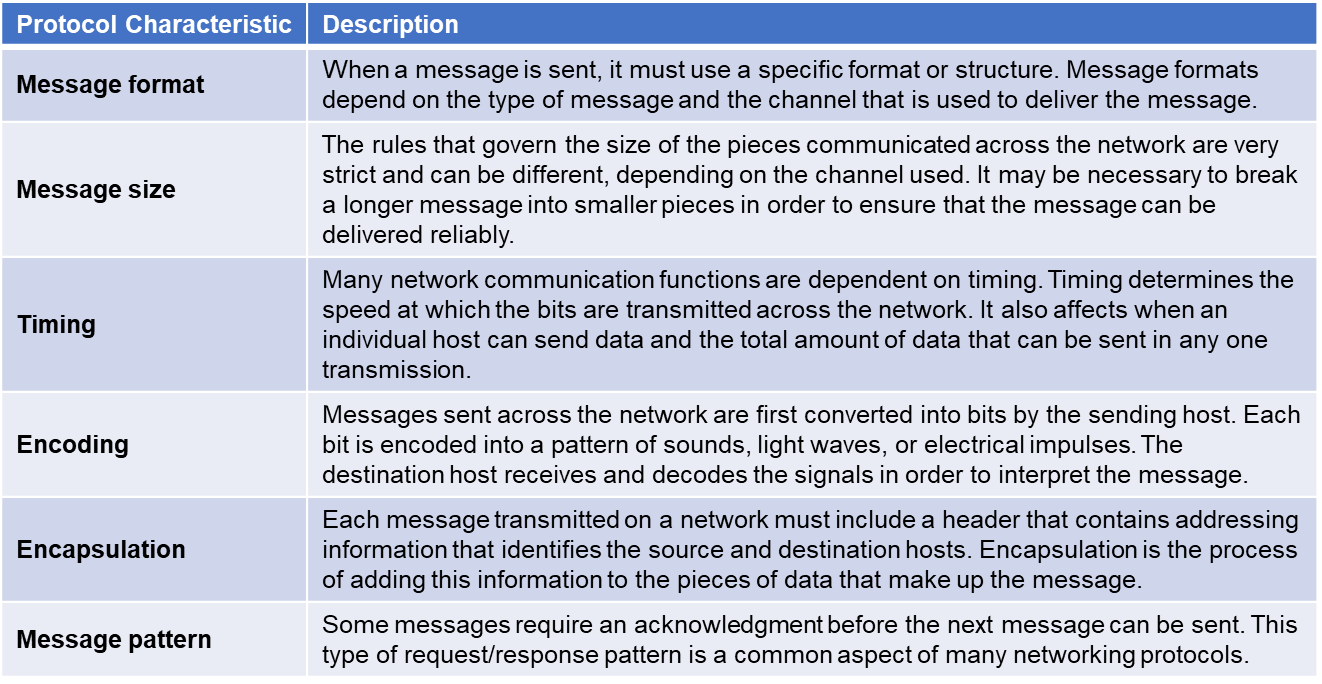
### The Three Elements

* 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

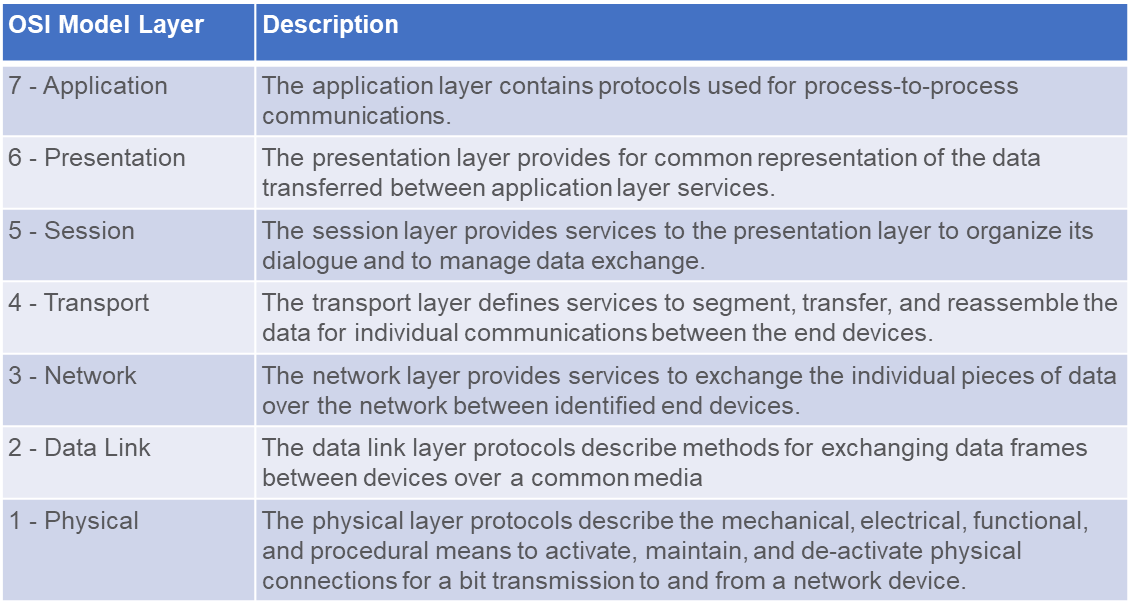
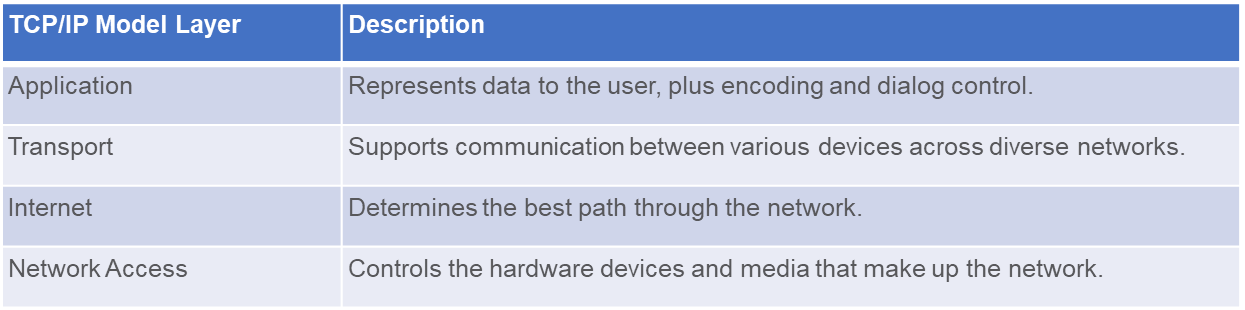
* **Transmission Control Protocol (TCP)**
  + Manages the individual conversations
  + Responsible for guaranteeing the reliable delivery of the information and managing flow control between end devices
* **Internet Protocol (IP)**
  + Responsible for delivering messages form the sender to the receiver
  + 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

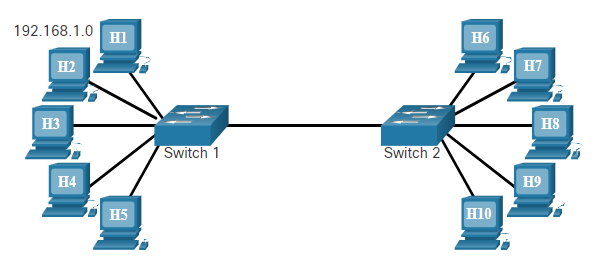
* LANs are under one administrative control
* LANs are usually either wired Ethernet or wireless

**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