Chapter Five : The Network Layer

5.1 Introduction

5.2 Internet Protocol

5.3 IPv4 Subnetting

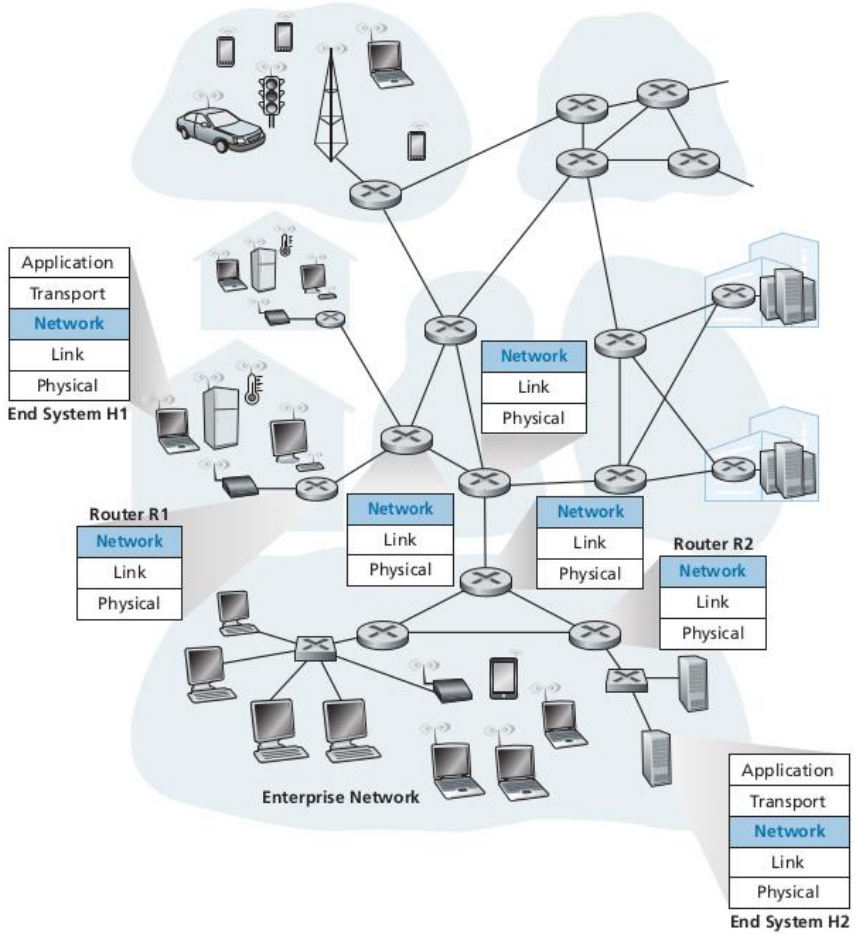
5.4 Routing

Introduction

- transport packet from sending to receiving hosts
- network layer protocols in every host, router

Two important functions:

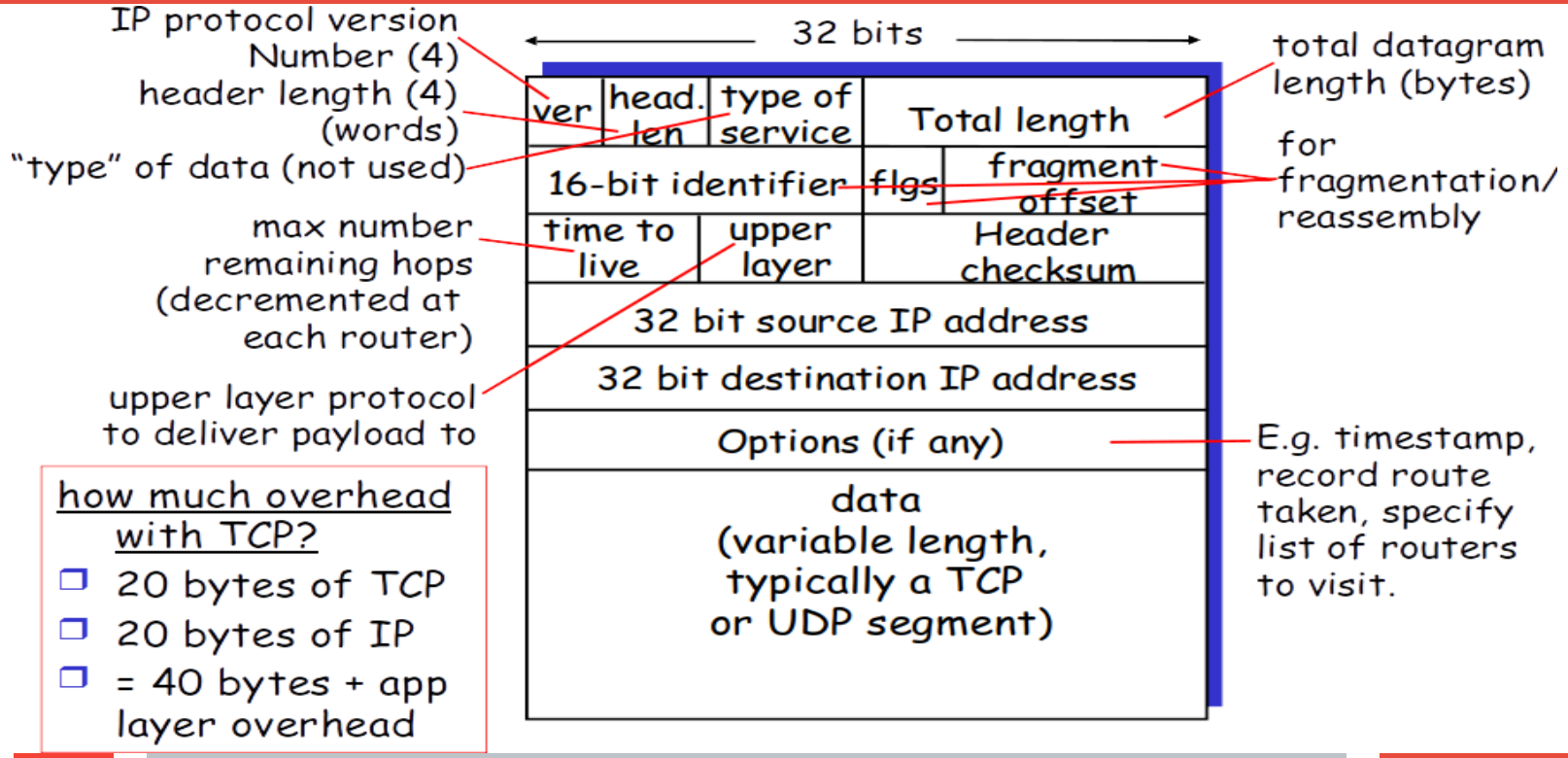
- **path determination**: route taken by packets from source to dest, called routing algorithms
- **forwarding**: move packets from router's input to appropriate router output



Introduction

- The network service model defines the characteristics of end-to-end delivery of packets between sending and receiving hosts
- Possible services that the network layer could provide:
  - Guaranteed delivery
  - Guaranteed delivery with bounded delay
  - In-order packet delivery
  - Guaranteed minimal bandwidth
  - Security
- The Internet's network layer provides a single service, known as **best-effort service**
  - No guarantee of order
  - No guarantee of delivery
  - No guarantee of bandwidth

Internet Protocol: IPv4 Datagram



how much overhead with TCP?

- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

Internet Protocol: IPv4 Datagram

- Version field
  - keeps track of which version of the protocol the datagram belongs to.
  - By including the version in each datagram, with some machines running the old version and others running the new one
  - IPv4 or IPv6
- Header Length
  - is provided to tell how long the header is, in 32-bit words.
  - minimum value is 5, which applies when no options are present.
  - maximum value of this 4-bit field is 15, which limits the header to 60 bytes, and thus the Options field to 40 bytes

Internet Protocol: IPv4 Datagram

- Type of service
  - It was and is still intended to distinguish between different classes of service.
  - Various combinations of reliability and speed are possible.
  - For digitized voice, fast delivery beats accurate delivery.
  - For file transfer, error-free transmission is more important than fast transmission
- Total length
  - includes everything in the datagram—both header and data.
  - The maximum length is 65,535 bytes.
  - At present, this upper limit is tolerable, but with future gigabit networks, larger datagrams may be needed
- Identification field
  - is needed to allow the destination host to determine which datagram a newly arrived fragment belongs to.
  - All the fragments of a datagram contain the same Identification value

Internet Protocol: IPv4 Datagram

- Fragment offset
  - tells where in the current datagram this fragment belongs.
  - All fragments except the last one in a datagram must be a multiple of 8 bytes, the elementary fragment unit.
  - Since 13 bits are provided, there is a maximum of 8192 fragments per datagram, giving a maximum datagram length of 65,536 bytes, one more than the Total length field
- Flags
  - Contains an unused bit followed by two 1-bit fields.
  - The fist bit (DF) stands for Don't Fragment. It is an order to the routers not to fragment the datagram because the destination is incapable of putting the pieces back together again.
  - The second bit (MF) stands for More Fragments. All fragments except the last one have this bit set. It is needed to know when all fragments of a datagram have arrived.

Internet Protocol: IPv4 Datagram

- Time to live (TTL):
  - is a counter used to limit packet lifetimes.
  - It is supposed to count time in seconds, allowing a maximum lifetime of 255 sec.
  - it must be decremented on each hop and is supposed to be decremented multiple times when queued for a long time in a router.
  - in practice, it just counts hops. When it hits zero, the packet is discarded
- Header checksum:
  - verifies the header only.
  - useful for detecting errors generated by bad memory words inside a router
- The Source and Destination IP addresses:
  - indicate the network number and host number of sender and receiver
- Options:
  - was designed to provide an escape to allow subsequent versions of the protocol to include information not present in the original design

Internet Protocol: IPv4 Address

- An IP address is a 32 bit value that contains both a network identifier and a host identifier.
- if the pc connected to NICS or NIC and Modem the pc may have two IP address .
- In LAN if the server is connected to internet, the server act as a Router.
- A hardware address is the code which is hard coded on the Network interface card

Internet Protocol: IPv4 Address

Static

- Addressing info doesn't change – "hard-coded"
- Needs to be configured manually
- Can't be used by any other device – "sharing" is not allowed
- Easy to make a mistake when entering
- Labor-intensive to change/update

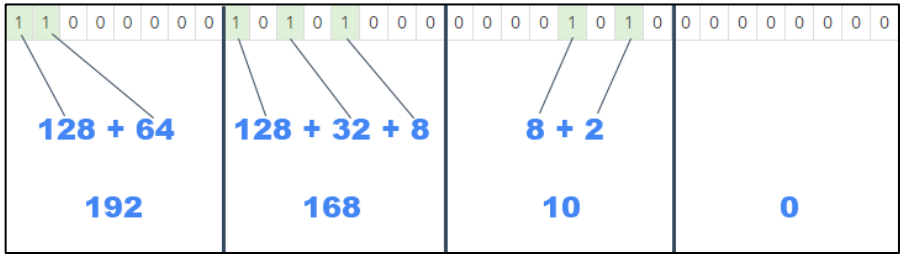
Dynamic

- Addressing info can change dynamically
- Not configured manually
- IP addresses can be "shared" – IP address pool
- Easy to make changes/updates
- Avoid manual configurations and errors
- DHCP - DYNAMIC HOST Configuration Protocol
- DHCP server is installed and address ranges (pools) are configured
- Clients are configured for dynamic addressing

Internet Protocol: IPv4 Address

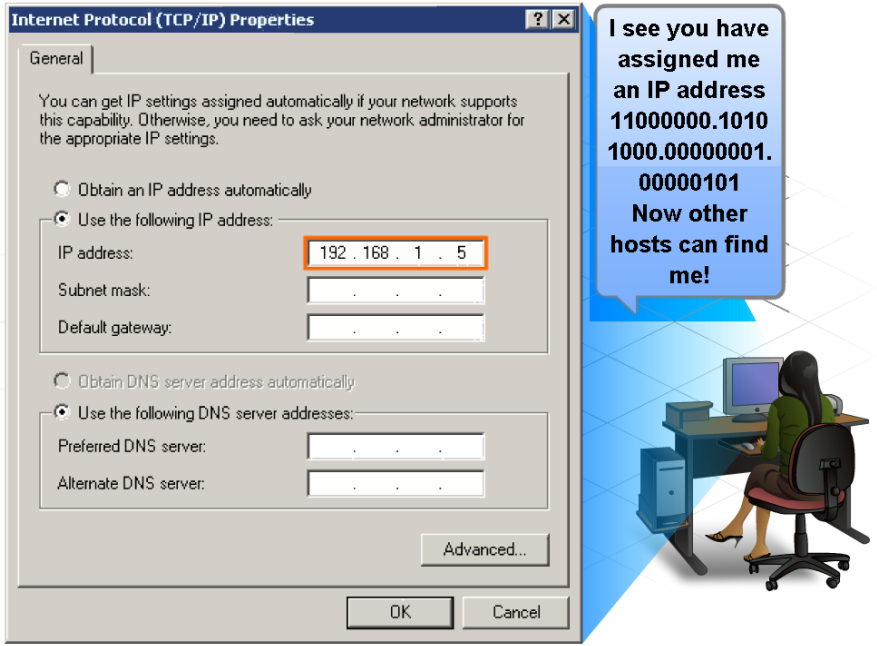
	Octet - 1	Octet - 2	Octet - 3	Octet - 4
In Binary	11000000	10101000	00001010	00000001
	8 bits	8 bits	8 bits	8 bits
In Decimal	192	168	10	1
	Total 32 bits			

Binary Conversion Table								
Bit Position	8	7	6	5	4	3	2	1
Bit Value	1	1	1	1	1	1	1	1
Decimal Value (2^n, start at 0)	128	64	32	16	8	4	2	1
		128÷2 = 64	64÷2 =32	32÷2 =16	16÷2 =8	8÷2 =4	4÷2 =2	2÷2 =1



Internet Protocol: IPv4 Address

- An IP datagram carries 32-bit source and destination addresses, each of which is partitioned into two parts
  - a constituent network prefix
  - a host number on that network.
  - All NICS on the same subnet (LAN) have the same network identifier but different host identifier



IP version 4 (IPv4) is the current form of addressing used on the Internet.

Internet Protocol: IPv4 Address

- IP address has two parts
  - Network identifier
  - Host identifier address

192.	168.	1.	101
255.	255.	255.	0

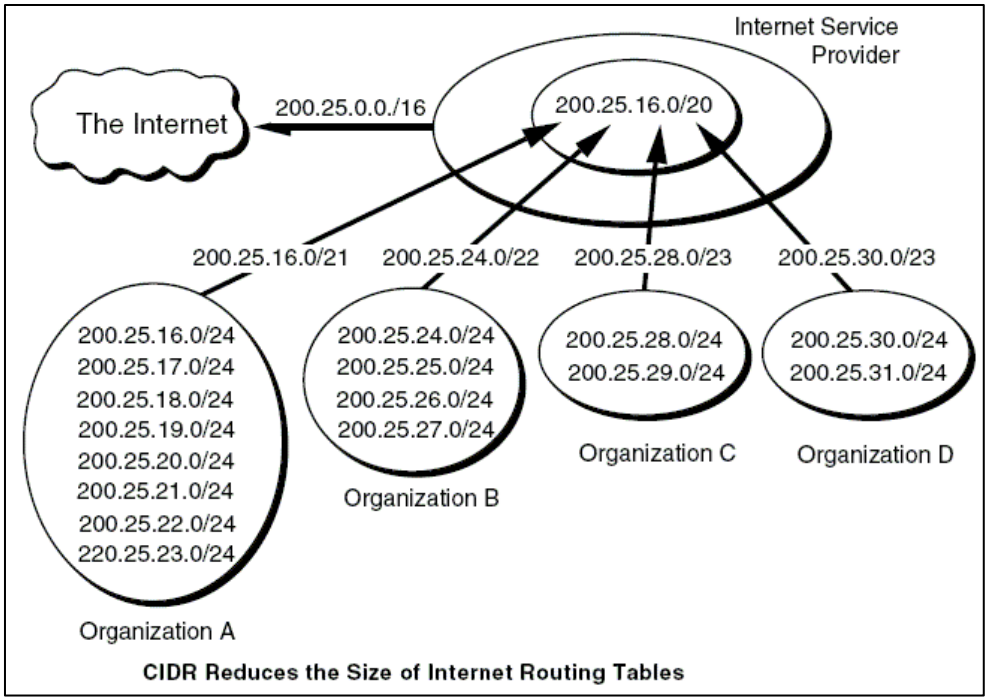
192.168.1.0 = network address
192.168.1.101 = host address .1 - .254
192.168.1.255 = broadcast address
255.255.255.0 = network mask
192.168.1.101 /24 = slash syntax

IP-address ::= {<Network-number>, <Host-number>}

IP-address ::= {<Network-number>, <Subnet-number>, <Host-number> }

Internet Protocol: IPv4 Address

- For the systems that are on the internet , the network identifiers are assigned by a body called THE INTERNET ASSIGNED NUMBER AUTHORITY(IANA)
- ISP - Internet Service Providers will get free IP addresses from IANA to distribute for their customers



CIDR Reduces the Size of Internet Routing Tables

Internet Protocol: IPv4 Address

- A network host uses the network ID and host ID to determine which packets it should receive or ignore and to determine the scope of its transmissions (only nodes with the same network ID accept each other's IP-level broadcasts).
- Because the sender's IP address is included in every outgoing IP packet, it is useful for the receiving computer system to derive the originating network ID and host ID from the IP address field.
- This task is done by using subnet masks

Internet Protocol: IPv4 Address

- Registered IP address are required for computers that are accessible from the Internet , but not by every computer that is connected to the Internet .
- For security reason, networks typically use a firewall or some other technology to protect their system from intrusion by outside computers .
- These firewalls use various techniques that provide workstations with access the Internet resources without making them accessible to other systems on the Internet.

Internet Protocol: IPv4 Address

- IP addresses are divided into 5 classes, each of which is designated with the alphabetic letters A to E.
- Class D addresses are used for multicasting.
- Class E addresses are reserved for testing & some mysterious future use.

Internet Protocol: IPv4 Address

- The Internet community has defined address *classes* to accommodate networks of varying sizes.
- The table on next slide summarizes the relationship between the first octet of a given address and its network ID and host ID fields.
- It also identifies the total number of network IDs and host IDs for each address class that participates in the Internet addressing scheme.
- This sample uses w.x.y.z to designate the bytes of the IP address

Internet Protocol: IPv4 Address

Class	w	Network ID	Host	Available networks	Available hosts
A	1–126	w	x.y.z	126	16,777,214
B	128–191	w.x	y.z	16,384	65,534
C	192–223	w.x.y	z	2,097,151	254

w.x.y.z

Class	Left-most Bit	Starting IP Address	Last IP Address
A	0xxx	0.0.0.0	127.255.255.255
B	10xx	128.0.0.0	191.255.255.255
C	110x	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

1. In which class is found the following IP address ?
   193.25.23.26

   ANS :- class C

1. In which class is the IP address
   115.25.68.156?

   ANS:- class A

AAiT
ADDIS ABABA INSTITUTE OF TECHNOLOGY
አዲስ አበባ ቴክኖሎጂ ኢንስቲትዩት
ADDIS ABABA UNIVERSITY
አዲስ አበባ ዩኒቨርሲቲ

IPv4 Subnetting

- An IP address has 2 parts:
  - The Network identification.
  - The Host identification.
- Frequently, the Network & Host portions of the address need to be separately extracted.
- In most cases, if you know the address class, it's easy to separate the 2 portions.
- With the rapid growth of the internet & the ever-increasing demand for new addresses, the standard address class structure has been expanded by borrowing bits from the Host portion to allow for more Networks.
- Under this addressing scheme, called Subnetting, separating the Network & Host requires a special process called Subnet Masking.

IPv4 Subnetting

- With the rapid growth of the internet & the ever-increasing demand for new addresses, the standard address class structure has been expanded by borrowing bits from the Host portion to allow for more Networks.
- Under this addressing scheme, called Subnetting, separating the Network & Host requires a special process called Subnet Masking.

IPv4 Subnetting

- The subnet masking process was developed to identify & extract the Network part of the address.
- A subnet mask, which contains a binary bit pattern of ones & zeros, is applied to an address to determine whether the address is on the local Network.
- If it is not, the process of routing it to an outside network begins.
- The function of a subnet mask is to determine whether an IP address exists on the local network or whether it must be routed outside the local network.

IPv4 Subnetting

- It is applied to a message's destination address to extract the network address.
- If the extracted network address matches the local network ID, the destination is located on the local network.

Default Subnet Masks	
Address Class	**Subnet Mask**
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

IPv4 Subnetting

- Subnetting reduces the size of the routing tables stored in routers.
- Subnetting extends the existing IP address base & restructures the IP address.
- As a result, routers must have a way to extract from a IP address both the Network address & the Host address.

IPv4 Subnetting

Decimal		Binary
IP Address	123.123.123.001	01111011.01111011.01111011.00000001
Subnet Mask	255.0.0.0	11111111.00000000.00000000.00000000
Network ID	123.0.0.0	01111011.00000000.00000000.00000000

- In the above example, the default Class A subnet mask (255.0.0.0) is AND'd with the Class A address (123.123.123.001) using Boolean Algebra, which results in the Network ID (123.0.0.0) being revealed.
- The default Class B subnet mask (255.255.0.0) strips out the 16-bit network ID
- The default Class C subnet mask (255.255.255.0) strips out the 24-bit network ID.

IPv4 Subnetting

Using the subnet mask to determine the network address for host 172.16.132.70/20

Convert binary network address to decimal

Host Address	172	16	132	70
Binary Host Address	10101100	00010000	10000100	01000110
Binary Subnet Mask	11111111	11111111	11110000	00000000
Binary Network Address	10101100	00010000	10000000	00000000
Network Address	172	16	128	0

IPv4 Subnetting

- Subnetting, a subnet & a subnet mask are all different.
- In fact, the 1st creates the 2nd & is identified by the 3rd.
- Subnetting is the process of dividing a network & its IP addresses into segments, each of which is called a subnetwork or subnet.
- The subnet mask is the 32-bit number that the router uses to cover up the network address to show which bits are being used to identify the subnet.
- A network has its own unique address, such as a Class B network with the address 172.20.0.0 which has all zeroes in the host portion of the address.
- From the basic definitions of a Class B network & the default Class B subnet mask, you know that this network can be created as a single network that contains 65,534 individual hosts.

IPv4 Subnetting

- Example of subnetting: when the network administrator divides the 172.20.0.0 network?
- We have to know how many bit should we borrow from the host number .
- .i.e. $2^x>5$ when x is the minimum possible value .
- X should be 3 , there for…….

IPv4 Subnetting

- The key concept in subnetting is borrowing bits from the host portion of the network to create a subnetwork.
- Rules govern this borrowing, ensuring that some bits are left for a Host ID.
- The rules require that two bits remain available to use for the Host ID& that all of the subnet bits cannot be all 1s or 0s at the same time.
- How many subnets can be created in 192.168.1.0 with each subnet having at least 5 hosts?

IPv4 Subnetting

How to create subnets:

- By using one or more of the host bits as network bits.
- This is done by extending the mask to borrow some of the bits from the host portion of the address to create additional network bits
- For each bit borrowed, we double the number of sub networks available.
- For example, if we borrow 1 bit, we can define 2 subnets, If we borrow 2 bits, we can have 4 subnets.

Example: if we borrow one bit

11111111.11111111.11111111.00000000 – Subnet 1
11111111.11111111.11111111.10000000 -- Subnet 2

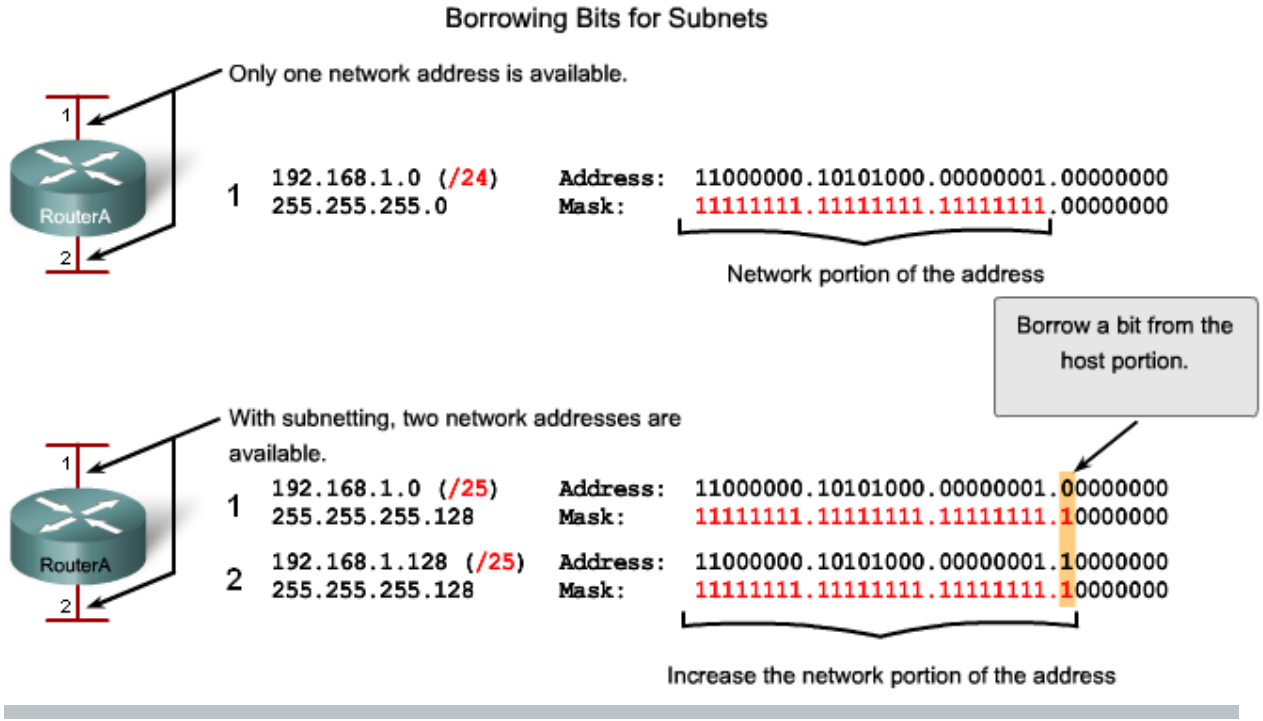
If we borrow two bit

11111111.11111111.11111111.00000000 – Subnet 1
11111111.11111111.11111111.01000000 -- Subnet 2
11111111.11111111.11111111.10000000 – Subnet 3
11111111.11111111.11111111.11000000 -- Subnet4

- However, with each bit we borrow, fewer host addresses are available per subnet

IPv4 Subnetting

RouterA in the figure has two interfaces to interconnect two networks. Given an address block of 192.168.1.0 /24, we need to create two subnets.



IPv4 Subnetting

Given an address block of 192.168.1.0 /24, we need to create two subnets.

- We borrow one bit from the host portion by using a subnet mask of 255.255.255.128, instead of the original 255.255.255.0 mask.
- The most significant bit in the last octet is used to distinguish between the two subnets.
- For one of the subnets, this bit is a "0" and for the other subnet this bit is a "1".

- Formula for calculating *subnets we can create by borrowing bits of host address*
  - 2^n where n = the number of bits borrowed
  - In this example, the calculation looks like this:
  - 2^1 = 2 subnets

IPv4 Subnetting

Formula for calculating the number of *hosts in the subnet*

- 2^n - 2 where n = the number of bits left for hosts
- Applying this formula, (2^7 - 2 = 126) shows that each of these subnets can have 126 hosts.
- For each subnet, examine the last octet in binary. The values in these octets for the two networks are:
  - Subnet 1: 00000000 = 0
  - Subnet 2: 10000000 = 128

- See the figure for the addressing scheme for these networks

Addressing Scheme: Example of 2 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/25	192.168.1.1 – 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 – 192.168.1.254	192.168.1.255

IPv4 Subnetting

Example 2: consider an internetwork that requires three subnets.

- Again we start with the same 192.168.1.0 /24 address block.
  - Borrowing a single bit would only provide two subnets.
  - To provide more networks, we change the subnet mask to 255.255.255.192 and borrow two bits. This will provide four subnets.

Calculate the subnet : 2^2 = 4 subnets

calculate the number of hosts, begin by examining the last octet:

Subnet 0: 0 = 00000000

Subnet 1: 64 = 01000000

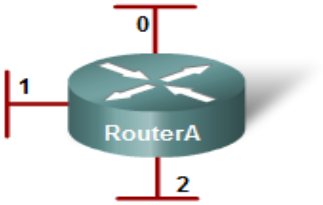
Subnet 2: 128 = 10000000

Subnet 3: 192 = 11000000

Apply the host calculation formula:

2^6 - 2 = 62 hosts per subnet

IPv4 Subnetting



Borrowing Bits for Subnets

-	192.168.1.0 (/24) 255.255.255.0	Address: Mask:	11000000.10101000.00010100.00000000 11111111.11111111.11111111.00000000
0	192.168.1.0 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.00000000 11111111.11111111.11111111.11000000
1	192.168.1.64 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.01000000 11111111.11111111.11111111.11000000
2	192.168.1.128 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.10000000 11111111.11111111.11111111.11000000
3	192.168.1.192 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.11000000 11111111.11111111.11111111.11000000

Two bits are borrowed to provide four subnets.

Unused address in this example.

A 1 in these positions in the mask means that these values are part of the network address.

IPv4 Subnetting

- Addressing scheme for the subnetted networks.

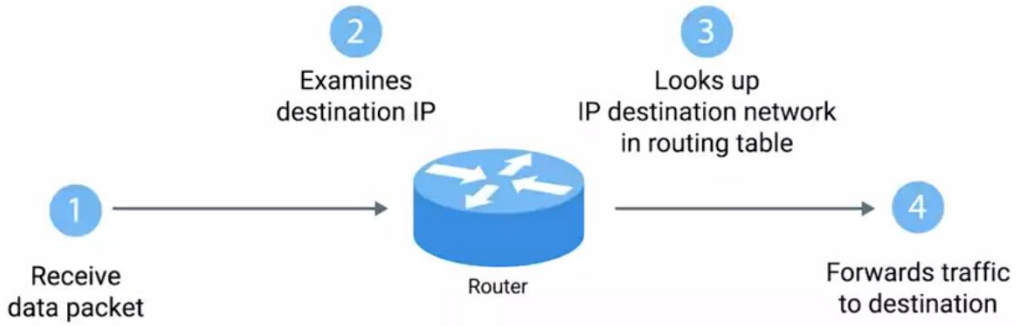
Addressing Scheme: Example of 4 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Routing

Router

- A networking device that forwards traffic depending on the destination address of the traffic
  - Determines the next network point to which a packet should be forwarded toward its destination
- Allow different networks to communicate with each other
- Has at least two interfaces



Routing

Router

- A packet will travel through a number of network points with routers before arriving at its destination
- Every router uses a **routing table** to make decisions where to send packets
  - The **routing table** contains a set of **routes**, where each **route** describes which gateway or interface the router needs to use to reach a specified network
- A **route** has four main components
  - Destination network address
  - Mask
  - Gateway or interface address
  - Route cost or metric
- To direct a message to the correct destination
  - The router looks at the destination IP address in the packet and then looks for a matching route in the routing table

Routing

Router

- In order for the router to determine if it has a route to the destination IP address in its table, it must first find out which bits represent the destination network address
  - The router looks up the **subnet mask** assigned to each potential route in the table
  - The router applies each subnet mask to the destination IP address in the packet
  - The resulting network address is then compared to the network address of the route in the table
  - If a match is found, the packet is forwarded out the correct interface, or to the appropriate gateway

Routing

Routing Protocol

- A set of rules used by the routers to speak to each other
- Used to facilitate the exchange of routing information between routers and populate the routing table with the routing protocol's choice of best paths
- The purpose of a routing protocol includes
  - Discovering remote networks
  - Maintaining up-to-date routing information
  - Choosing the best path to destination networks
  - Having the ability to find a new best path if the current path is no longer available

Routing

The components of a routing protocol

- **Data structures**: - Some routing protocols use tables or databases for their operations - This information is kept in **RAM**
- **Algorithm**: - Routing protocols use algorithms for processing routing information and for best-path determination
- **Routing protocol messages**: - Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and do other tasks to learn and maintain accurate information about the network

Routing Protocols

- All routing protocols have the same purpose:
  - To learn about remote networks
  - To quickly adapt whenever there is a change in the topology
- A router can learn about remote networks in one of two ways:
  - Statically/Manually - Remote networks are manually entered into the route table using static routes
  - Dynamically - Remote routes are automatically learned using a dynamic routing protocol

Routing Protocols: Static

- When an administrator manually assigns the path from source to destination network

Advantage

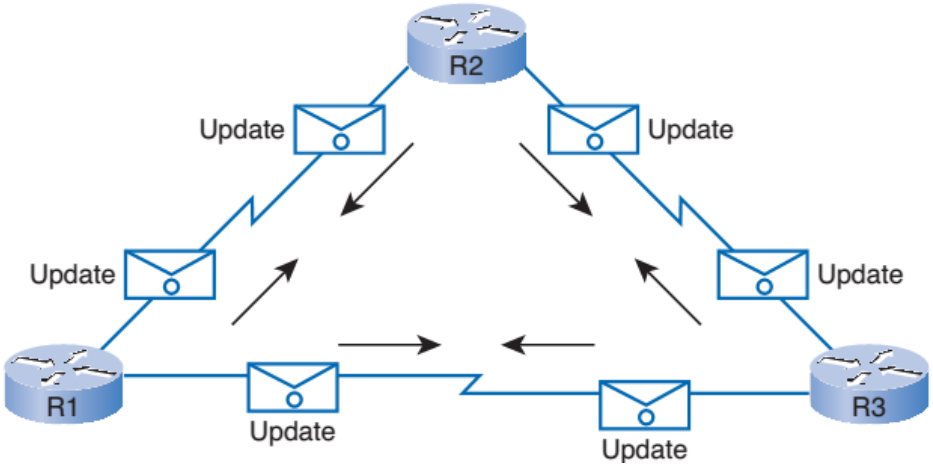
- No overhead on router CPU - Minimal CPU processing
- No bandwidth usage between links
- Easier for administrator to understand and configure
- Provide more security to the network (only administrator add routes)

Disadvantages

- Configuration and maintenance are time-consuming
- Not practical on large networks as it is time intensive
- Administrator intervention is required to maintain changing route info
- When a link fail in the internetwork all the network goes down
- Does not scale well with growing networks

Routing Protocols: Dynamic

- Allow routers to dynamically learn information about remote networks and automatically add this information to their own routing tables
  - Routers exchange routing information whenever there is a topology change
  - This allows routers to find alternate paths if there is a link failure to a current network



Dynamic Routing Protocols

Advantages

- Less work in maintaining the configuration when adding and deleting networks
- Automatically react to the topology changes
- More scalable
- Configuration is less error-prone

Disadvantages

- Router resources are used including CPU time, network link bandwidth and memory
- More administrative knowledge is required for configuration

Feature	Dynamic Routing	Static Routing
Configuration complexity	Generally independent of the network size	Increases with network size
Required administrator knowledge	Advanced knowledge required	No extra knowledge required
Topology changes	Automatically adapts to topology changes	Administrator intervention required
Scaling	Suitable for simple and complex topologies	Suitable for simple topologies
Security	Less secure	More secure
Resource usage	Uses CPU, memory, and link bandwidth	No extra resources needed
Predictability	Route depends on the current topology	Route to destination is always the same

END.