Fundamentals of Computer Networks

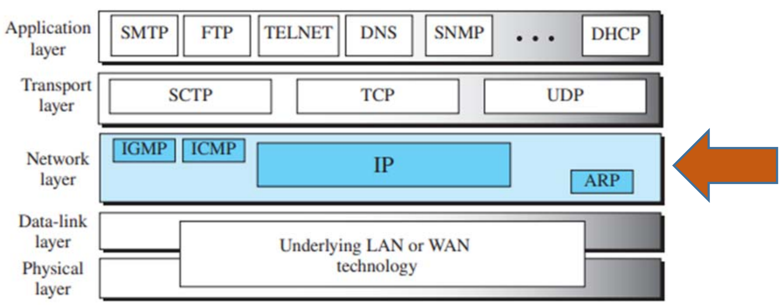
Understand computer network technology

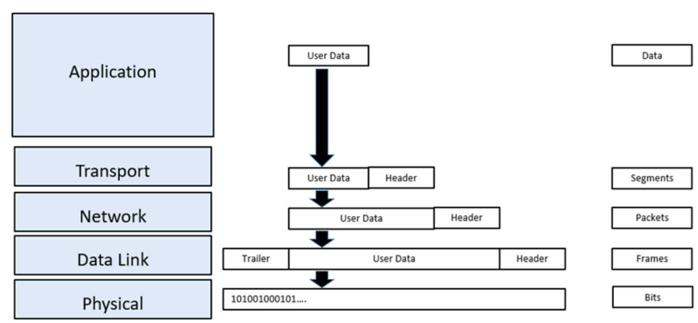
Lesson 3

Network Layer

TCP/IP Protocol Suite - Network layer (Recall)

- The main purpose of this layer is to select the best path for the data to travel through from the source to the destination, i.e., routing.
- The leading protocol operating in this layer is Internet Protocol (IP).
- There is a group of supporting protocols that support IP in doing its job, such as the Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and Reverse Address Resolution Protocol (RARP).





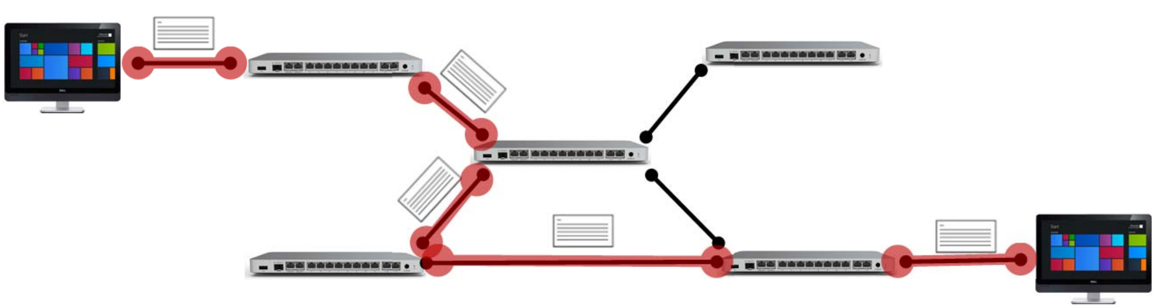
TCP/IP Protocol Suite

Mode of Data Transfer

Circuit Switching & Packet Switching

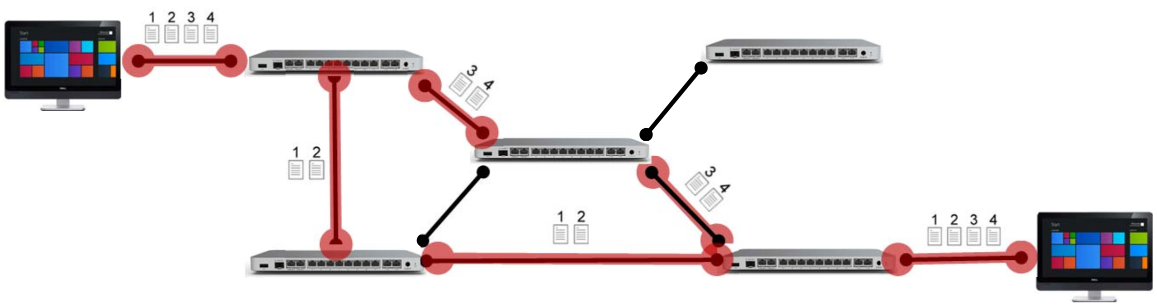
Mode of Data Transfer - Circuit Switching

- Connection-oriented.
- a connection needs to be established before the start of transmitting data from the sender to the receiver.
- Data moves across the same path throughout the entire communication.
- Example: early telephone systems – path was established between caller and callee.
- Never implemented at the network layer.



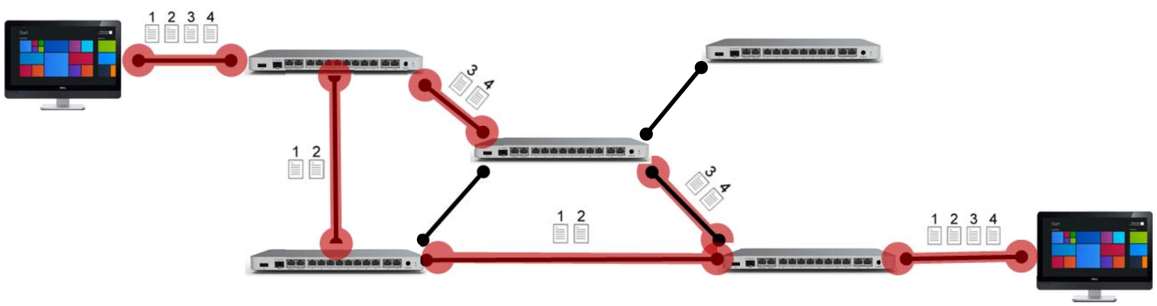
Mode of Data Transfer - Packet Switching

- Connectionless.
- No connection is established before the start of transmission of data
- Data is fragmented into smaller, more manageable chunks called packets.
- Each packet is then individually addressed and sent to its intended recipient.
- Each packet finds its own way to the receiver.



Mode of Data Transfer - Packet Switching

- Receiving computer wait for all packets of the message and reassembles the packets into the original message before delivering the message to the upper level.
- Network layer in the Internet is packet-switched network.



Packet Switching at Network Layer

- Routing is the process of selecting the best path for a packet to reach its destination.
- At the network layer, IP is responsible for sending packets from Host A to Host B, possibly via one or more routers.
- Key steps to perform this task:

Packet Switching at Network Layer

- At Host A.
  - Packetizing/Packet Creation - Encapsulate the data into an IP packet – adding the IP header which include the source IP address (Host A) and the destination IP address (Host B).
  - Routing decision – consult routing table :
    - If Host B is on the same local network, it sends the packet directly. This is known as direct delivery.
    - Otherwise (different network), forwards the packet to the default gateway (usually a router). This is call an indirect delivery.
  - Fragmentation
    - If the size of data is greater than the limitation of the size of the data to be carried in a frame. The packet will need to be fragmented to smaller units before being passed to the data-link layer. The size limit is the Maximum Transmission Unit (MTU).

Packet Switching at Network Layer

- At the router
  - Router receives the packet from Host A
  - Validate (header) of each packet, ensure header is not corrupted and packet is delivered to the correct router.
  - Checks the destination IP address in the packet
  - Consult routing table to determine the next hop to send the packet toward Host B and forward the packet to the next hop
  - Fragmentation of the packet into to smaller units before being passed to the data-link layer.
  - If multiple routers are involved, they will perform the same steps above

Packet Switching at Network Layer

- At Host B
  - Validate (header) of each packet, extract data from each fragment and stored
  - When all fragments have arrived, reassemble data and deliver data to upper layer (transport layer).
  - Network layer sets a reassembly timer. If the timer expired, all data fragments are destroyed and an error message is sent and all datagram need to be resent.

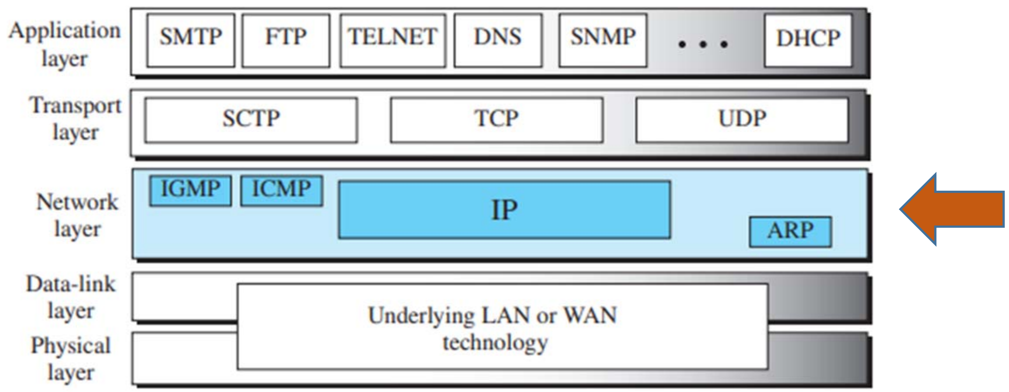
Things to do …

- Differences between circuit switching and packet switching
- Find out the advantages and disadvantages of circuit switching
- Find out the advantages and disadvantages of packet switching

Protocol

- A set of rules, standards, or procedures that govern how data is transmitted, received, and interpreted between devices in a communication network.
- Features of a Protocol
  - Protocols are standardized to ensure compatibility and interoperability between different systems, devices or software.
  - Protocols define how data is formatted and organized during transmission.
  - Protocols specify how devices initiate, maintain and terminate communication.
  - Protocols specify how errors are handled – detecting and correcting errors during transmission.

Network Layer - Protocols



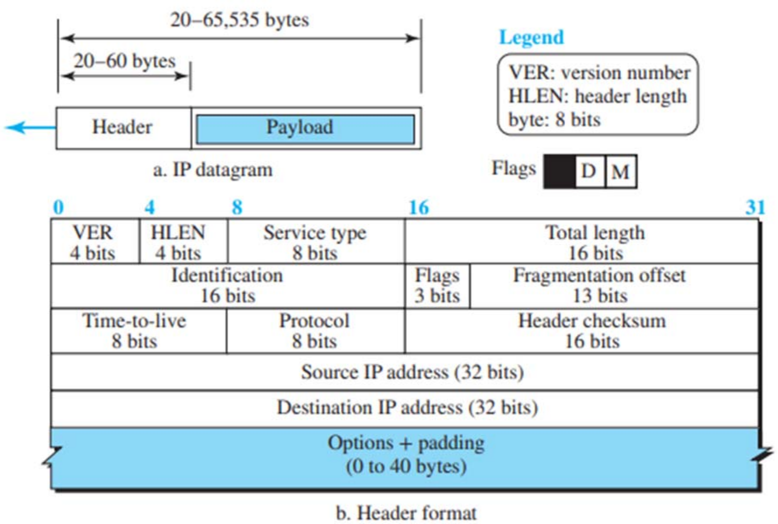
Protocols	Purpose
Internet Protocol version 4 (IPv4)	Responsible for packetizing, forwarding, and delivery of a packet at the network layer
Internet Control Message Protocol version 4 (ICMPv4)	supports the unreliable and connectionless IP by handling errors that may occur in the network-layer delivery
Internet Group Management Protocol (IGMP)	help IPv4 in multicasting
Address Resolution Protocol (ARP)	to glue the network and data-link layers in mapping network-layer addresses to link-layer addresses

Network layer - IP

IP is an unreliable connectionless protocol responsible for source-to-destination delivery.

- Protocol data unit (PDU) in the Network layer : Packets.
- Provide best-effort delivery service.
- Packets can be corrupted, lost, arrive out of order, delayed or create congestion for the network.
- Each packet is handled independently and can follow a different route to the destination

Network layer - IP



Field	**Size (bits)**	Description
Version (VER)	4	Indicates the IP version. For IPv4, this is always **4**.
Header Length (HLEN)	4	Specifies the length of the header in 32-bit words. Minimum value is 5 (20 bytes).
Service Type	8	Originally used to indicate priority. Now used as **DSCP** for Quality of Service (QoS).
Total Length	16	Length of the entire packet (header + data), in bytes. Maximum is 65,535.
Identification	16	A unique value used for identifying fragments of the same original packet.
Flags	3	Controls fragmentation. Includes **DF (Don't Fragment)** and **MF (More Fragments)** flags.
Fragmentation Offset	13	Used to reassemble fragmented packets in the correct order.
Time to Live (TTL)	8	Limits the packet's lifespan. Each router decrements it; packet is dropped when TTL reaches 0.
Protocol	8	Specifies the next-level protocol (e.g., **1 = ICMP**, **6 = TCP**, **17 = UDP**).
Header Checksum	16	Error-checking of the IPv4 header only (not the payload).
Source IP Address	32	The IPv4 address of the sender.
Destination IP Address	32	The IPv4 address of the intended recipient.
Options (optional)	Variabl e	Additional control information; rarely used. Header length increases if present.
Padding	Variabl e	Extra bits added to make header length a multiple of 32 bits.

https://datatracker.ietf.org/doc/html/rfc791

* **RFC stands for Request for Comments, a series of documents that are the foundation of Internet standards and protocols.**

Network layer - IP

How a packet is send from the host to source?

- The source and destination IP addresses are placed in the IP header as the packet moves down the TCP/IP stack.
- The Network layer checks whether the destination is on the same local network or a different (remote) network. This decision is based on comparing the destination IP address with the subnet mask to the source IP address with the subnet mask. If equal means the same subnet.
- If the destination is in the same subnet, the packet is sent directly to the destination host. This is known as direct delivery.

Network layer - IP

- If the destination is not in the same subnet, the packet is sent via the default gateway or router to reach the correct network. This is known as an indirect delivery.
- If the size of packet is greater than the limitation of the size of the data to be carried in a frame. The packet will need to be fragmented to smaller units before being passed to the data-link layer. The size limit is the Maximum Transmission Unit (MTU).
- The MAC address of the next hop/destination device (host/router) is obtained before passing the packet to the data link layer.
- MAC address resolution - using destination IP address using ARP

Network layer - ARP

- Address Resolution Protocol (ARP)
  - Main purpose is to map between logical protocol addresses (IP address) and hardware address (MAC address).
  - Resolve the IP address to hardware address.
  - Steps to resolve the hardware address
    - Look in ARP cache, if found – no future resolution – the ip-mac address is stored in the ARP cache for 2 minutes (max 10min)
    - If not found, an ARP request broadcast is initiated– all nodes in the local network received a copy of the ARP request.
    - The destination node that has the IP address contained in the destination protocol address field responds with its hardware address.

Network layer – ICMP/IGMP (Info)

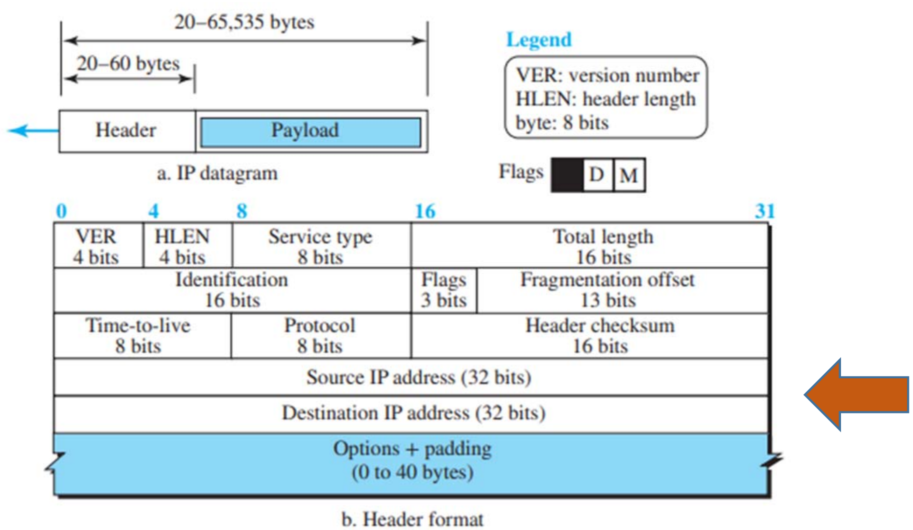
- Internet Control Message Protocol (ICMP)
  - Protocol used for sending error message, performing diagnostics, control the flow of data
  - ICMP source-quench packet sent by router to a source host to tell the host to slow down because the router is overloaded.
  - PING sent 4 ICMP echo request packets to test for connectivity
- Internet Group Message Protocol (IGMP)
  - Protocol that enables one host to send one stream of data to many hosts at the same time.
  - Multicast – move streams of data to hosts concurrently

Network Layer

IP Address

Network layer – IP Address

- Every host on a TCP/IP network needs to have a unique address. With this unique address, it is possible to send data from host to host.
- Every packet contains addressing information in the header, and the IP address in the header is used to route packets.

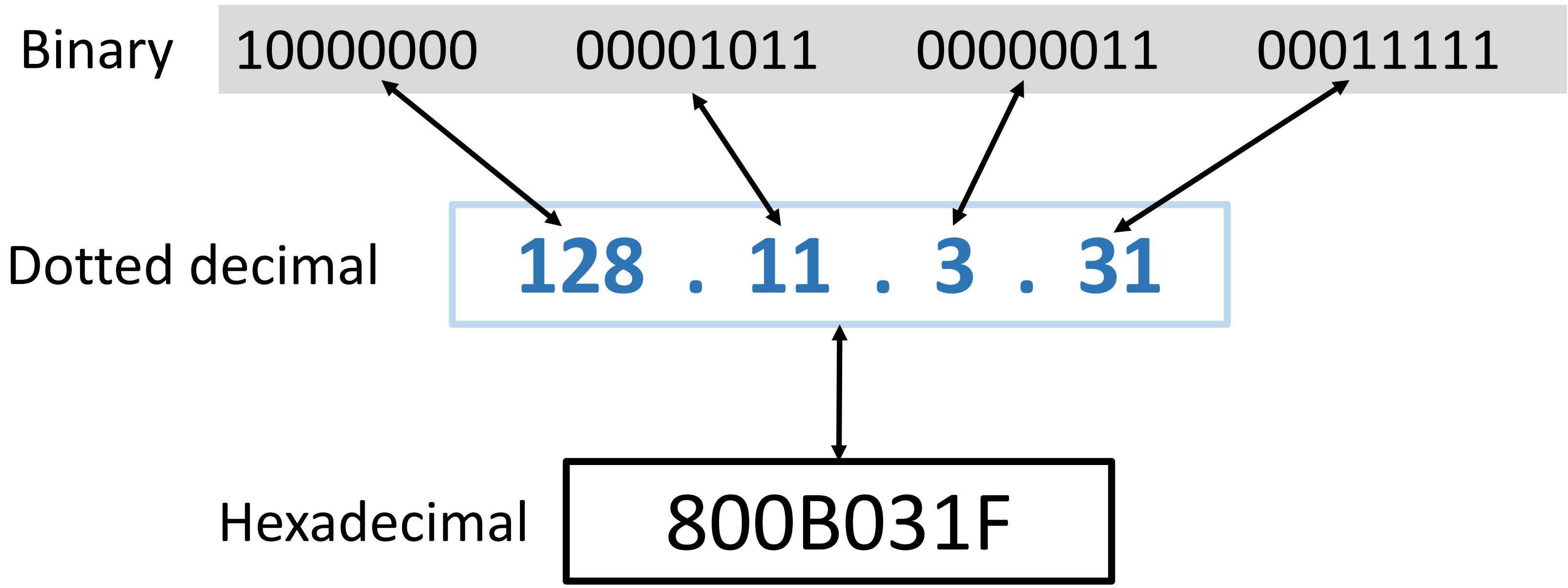


IPv4

- IPv4 – a 32-bit address that uniquely identifies every host on a network.
- Known as logical address – software assigned address and non-permanent
- IPv4 addresses are represented by a 32-bit unsigned binary value which is usually expressed in a dotted-decimal notation (more readable). Eg. 172.16.254.1
- https://www.youtube.com/watch?v=MwxMsaFFycg&t=3s

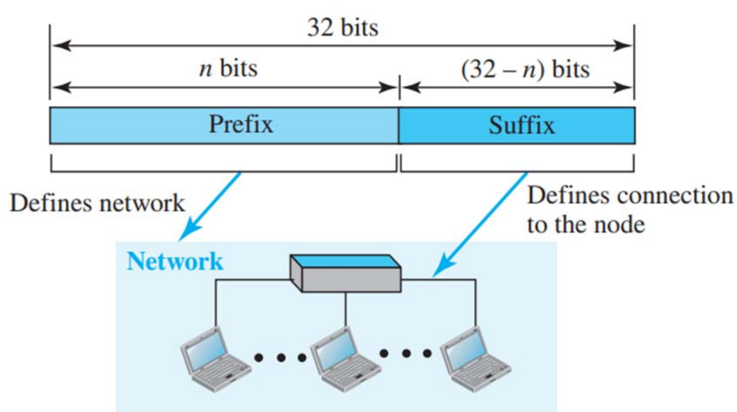
IPv4

Three different notations in IPv4 addressing



IPv4

- IPv4 is divided into 2 parts.
- First part (prefix) defines the network.
- Second part (suffix) defines the host (connection of a device to the Internet)
- The prefix length is n bits, the suffix length is (32 - n) bits



IPv6

- 128-bits addresses – possible unique addresses : 2^{128}
- Written in hexadecimal form – 32 hex digits
- 8 groups of 4 hex digits (16 bits)

    eg. `EFDC:BA62:7654:3312:EFDC:BA72:7653:3210`

- IPv4 can be used within the IPv6 addressing scheme
    - Hexa-decimal IPv4 address is placed in the last 32 buts of the IPv6 address.
    - Eg. IPv4 address - `192.168.2.100`

      IPv6 address - `::C0A8:0264`

IPv6

- IPv6 address with many 0s can be shorten (Zero compression)
  - Step 1: Non-significant and leading 0s can be dropped
  - Step 2: Address with consecutive 0s can be dropped and just push the colons together using double-colon notation. This can only be used once.

eg. `1080:0000:0000:0000:0008:0800:200C:417A`

Step 1: `1080:0:0:0:8:800:200C:417A`

Step 2: `1080::8:800:200C:417A`

IPv6 vs IPv4

Feature	IPv4	IPv6
Address size	32 bits	128 bits
Address format	Dotted decimal	Hexadecimal colon-separated
Number of addresses	$\sim 2^{32}$	$\sim 2^{128}$
Header size	Variable	Fixed, simplified
Broadcast	Supported	Replaced by multicast

IPv6 Address Types

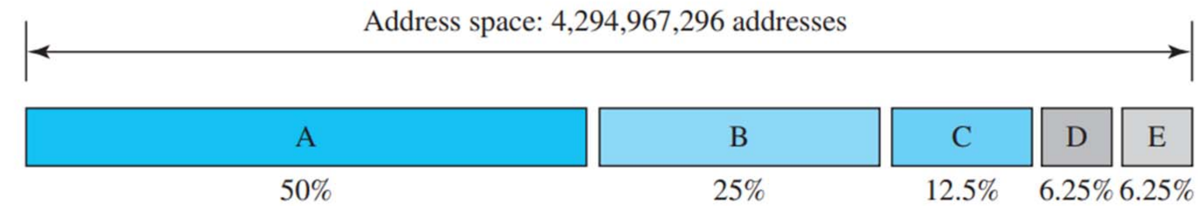
Address Type	Description	Starts With
Unicast	One-to-one communication	Depends on allocation
Multicast	One-to-many communication (like groups)	FF00::/8
Anycast	One-to-nearest (in routing terms)	Assigned to multiple interfaces
Link-local	For local communication within a network	FE80::/10
Global Unicast	Public IPv6 address	2000::/3

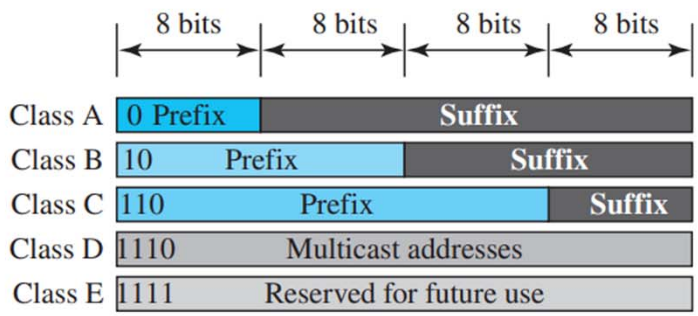
Network Layer

IPv4

IPv4 - Classful Addressing Scheme

- Fixed-length prefix – represent unique network address
- 3 fixed-length prefixes were designed to accommodate both small and large networks. n=8,16 and 24





Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

IPv4 – Class A

- Network portion has 8 bits (first octet).
  - First bit is always 0.
  - Possible network numbers is 2^7 or 128 possible network numbers
  - 0.0.0.0 is reserved and used for default route or special addressing
  - 127.0.0.0 is reserved and used for loopback
  - Usable Class A network addresses is 128 – 2 = 126
- Host portion has 24 bits
  - Possible combinations host is 2^{24} or 16,777,216
  - All host bits are 0: is for network address eg. 10.0.0.0
  - All host bits are 1: is for broadcast address eg. 10.255.255.255
  - Usable Class A host addresses is 2^{24} -2 or 16,777,214 (for each class A network)

IPv4 – Class B

- Network portion has 16 bits.
  - First 2 bits is always 10_2.
  - Usable network numbers is 2^{14} or 16,384 possible network numbers
- Host portion has 16 bits
  - Possible combinations host is 2^{16} or 65,536
  - All host bits are 0: is for network address eg. 172.16.0.0
  - All host bits are 1: is for broadcast address eg. 172.16.255.255
  - Usable Class B host addresses is 2^{16} -2 or 65,534 (for each class B network)

IPv4 – Class C

- Network portion has 24 bits.
  - First 3 bits is always 110_2.
  - Usable network numbers is 2^{21} or 2097152 possible network numbers
- Host portion has 8 bits
  - Possible combinations host is 2^8 or 256
  - All host bits are 0 : is for network address eg. 192.168.1.0
  - All host bits are 1 : is for broadcast address eg. 192.168.1.255
  - Usable Class C host addresses is $2^8 - 2$ or 254 (for each class C network)

IPv4 – Class D

- First bits: 1110
- Address range : 224.0.0.0 to 239.255.255.255
- Used for multicasting – send data to a selected group (multicast group) of devices (devices that join the multicast group)
- Not used for regular host address
- Usage : Video conferencing, streaming media, routing protocol

IPv4 – Class E

- First bits: 1111
- Address range : 240.0.0.0 to 255.255.255.255
- Reserved for experimental and future use
- Not used in public network
- Most systems ignore or block these addresses by default
- 255.255.255.255 is a limited broadcast address used to send to all hosts on the local network.

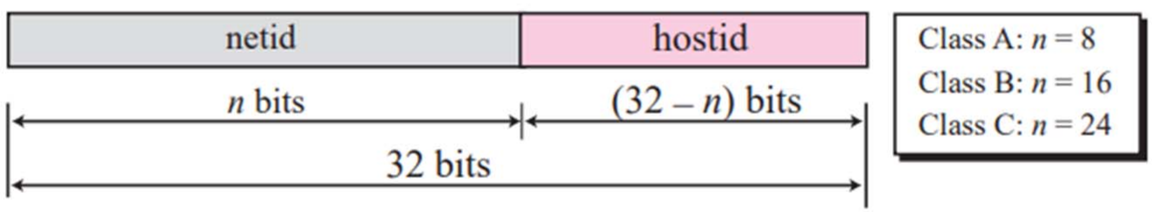
IPv4 – Different type of Address

- Network address
  - Identifies the entire network segment and it is not assigned to any device
  - Used by routers/devices to determine where to route packets (routing table)
  - First address in any subnet
- Broadcast address
  - Used to send a message to all hosts on the network at once and it is the last address in a subnet
- Multicasting* – send data to a selected group (multicast group) of devices (devices that join the multicast group)

*Broadcast vs Multicast

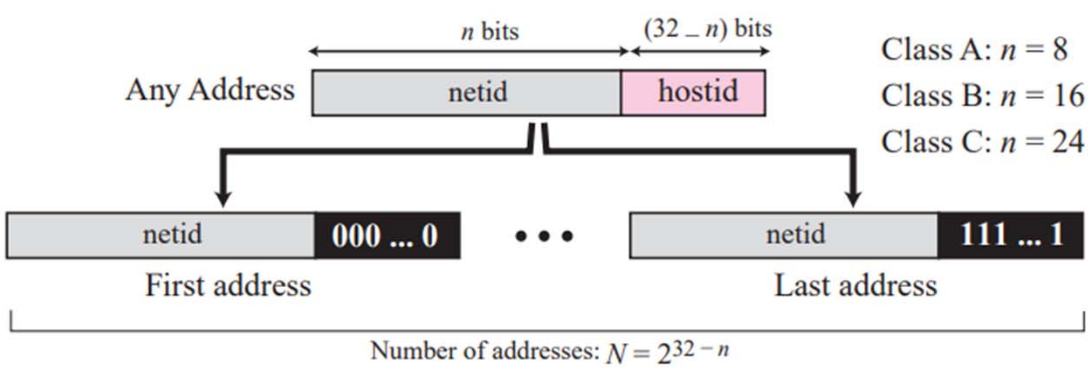
IPv4 - Classful Addressing Scheme

- Two level addressing in classful addressing
  - Each address in classful addressing contains 2 parts:
    - netid – defines the network
    - hostid – defines a particular host connected to the network (with the netid)



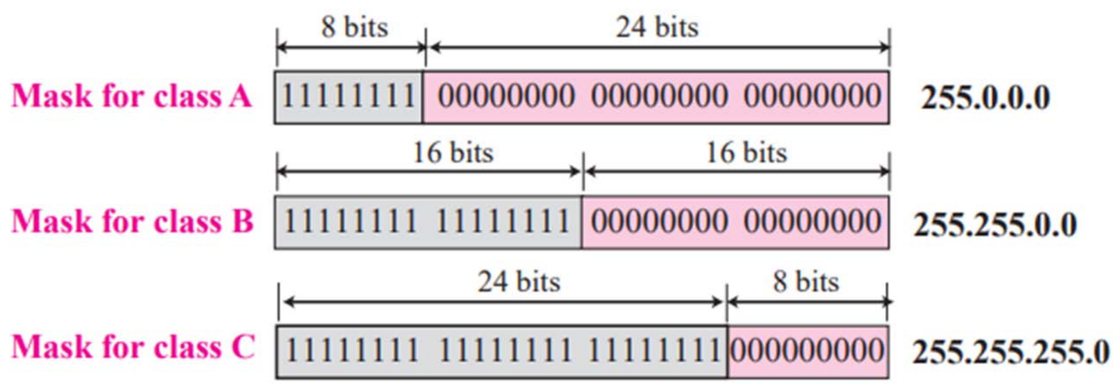
IPv4 - Classful Addressing Scheme

- Given any IP address (in classful address) we are able to find:
  - The class of the IP address and the value of *n*.
  - The number of addresses in the block (a range of addresses)
    - ➔ number of addresses in the block $N = 2^{32 - n}$
  - The first and last address in the block
    - ➔First address : keep the n leftmost bits and set the (32 - *n*) rightmost bits all to 0s
    - ➔Last address: keep the n leftmost bits and set the (32 - *n*) rightmost bits all to 1s



IPv4 – Network Mask

- A 32-bit number with the *n* leftmost bits set to 1s and the rest of the bits (32 - *n*) are set to 0s



- It is use to extract the network address from IP address by using the AND operation.

IPv4 – Network Mask

- Find network address of IP address: 201.24.67.32.
- Step 1: Find the class of IP address: class B
- Step 2: Network mask of class B is 255.255.0.0
- Step 3: Network address is

201.24.67.32 AND 255.255.0.0 → 201.24.0.0

Logical AND

IPv4 – Limitations

- IP addresses in fixed sizes (Class A,B,C) is either too large or too small for most organizations – IP address wastage and issues with scaling.
- Routing tables grew large and inefficient
- Rapid IPv4 exhaustion – classful structure wasted address space speeds up the exhaustion
- Not flexible and could not tailor address block size to network size

IPv4 – Strategies to overcome limitations

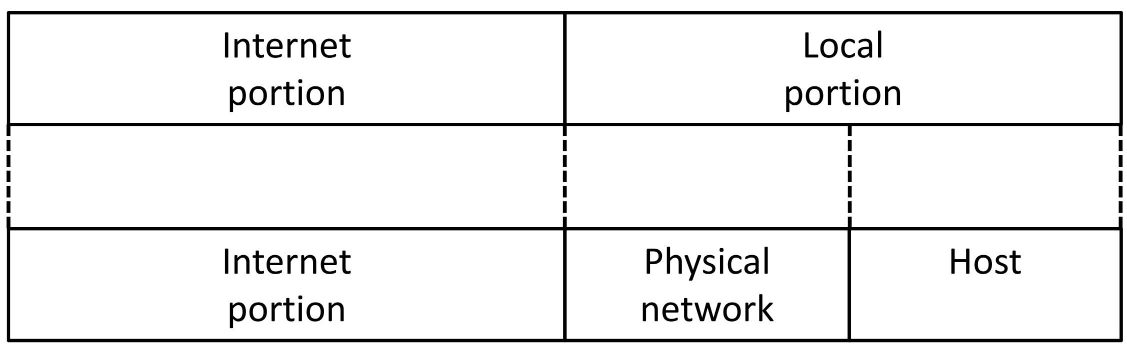
- Subnetting
- Variable-length Subnet Masking (VLSM)
- Network Address Translation (NAT)
- Private IP Address Range
- Classless Inter-Domain Routing (CIDR)
- Transition to IPv6 (long term strategy)

IPv4 – Subnet Addressing/subnetting

- A process of dividing a larger network into smaller, more manageable subnetworks
- Resolve the issue of insufficient network addresses in classful addressing scheme (especially class B) without abandoning the classful addressing scheme.
- Allows a single network prefix to be used for multiple physical networks.
- Help organize networks and reduce broadcast traffic

IPv4 – Subnet Addressing/subnetting

- 32-bit IPv4 address have a internet portion and a local portion
  - Internet portion identifies a site
  - Local portion identifies a physical network and host at that site



IPv4 – Subnet Addressing/subnetting

Purposes:

- Allocate IP addresses more efficiently by reducing wastage, especially in large networks
- Reduces congestion and minimizes excessive broadcast traffic, leading to better network performance
- Isolate certain parts of the network, reducing the risk of unauthorized access and containing security threats

IPv4 – Subnet Addressing/subnetting

- Subnetting imposes a form of hierarchical addressing that leads to hierarchical routing.
- Routers (Internet) use the top level of the hierarchy to forward a packet to the correct site.
- Once the packet enters the site, local routers use the physical network octet to select the correct network.
- When the packet reaches the correct network, a router uses the host portion to identify a particular host.
- Fixed-length subnetting
- Variable-length subnetting

IPv4 – Subnet Addressing/subnetting

- Fixed-length subnetting – a site that choose a division for local portion of its address and then using the division throughout the site.

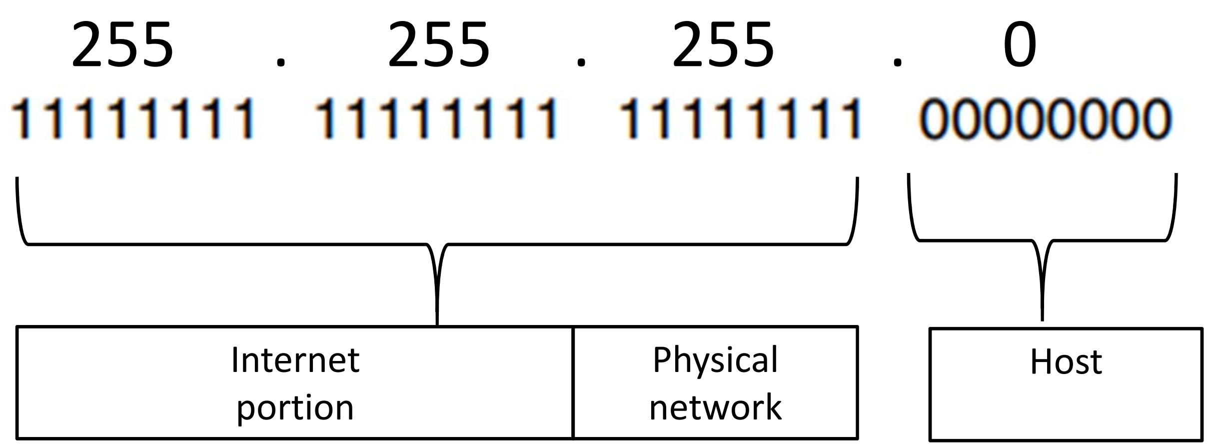
Network Bits	Number of Networks	Hosts per Network
0	1	65534
2	2	16382
3	6	8190
4	14	4094
5	30	2046
6	62	1022
7	126	510
8	254	254
9	510	126
10	1022	62
11	2046	30
12	4094	14
13	8190	6
14	16382	2

IPv4 – Subnet Addressing/subnetting

- Variable-length subnetting - each network will select a subnet partition. Once a partition has been selected for a particular network, it **does not vary over time**.
- Advantage of the variable-length subnetting
  - flexibility of having a mixture of large and small network
  - achieve higher utilization of the address space.
- Disadvantage: difficult to administer – partition for each subnet and the values chosen for subnet numbers must be assigned carefully to avoid address ambiguity – an address is interpreted differently on two physical networks.

IPv4 – Subnet Mask

- A number that looks like an IP address (32 bits) –shows how many bits are used for the network portion and the host portion.
- The mask covers the internet portion and the physical network part of the local portion.
- Bits in the subnet mask are set to 1 for subnet prefix and 0 for host identifier



IPv4 – Subnet Addressing/subnetting

- Network Address Translation (NAT) – a method used in routers to translate private IP addresses used inside a local network into public addresses used on the internet and vice versa.
- Enables multiple devices on a private network to share one public IP address.

IPv4 - Classless Addressing Scheme

- Classless Inter-Domain Routing (CIDR) is an IP addressing scheme that was developed after the classful addressing scheme.
- Introduce in 1993 (RFC 1519)
- Prevent IP address exhaustion of IPv4
- More flexible allocation of IP addresses
- Support route aggregation – reducing routing table sizes

IPv4 - Classless Addressing Scheme

- CIDR addressing still represents IP addresses in the dotted decimal notation but highlights the network portion with a slash followed by a number.
- Eg. `167.199.170.82/27` where `27` indicates the prefix length
- The number after the slash is the number of bits that represent the network portion of the IP address.

IPv4 - Classless Addressing Scheme

- First address: keep the n leftmost bits and set the (32-n) rightmost bits all to 0s
- Last address: keep the n leftmost bits and set the (32-n) rightmost bits all to 1s.
- Eg. Address: 167.199.170.82/27

  10100111 11000111 10101010 01010010

  First /Network Address: 167.199.170.64/27

  10100111 11000111 10101010 01000000

  Last/Boardcast Address: 167.199.170.95/27

  10100111 11000111 10101010 01011111

IPv4 – IP addresses for private network

- The CIDR blocks are reserve for private network and not routable on public internet.
- If a packet containing one of the private addresses is accidentally forwarded onto the global Internet, a router will detect the problem and discard the packet.
- To access the internet, NAT translates the private IP to a public IP.

Prefix	Lowest Address	Highest Address
10.0.0.0 / 8	10.0.0.0	10.255.255.255
172.16.0.0 / 12	172.16.0.0	172.31.255.255
192.168.0.0 / 16	192.168.0.0	192.168.255.255
169.254.0.0 / 16	169.254.0.0	169.254.255.255

- The CIDR block 169.254.0.0/16 is a link-local address. Device will assigns itself an address in the block if it fails to connect to a DHCP server to obtain an IP address automatically.

End