LECTURE 2 - Internet Protocol version 4 (IPv4)

CPSC-456 Network Security Fundamentals

Overview: Networking Concept Review

- A network can be as small as any two devices linked together. Most often when networks get larger, however, they are clearly comprised of relatively smaller networks connected, they are no longer called networks but Internetwork, or Internet for short.

- A *subnetwork* (subnet or subnet ID) is a portion of a network, or a network that is part of a larger internetwork. This term is also a rather subjective one; subnetworks can be rather large when they are part of a network that is very large. *For instance, an IPv4 Class A subnet can be larger than an entire Class B or Class C or both networks combined.*

- A subnet mask is used to divide an IP address into its corresponding network(subnet) ID and host ID. It can be represented in 3 ways - Dotted-decimal notation, binary form, or Classless Inter-Domain Routing (CIDR) notation. Its binary representation is a contiguous ones (network) and zeros (host).

Outline

- Internet Protocol (version 4)
  - Overview
    - Circuit-Switching and Packet-Switching Networks
    - Message Addressing and Transmission Methods
    - TCP/IPv4 Timeline
    - IPv4 Overview
    - Solutions to IPv4 Address Space Exhaustion
  - IPv4 Network
    - Internet Protocol version 4
    - Address Space
    - Private and Special Address Spaces
    - Classful Address Space Limitations
    - Subnetting with CIDR

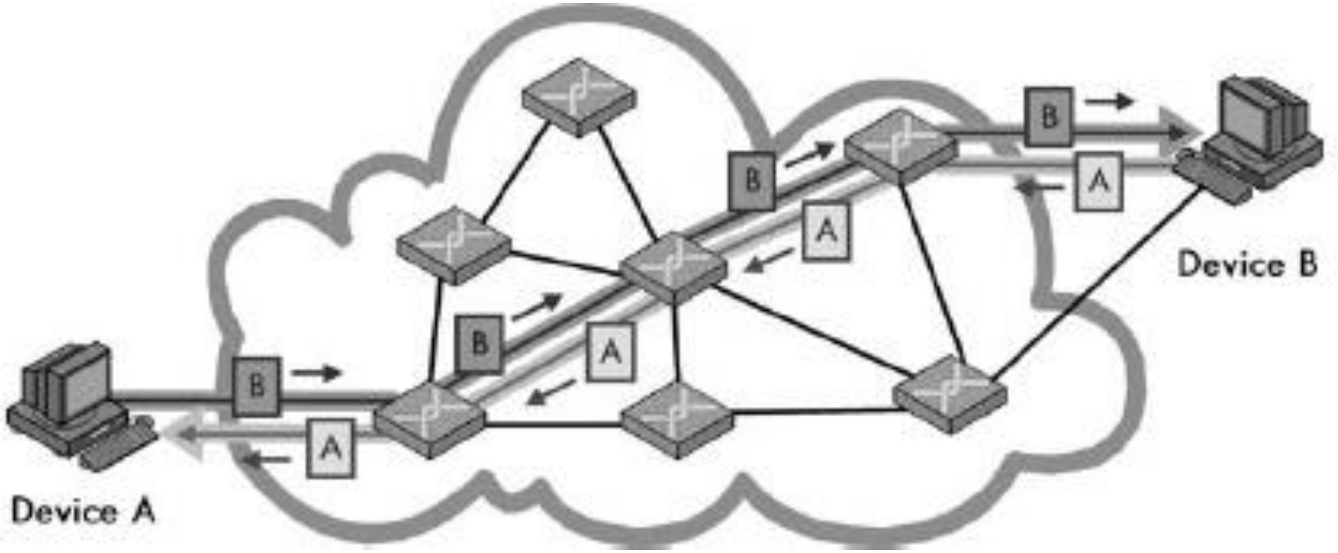
Switching:

- Switching in computer network helps in deciding the best route for data transmission if there are multiple paths available in larger network.

- Types of Switching:
  - Circuit Switching
  - Packet Switching
  - Message Switching

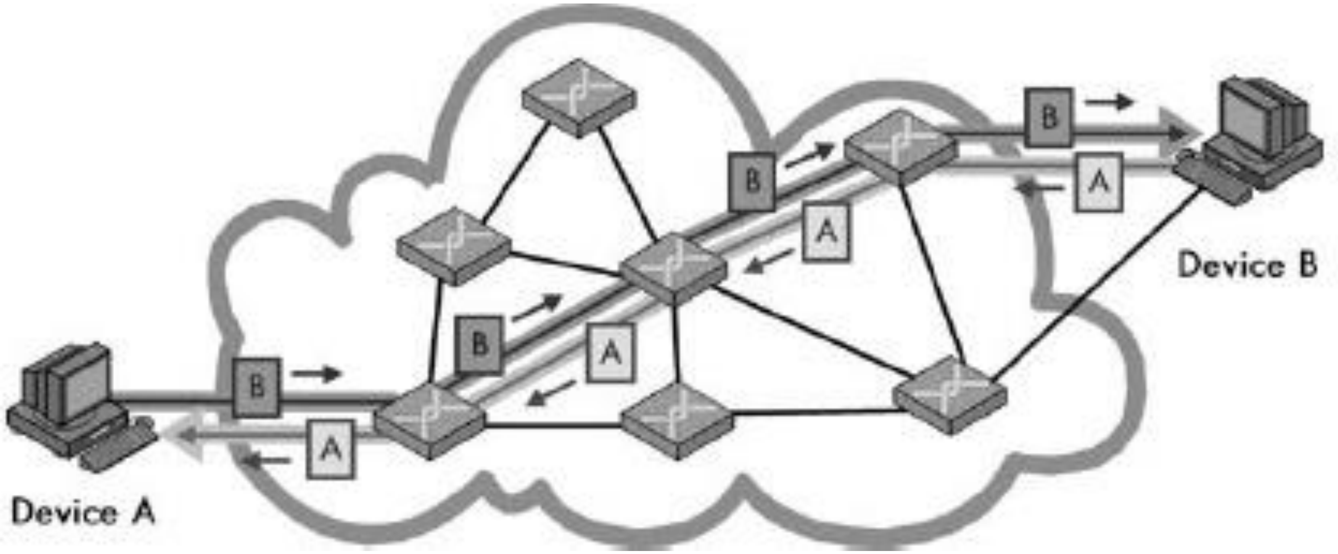
Circuit-Switching and Packet-Switching Networks

- In the *circuit-switching* networking method, a connection called a *circuit*, which is used for the whole communication, is set up between two devices. Information about the nature of the circuit is maintained by the network. The circuit may be either a fixed one that is always present or one that is created on an as-needed basis. Even if many potential paths through intermediate devices may exist between the two devices that are communicating, only one will be used for any given dialogue



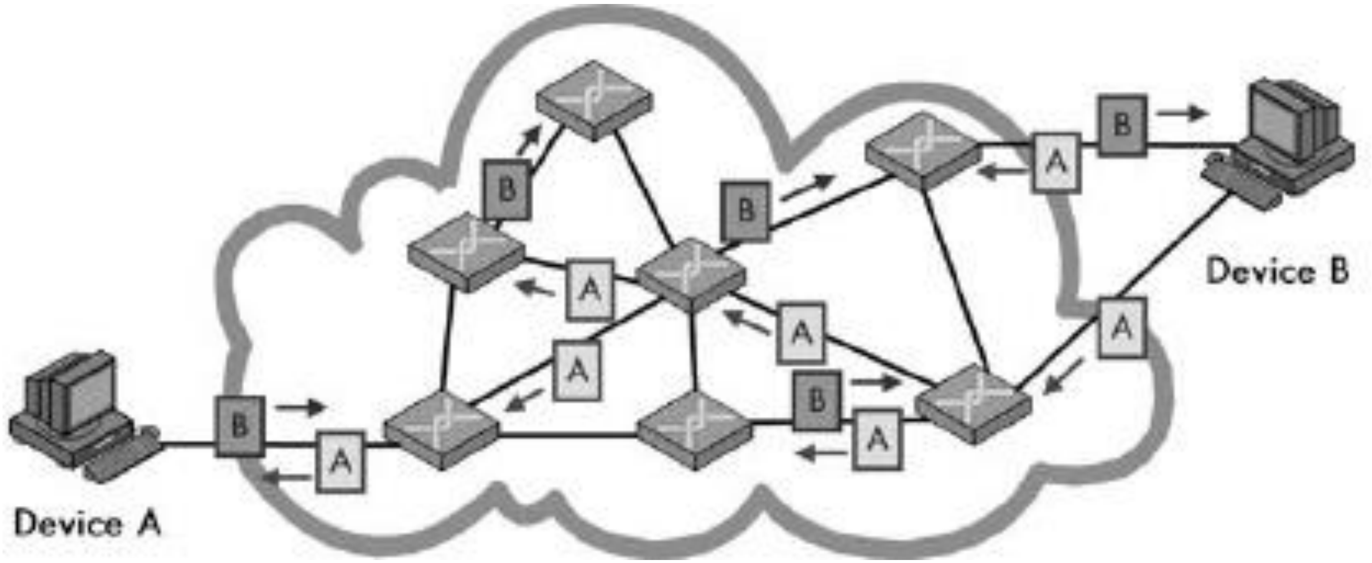
Circuit-Switching and Packet-Switching Networks – Cont'd

- Circuit switching: Before communication can occur between two devices, a circuit is established between them. This is shown as a darker line for the conduit of data from Device A to Device B, and a matching lighter line from B back to A. Once it's set up, all communication between these devices takes place over this circuit, even though there are other possible ways that data could conceivably be passed over the network of devices between them.



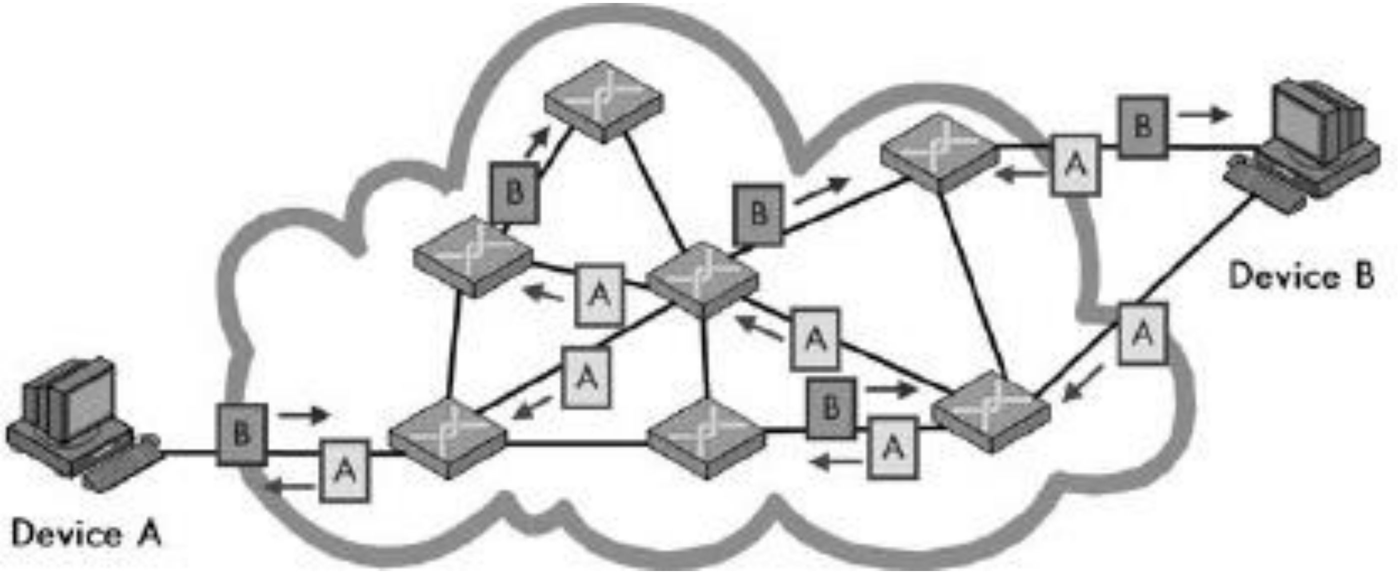
Packet-Switching Networks

- In the *packet-switching* network type, no specific path is used for data transfer. Instead, the data is chopped up into small pieces called *packets* and sent over the network. You can route, combine, or fragment the packets as required to get them to their eventual destination. On the receiving end, the process is reversed — the data is read from the packets and reassembled to form the original data.



Packet-Switching Networks

- Packet switching: In a packet-switched network, no circuit is set up prior to sending data between devices. Blocks of data, even from the same file or communication, may take any number of paths as they journey from one device to another



Packet-Switching Networks

- Packet switching has two approaches:
  - 1.Datagram Approach
  - 2.Virtual Circuit Approach

Packet-Switching Networks

- 1.Datagram Approach

- Datagram packet switching is also known as connectionless switching.
- Each independent entity is called as datagram.
- Datagrams contains destination information and the intermediary devices uses this information to forward datagram to right destination.
- In Datagram approach path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.

Packet-Switching Networks

- 2. Virtual Circuit Approach

- Virtual Circuit Approach is also known as Connection-oriented Switching.
- In the case of virtual circuit switching, a preplanned route is established before the messages are sent.
- In this approach, the path is fixed for the duration of a logical connection.

Message Switching

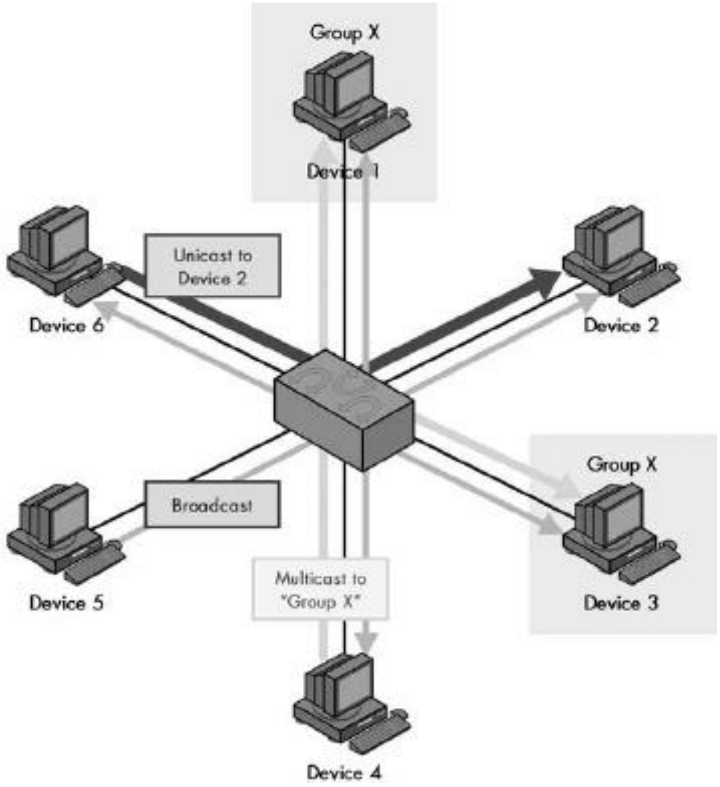
Store and forward Mechanism.

Broadcast Messages Message is transferred as a complete unit and forwarded using store and forward mechanism at the intermediary node.

Not suitable to streaming media and real-time applications

Message Addressing and Transmission Methods – Cont'd

Multicast Messages are sent to a group of stations that meet a particular set of criteria. These stations are usually related to each other in some way. For example, they serve a common function or are set up into a particular *multicast group*. Note that you can also consider broadcast messages to be a special case of multicast in which the group is "everyone."



Overview: TCP/IPv4 Timeline

- The early Internet and TCP/IP were developed together as part of the US DARPA ARPAnet project
- In 1973, a complete internetworking system for the ARPAnet officially began
- December 1974: Request-For-Comment (RFC) 675 for early TCP
- March 1977 : TCP version 2
- 1978 through 1980, TCP/IP version 3 was developed
- In early 1980's, many machines (UNIX) and networks started using TCP/IP version 4 on the ARPAnet

Overview: IPv4 Timeline

- Developed in the early 1980s –IPv4 has 2^{32} address space (~4.29 billion)

- It seemed like a lot of addresses back then... No WWW, no mobile devices, no IoT - mostly mainframe/minicomputers and PCs
  - The World Wide Web (WWW) was introduced in 1990s
  - Internet routing tables growing rapidly -- 20,000 routes in 1994
  - Internet Engineering Task Force (IETF) realized that it would soon run out of IPv4 address space;

    Short-term fixes that became long standing solutions to this day:
    - Network Address Translation (NAT)/Port Address Translation (PAT):
      NAT- Convert a single IPv4 address space into another IPv4 address or network
      PAT - Shared one public IPv4 address among internal LAN devices
    - Private address space: Reusable address space within local area networks (LANs)
    - CIDR: Be able to subdivide or combine networks

Overview: Solutions To IPv4 Address Space Exhaustion

- Network Address Translation (NAT)
  - Convert a single IPv4 address space into another network using static or dynamic mappings

    e.g.: 192.168.1.0/24 <=> 3.12.20.16/29
    192.168.1.2 <=> 3.12.20.20
    192.168.1.6 <=> 3.12.20.21

  - Port Address Translation (PAT)

    One shared public IP address among internal LAN devices

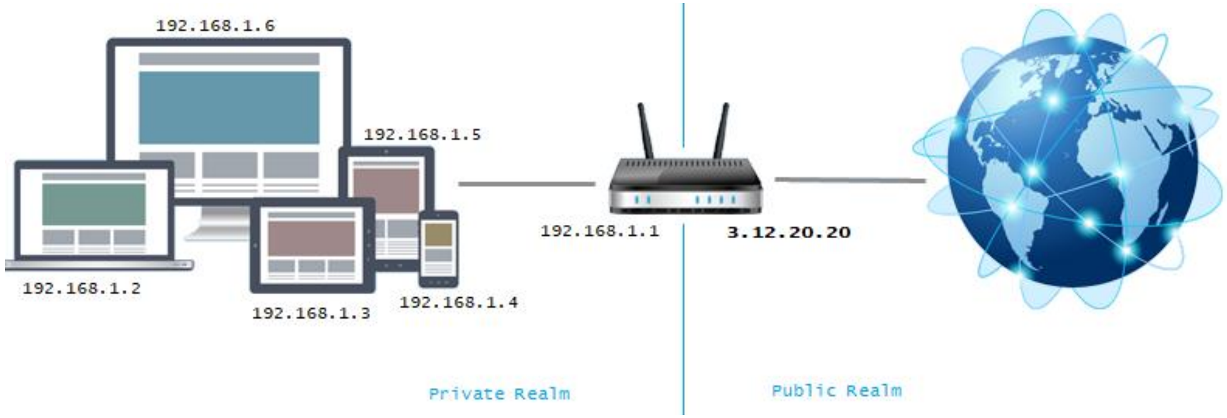
    e.g.:
    192.168.1.2:80 <=> 3.12.20.20:8000
    192.168.1.6:80 <=> 3.12.20.20:8001

- Private Address Space
  - Reusable address space within local area networks (LANs)
  - Hides internal LAN from the outside

    e.g.: 192.168.1.0/24, 10.0.0.0/8

- Classless Inter-Domain Routing (CIDR)
  - Subdivide or combine networks

    e.g.: 137.151.0.0/17 & 172.16.0.0/12

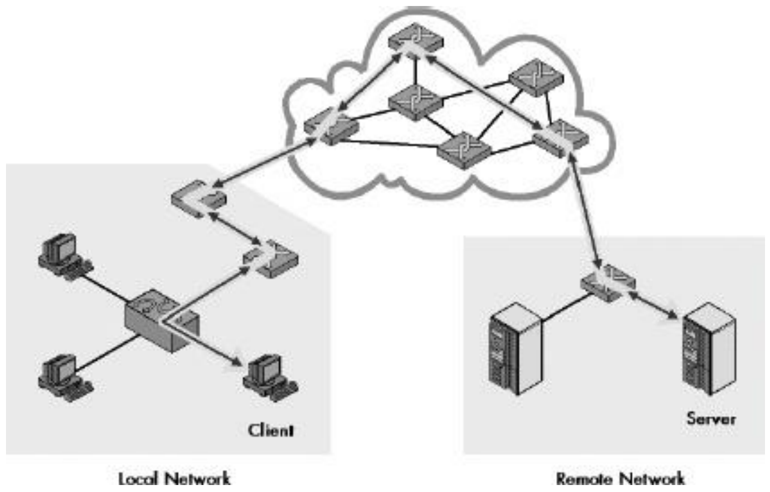


Outline

- Internet Protocol (version 4) Network
  - Overview
    - Networking Concept Review
    - Internet Protocol
    - TCP/IPv4 Timeline
    - IPv4 Timeline
    - Solutions to IPv4 Address Space Exhaustion
  - IPv4
    - Internet Protocol version 4
    - Address Space
    - Private Address Space
    - Classful Address Space Limitations
    - Subnetting with CIDR

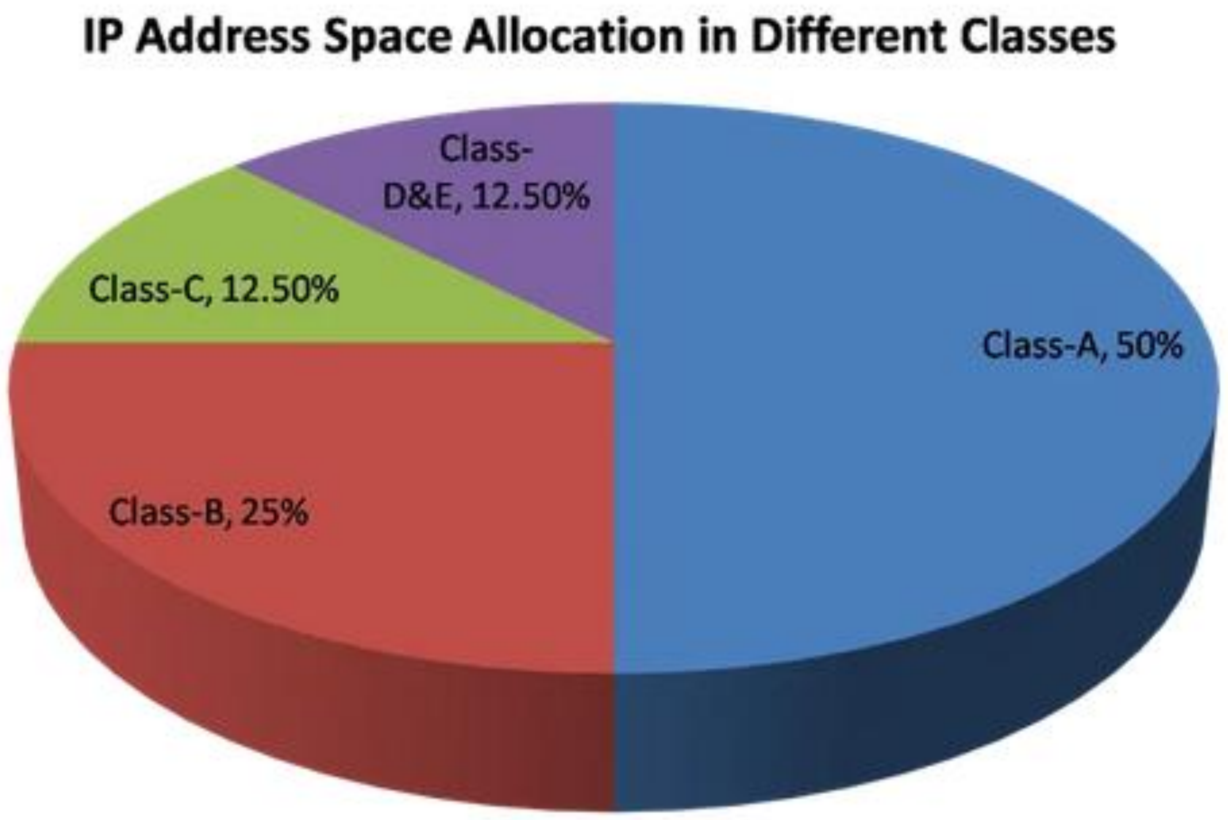
IPv4: Internet Protocol version 4

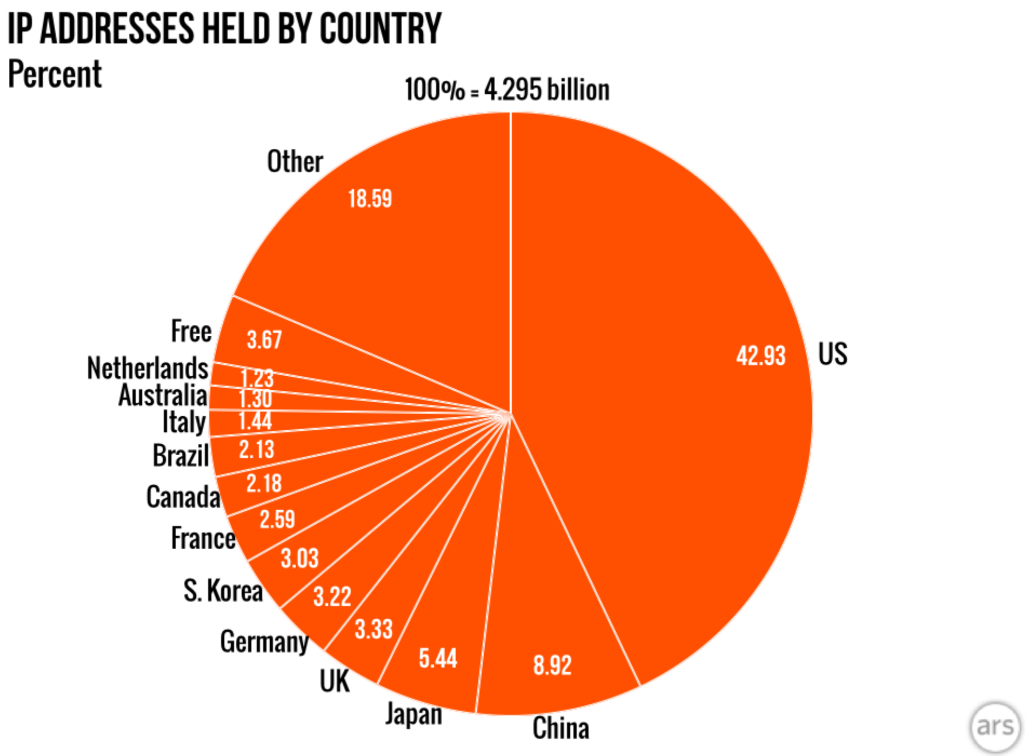
- Internet Protocol is the workhorse of TCP/IP protocol suite.
- IP implements key network layer functions:
    - Addressing (IPv4 & IPv6)
    - Routing datagram through intermediate routers
    - Datagram handling
        - Max Transmission Unit (MTU)
        - Fragmentation and reassembly



- IP sends *datagram* from point A to point B over an internetwork

IPv4: Address Space





IPv4: Conventional (Classful) Address Space

This original IP addressing scheme is set up so that the dividing line occurs only within its predetermined octet boundary (*default subnet mask*). The 3 main classes of addresses (A, B, and C) are differentiated based on how many octets are used for their network ID.

- Class A: Has **8**-bit subnet mask and up to 2^{24} unique IP addresses
- Class B: Has **16-bit** subnet mask and up to 2^{16} unique IP addresses
- Class C: Has **24-bit** subnet mask and up to 2^{8} unique addresses

The **IP address 0.0.0.0** is used as a default IP address placeholder upon connecting to a network. E.g., DHCPDiscover Packet

The **IP address 255.255.255.255** is used as a default broadcast address that the client using the IP address of 0.0.0.0 to discover DHCP server(s) on the current network.

IPv4: Classful Network Breakdown

Class	# of Networks	# of Nodes	Address Range
A (large)	128	16,777,216	0.0.0.0 to 127.255.255.255
B (medium)	16,384	65,536	128.0.0.0 to 191.255.255.255
C (small)	2,097,152	256	192.0.0.0 to 223.255.255.255
D (multicast)	N/A	N/A	224.0.0.0 to 239.255.255.255
E (future use)	N/A	N/A	240.0.0.0 to 255.255.255.255

Class	High Order Bits (First Octet)	Start Address	End Address
Class A	0xxxxxxx	0.0.0.0	127.255.255.255
Class B	10xxxxxx	128.0.0.0	191.255.255.255
Class C	110xxxxx	192.0.0.0	223.255.255.255
Class D	1110xxxx	224.0.0.0	239.255.255.2555
Class E	1111xxxx	240.0.0.0	255.255.255.255

Image source:https://en.wikipedia.org/wiki/File:Data_Networks_classification_by_spatial_scope.png

IPv4: Private and Special Address Spaces

Private IPv4 Address ranges: All private addresses are non-routable in the public domain (i.e., cannot be used outside the private network to an external network)

- Class A: 10.0.0.0/8 (10.0.0.0-10.255.255.255)
- Class B: 172.16.0.0/12 (172.16.0.0-172.31.255.255)
- Class C: 192.168.0.0/16 (192.168.0.0-192.168.255.255)

Special non-routable IPv4 addresses:

- Automatic Private IP Addressing (APIPA): 169.254.0.0/16 (169.254.0.0 to 169.254.255.255)
  Self-assigned IPv4 address and subnet mask when a Dynamic Host Configuration Protocol (DHCP) server is not reachable or available

- Localhost: 127.0.0.0/8 (127.0.0.0– 127.255.255.255)
  The Default IPv4 *home or loopback address* is 127.0.0.1

Image source: https://fineartamerica.com/featured/there-is-no-place-127001-aadil-farooq.html

IPv4: Structure

- 32-bit binary (4 octets)
- Dotted-decimal notation: x.x.x.x (where x has a value between 0 and 255)
- Structure: | Network ID | Host ID |
  - Network ID: prefix of all machines on the network (starting from the leftmost bit)

    How to find the network ID? Perform a **bitwise AND** operation between the IP Address and the subnet mask.

Bitwise AND (&) Truth Table				
	0	0	1	1
	0	1	0	1
	0	0	0	1

  - **Host ID**: The remainder bits to identify the host on the network

    How to find the host ID? Perform a **bitwise XOR** operation between the IP Address and the network ID.

Bitwise XOR (^) Truth Table				
	0	0	1	1
	0	1	0	1
	0	1	1	0

- Subnet Mask is a 32-bit mask that divides the network ID and **host ID**,

  where its binary representation is a **contiguous** 1's (network ID) and 0's (host ID)

  e.g.: 255.0.0.0 or /8 ➡ 11111111.00000000. 00000000. 00000000

IPv4: Structure - Cont'd

8-bit (Octet) To Decimal Conversion (IPv4 Address)								
Bit Positions	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal Values	128	64	32	16	8	4	2	1
8-bit Example	1	0	0	0	0	0	0	1

$\Sigma($ 128 0 0 0 0 0 0 1 $)=129$

Subnet Mask Table	
Decimal	Binary
255	11111111
254	11111110
252	11111100
248	11111000
240	11110000
224	11100000
192	11000000
128	10000000
0	00000000

Ex: Find the network and host IDs of 192.168.1.34/255.255.255.0.

	Address	Binary
IP Address	192.168.1.34	11000000.10101000.00000001.00100100
Subnet Mask	255.255.255.0	11111111.11111111.11111111.00000000
Network ID (IP & SM)	192.168.1.0	11000000.10101000.00000001.00000000
Host ID (IP ^ Net ID)	0.0.0.34	00000000.00000000.00000000.00100100

IPv4: Classful Address Space Limitations

Question: **What are some of the limitations of classful IPv4 addressing?**

- Limited number of network addresses
- Same size host addresses per network
- Mostly result in numerous unused host addresses in a network (particularly larger classes of networks)
- What if there is a need for multiple networks?

How do we solve this issue of network design flexibility?

Solution: *Classless addressing; Subnetting/Supernetting* using CIDR

Additional Benefits:

- Optimize network traffic by making networks smaller
- Reduce the number or routing table entries
- Effectively manage a given network's IP address space

IPv4: Subnetting with CIDR

Subnetting is the process to subdivide a network into multiple subnetworks (subnets) by borrowing subnet mask host bit(s) to be turned into network bit(s).

e.g.: Turn a class B network (137.151.0.0/16) into 4 subnetworks.
137.151.0.0/18 137.151.64.0/18 137.151.128.0/18 137.151.192.0/18

Note: Supernetting is the reverse process of subnetting to combine multiple networks into a bigger network by borrowing subnet mask network bit(s) to be turned into host bit(s). *Mostly used in routing advertisement aggregation on network routers.*

e.g.: Turn multiple networks (192.168.0.0/24 and 192.168.1.0/24) into a bigger network.
192.168.0.0/23

Classless Inter-Domain Routing (CIDR) Notation:

- Prefix a slash to the IP address followed by the total network bits of the subnet mask
  Ex.: 192.168.0.0/255.255.255.128 => 192.168.1.0/25

IPv4: Subnetting with CIDR – Cont'd

Total_Subnets = 2^b (where $b>0$ refers to the borrowed host bit(s) starting from the leftmost bit)

Size_per_Subnet = 2^h (where h refers to the total remaining host bits)

Block_Size = 2^r (where r refers to the number of remaining host bit(s) of the subdivided/interesting octet)

Available_Hosts_per_Subnet = Size_per_Subnet - 2

Why minus 2? Because for every network there two reserved addresses. i.e., Non-assignable addresses that cannot be assigned to hosts

- The first IPv4 address in each ***network address*** or simply **subnet address**. (All host bits are set to 0)
- The last IPv4 address in each subnet is used as its *directed broadcast address*. (All host bits are set to 1)

IPv4: Subnetting with CIDR - Cont'd

Example 1: Create two subnets from the IPv4 network address 192.168.1.0/255.255.255.0. *How many host bit(s) to borrow to create 2 subnets? What is the size of each subnet? List the subnets, available host address ranges, and broadcast addresses.*

Answer: Subnet Mask Prefix Conversion: 255.255.255.0 => /24

Borrow 1 host bit to get 2 subnets

Total_Subnets = $2^b = 2^1 = 2$

After borrowing 1 host bit, the new subnet mask is /25 for both subnets.

Size_per_Subnet = $2^h = 2^{32-25} = 2^7 =$ **128**

Subnets created: 192.168.1.0/25 and 192.168.1.128/25

Subnet/Network Address	Available/Assignable Host Addresses	Broadcast Address
192.168.1.0/25	192.168.1.1-192.168.1.126	192.168.1.127
192.168.1.128/25	192.168.1.129-192.168.1.254	192.168.1.255

IPv4: Subnetting with CIDR – Cont'd

Example 2: Divide the *last* subnet from example 1 to create 4 subnets. How many host bits to borrow? How many available host addresses can be assigned for each subnet? List the 4 subnets.

Answer: The last subnet from example 1: 192.168.1.128/25

Borrow 2 host bits => Total_Subnets = $2^b = 2^2 = 4$

Size_per_Subnet = $2^h = 2^{32-27} = 2^5 =$ **32**

Available_Hosts_per_Subnet = Size_per_Subnet – 2 = 32 – 2 = 30

After borrowing 2 host bits, the new subnet mask is /27 for two subnets.

New Subnet Mask in Dotted-decimal notation: 255.255.255.224

Binary: 11111111.11111111.11111111.11100000

Interesting octet: 4^{th}

Block_Size = $2^r = 2^{7-2} = 2^5 = 32$

Subnets created: 192.168.1.128/27, 192.168.1.160/27, 192.168.1.192/27, and 192.168.1.224/27

IPv4: Subnetting with CIDR – Cont'd

Question: If the *total number of subnets* needed is partial and not divisible by 2^n, how many host bit(s) **must** be borrowed to satisfy such requirement?

Answer: If the total subnets requested is not divisible by 2^n, then borrow additional host bit to accommodate the requirement while adhering to other factors such as required total number of hosts available per subnet.

For example: *If total subnets needed is 3 which is not divisible by 2^n, then 2 host bits must be borrowed to have 2^2 subnets since 2^1 does is not enough to satisfy the requirement. In this example, there will be an extra subnet that can be used in the future.*

References:

TCP/IP Guide, Charles M. Kozierok
TCP/IP Fundamentals, Michael Shannon