Computer Networks (CIE 447)

Lab 5 : Network layer layer-Static Routing

Dr. Samy Soliman

T. A. :Eng. Menna Mohamed , Eng. Nourhan Tarek

Last Time we talked about:

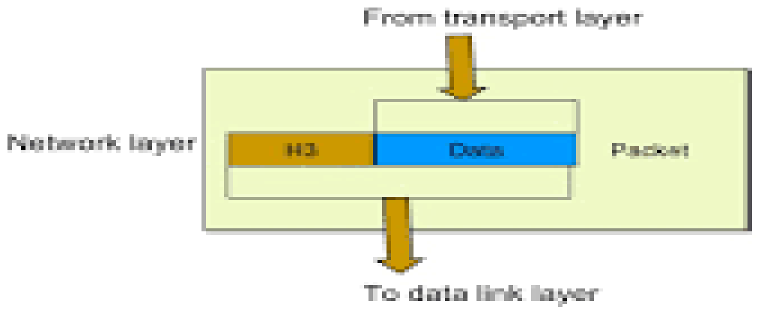
- *Data link layer*
- *Ethernet frame*
- *MAC addresses*
- *Address Resolution Protocol(ARP)*
- *Wireshark(lab)*
- *Packet tracer (Lab)*

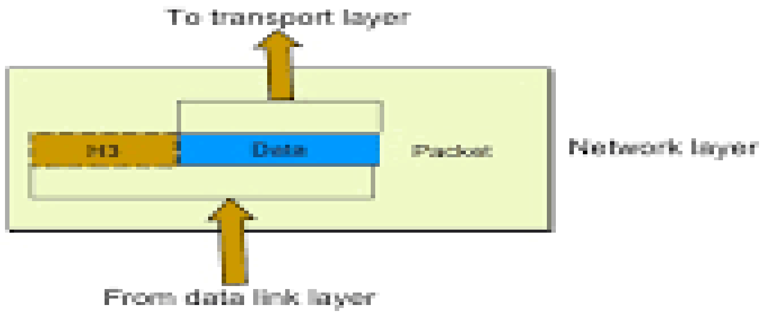
Today
we are talking about:

- *Network layer*
- *IP Orientation*
- *IPV4*
- *Subnetting*
- *ICMP*
- *Static IP*
- *Directly connected subnets*
- *Static routing*
- *Lab Experiment*

Network layer

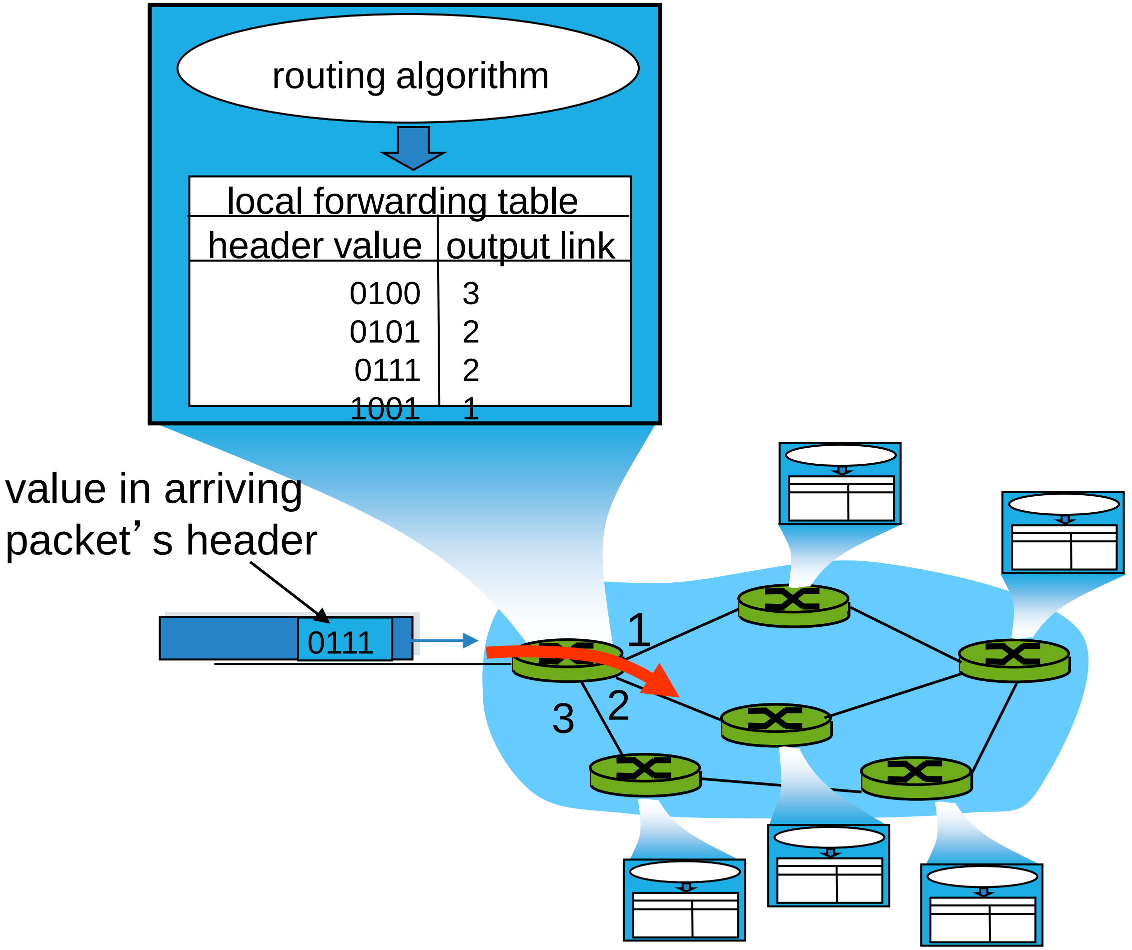
- The network layer is the third level of the Open Systems Interconnection Model (OSI Model)
- the layer that provides data routing paths for network communication.
- network layer protocols in *every* host, router
- Data is transferred in the form of packets via logical network paths in an ordered format controlled by the network layer.
- on sending side encapsulates segments into datagrams
- on receiving side, delivers segments to transport layer





Two key network-layer functions

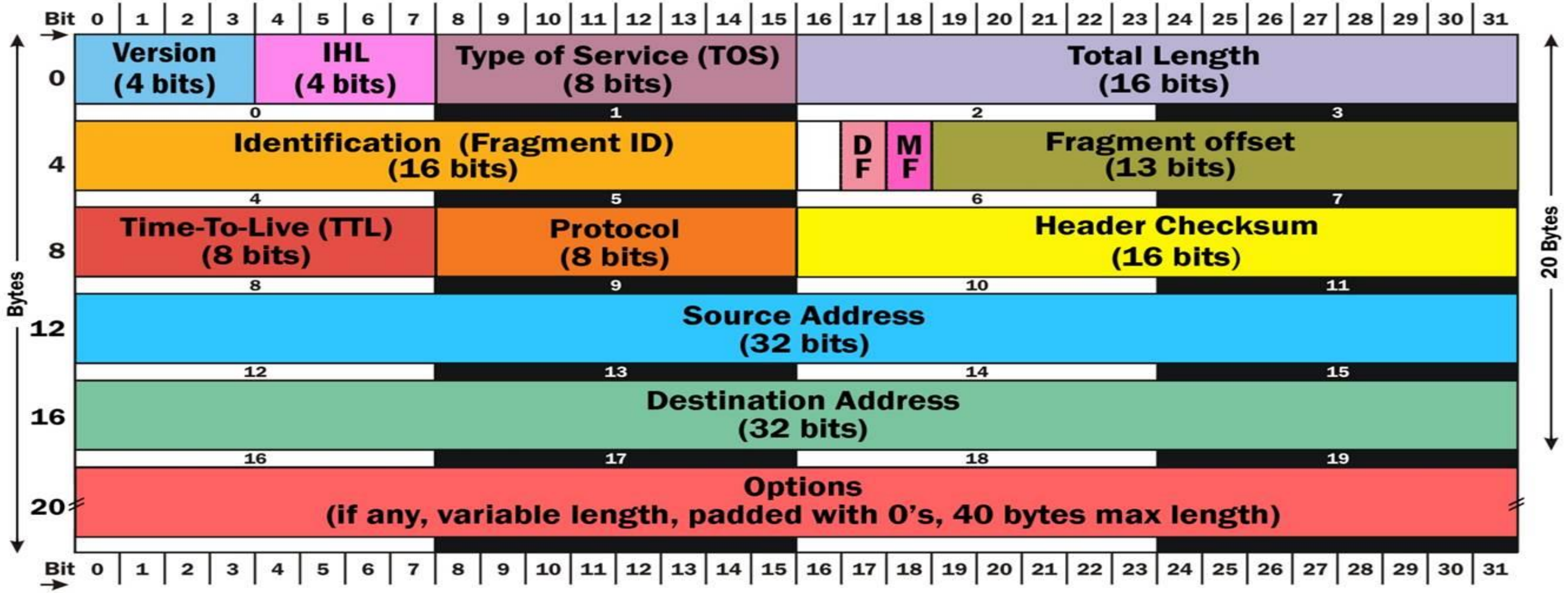
- ***forwarding***: move packets from router's input to appropriate router output.
- ***routing***: determines end-end-path through network.
  - *routing algorithms*



Internet protocol IP

- The Internet Protocol (IP) is a network-layer (Layer 3) protocol.
  - Contains addressing information and some control information that enables packets to be routed.
- IP is documented in **RFC 791** and is the primary network-layer protocol in the Internet protocol suite.
- IP has two primary responsibilities:
  - providing connectionless, best-effort delivery of datagrams through an internetwork
  - providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes

IP Header



Bit 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
0
Version (4 bits)
IHL (4 bits)
Type of Service (TOS) (8 bits)
Total Length (16 bits)
0 1 2 3
4
Identification (Fragment ID) (16 bits)
D F
M F
Fragment offset (13 bits)
4 5 6 7
8
Time-To-Live (TTL) (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
8 9 10 11
12
Source Address (32 bits)
12 13 14 15
16
Destination Address (32 bits)
16 17 18 19
20
Options (if any, variable length, padded with 0's, 40 bytes max length)
Bytes
20 Bytes

IP Header

- **Version**: A 4-bit field that identifies the IP version being used. The current version is 4, and this version is referred to as IPv4.
- **IP Header Length** (IHL): A 4-bit field containing the length of the IP header in multiple of 4 bytes
  - The minimum length of an IP header is 20 byte.
- **Type of service**: Specifies how an upper-layer protocol would like a current datagram to be handled, and assigns datagrams various levels of importance.
- **Total Length**:

Specifies the length of the IP packet that includes the IP header and the user data. The length field is 2 bytes

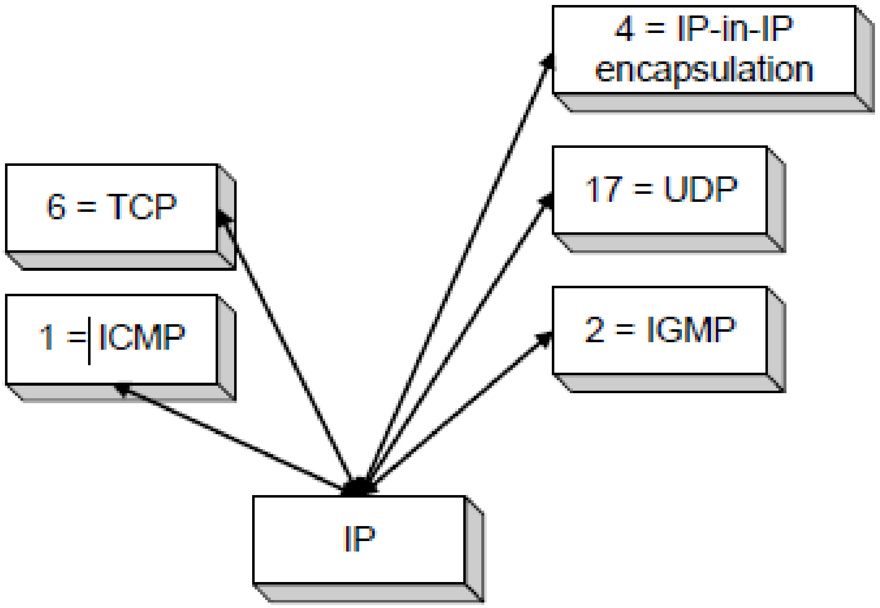
- **Identifier, Flags, and Fragment Offset**:

As an IP packet moves through the Internet, it might need to cross a link that cannot handle the size of the packet. The packet will be divided, or fragmented, into smaller packets and reassembled later. These fields are used to fragment and reassemble packets.

- **Identifier:** Unique identification of a datagram from a host. Incremented whenever a datagram is transmitted.
- **Flags (3 bits):** First bit always set to 0
  - DF bit (Do not fragment)
  - MF bit (More fragments)

IP Header

- **Time to Live (TTL):** The TTL field is initially set to a number and decremented by every router that is passed through. When TTL reaches 0 the packet is discarded.
- **Protocol**: identifies a protocol that sits above the IP layer that is used for application identification.
- **Header Checksum:** 2 bytes to determine if any errors have been introduced during transmission.
- **Source IP Address**: 32-bit IP address of the sender.
- **Destination IP Address**: 32-bit IP address of the intended recipient.
- **Options:** Record Route, Timestamp.



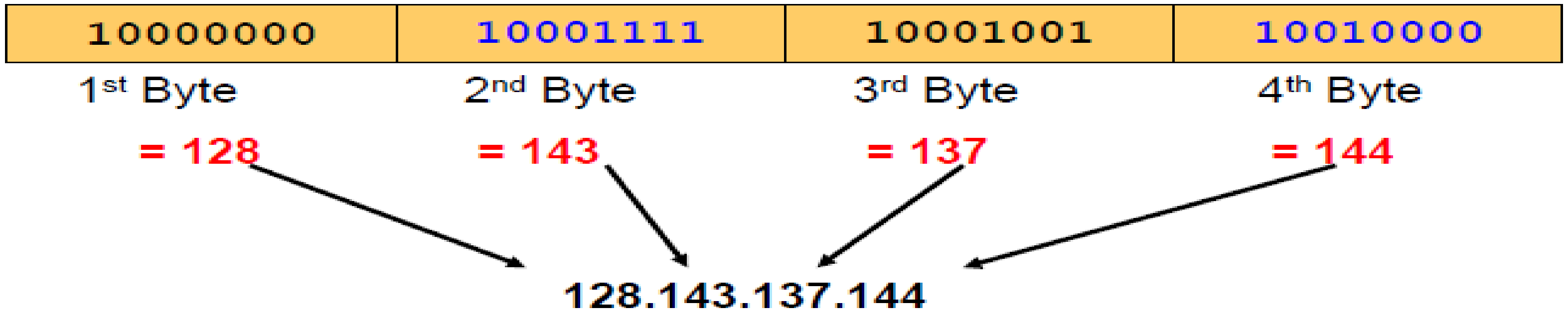
IP traffic types

- There are 3 main IP traffic types: unicast, broadcast and multicast.
  - Unicast traffic is to a single destination host.
  - Broadcast traffic is to all hosts on the subnet.
  - Multicast traffic is to multiple interested hosts.

IPv4 addressing

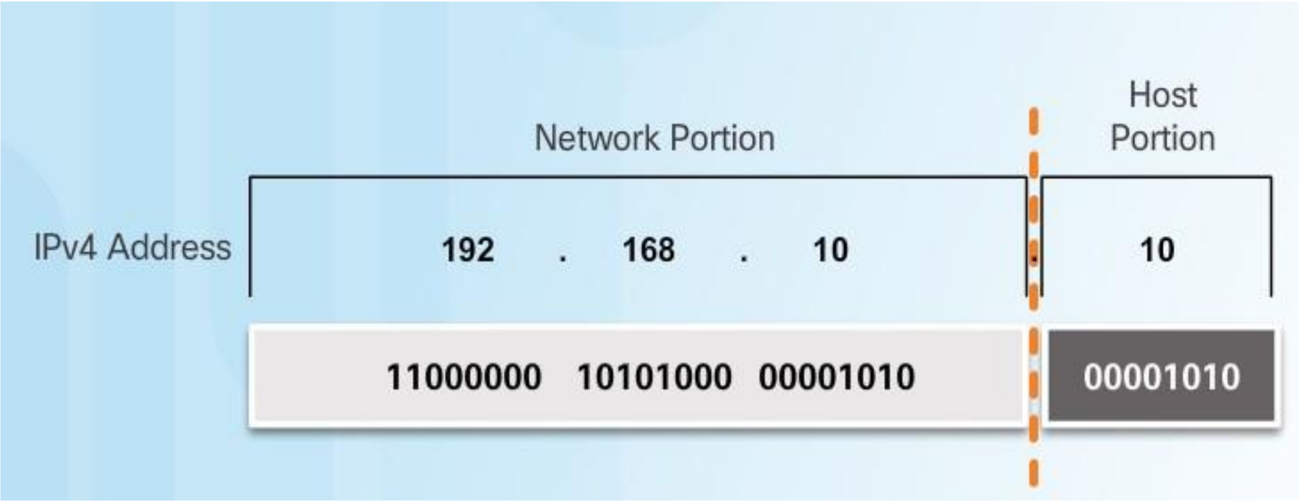
IPv4 Addressing

- IP address is the logical address for a network interface.
- An IP address: is a **32 bit long** identifier written in ***dotted decimal* notation**
- Each byte is identified by a decimal number in the range [0->255]
- The IP address is usually set manually on servers, printers and network devices such as routers and switches.
- It is usually assigned automatically through the Dynamic Host Configuration Protocol (DHCP) on desktop computers



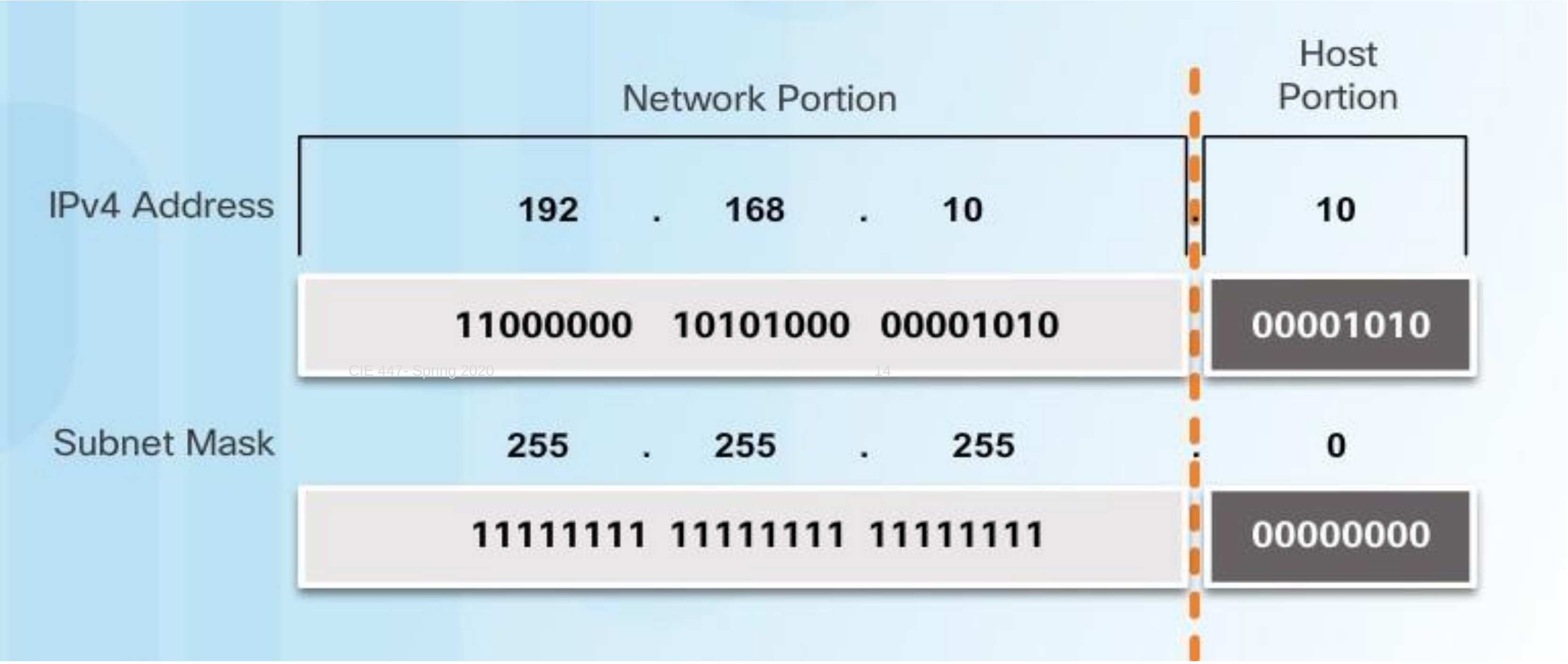
Network and Host Portions

- An IPv4 address is hierarchical.
  - Composed of a Network portion and Host portion.
- All devices on the same network must have the identical network portion.
- The Subnet Mask helps devices identify the network portion and host portion.
- Three IPv4 addresses must be configured on a host:
  - Unique IPv4 address of the host.
  - Subnet mask - identifies the network/host portion of the IPv4 address.
  - Default gateway -IP address of the local router interface.



The Subnet Mask

- The IPv4 address is compared to the subnet mask bit by bit, from left to right.
- A 1 in the subnet mask indicates that the corresponding bit in the IPv4 address is a network bit.



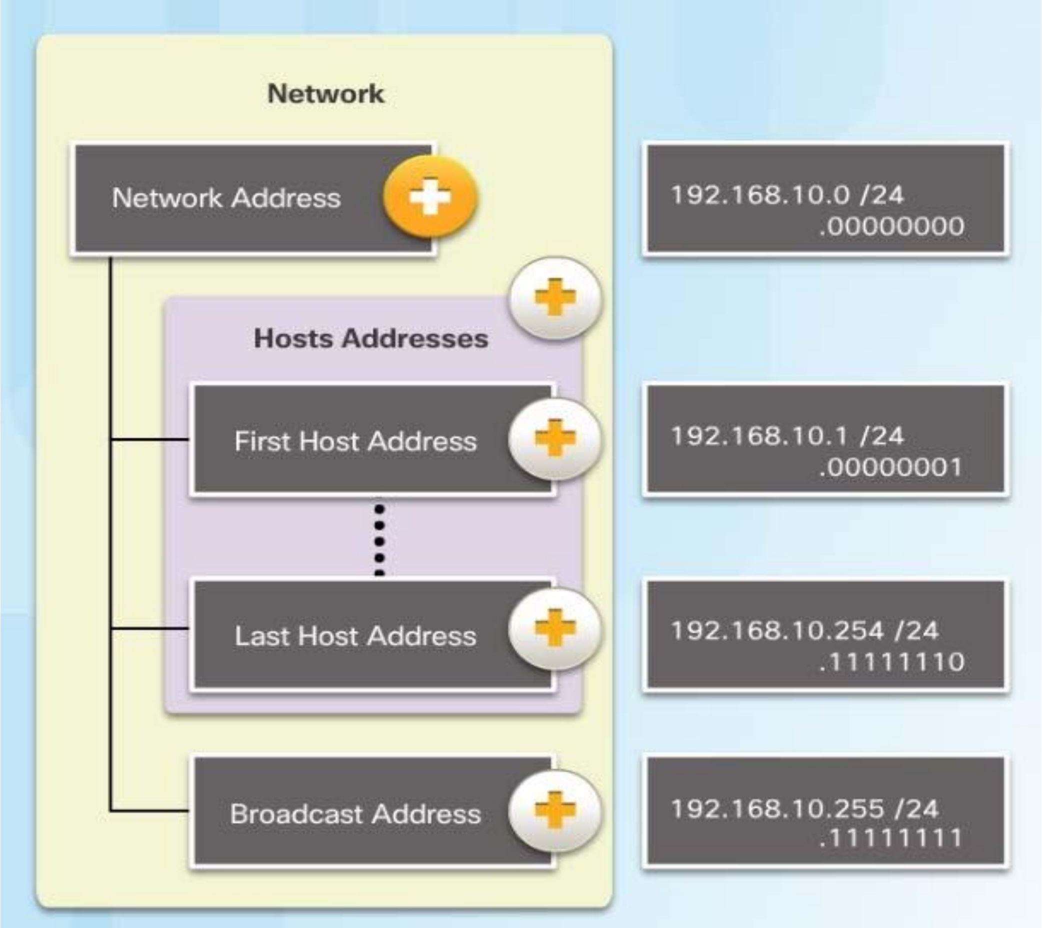
The Prefix Length

Comparing the Subnet Mask and Prefix Length

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

- The Prefix Length:
  - Shorthand method of expressing the subnet mask.
  - Equals the number of bits in the subnet mask set to 1.
  - Written in slash notation, / followed by the number of network bits.

Network, Host, and Broadcast Addresses



- Types of Addresses in Network 192.168.10.0/24
  - Network Address - host portion is all 0s (.00000000)
  - First Host address - host portion is all 0s and ends with a 1 (.00000001)
  - Last Host address - host portion is all 1s and ends with a 0 (.11111110)
  - Broadcast Address - host portion is all 1s (.11111111)

Classful Addressing

- In 1981, Internet IPv4 addresses were assigned using classful addressing (RFC 790)
- Network addresses were based on 3 classes:
  - **Class A** (0.0.0.0/8 to 127.0.0.0/8) – Designed to support extremely large networks with more than 16 million host addresses.
  - **Class B** (128.0.0.0 /16 – 191.255.0.0 /16) – Designed to support the needs of moderate to large size networks up to approximately 65,000 host addresses.
  - **Class C** (192.0.0.0 /24 – 223.255.255.0 /24) – Designed to support small networks with a maximum of 254 hosts.

Class A

- Class A addresses are assigned to networks with a very large number of hosts.

Class A Specifics	
Address Block	0.0.0.0 – 127.0.0.0
Default Subnet Mask	/8 (255.0.0.0)
Maximum Number of Networks	128
Number of Host per Network	16,777,214
High order bit	0xxxxxxx.___.___.___

* 0.0.0.0 and 127.0.0.0 are reserved and cannot be assigned

Class B

- Class B addresses are assigned to medium-sized to large-sized networks.

Class B Specifics	
Address Block	128.0.0.0 - 191.255.0.0
Default Subnet Mask	/16 (255.255.0.0)
Maximum Number of Networks	16,384
Number of Host per Network	65,534
High order bit	10xxxxxx.___.___.___

Class C

- Class C addresses are used for small networks.

Class C Specifics	
Address Block	192.0.0.0 - 223.255.255.0
Default Subnet Mask	/24 (255.255.255.0)
Maximum Number of Networks	2,097,152
Number of Host per Network	254
High order bit	110xxxxx.___.___.___

Class D

- Class D addresses are reserved for IP multicast addresses.
  - The four high-order bits in a class D address are always set to binary 1 1 1 0.
  - These addresses are not allocated to hosts and there is no default subnet mask
  - Valid addresses range from 224.0.0.0 to 239.255.255.255
  - 227.1.192.5

Class E

- Class E addresses are ‘experimental and reserved for future use’.
  - The high-order bits in a class E address are set to 1111
  - These addresses are not allocated to hosts and there is no default subnet mask
  - Addresses range from 240.0.0.0 to 255.255.255.255
  - 255.255.255.255 is the broadcast address for ‘this network’
  - 243.1.192.10

Special User IPv4 Addresses

Loopback interfaces

- all addresses 127.0.0.1-127.255.255.255 are reserved for loopback interfaces
- Most systems use 127.0.0.1 as loopback address

IP address of a network

- Host number is set to all zeros e.g., 128.143.**0.0**

Private / Test / Experimental addresses Certain address ranges are reserved for “experimental use”.

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Convention (but not a reserved address)

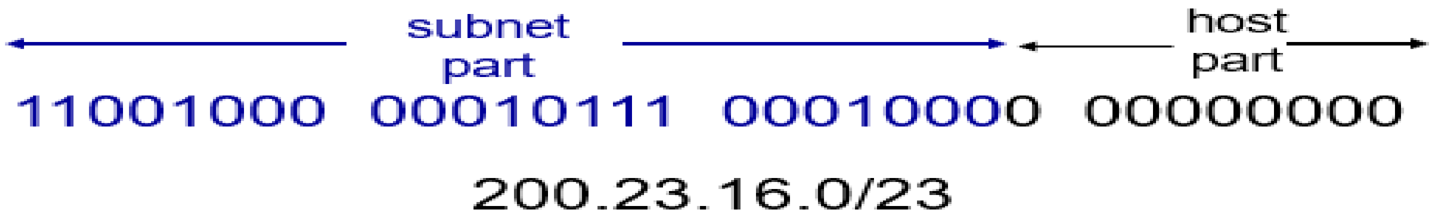
- Default gateway has host number set to ‘1’ e.g., 192.0.1.**1**

Classless Addressing

- Classful Addressing wasted addresses and exhausted the availability of IPv4 addresses.
- Classless Addressing Introduced in the 1990s
  - Classless Inter-Domain Routing **(CIDR, pronounced "cider")**
  - Allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C.

Classless Inter-Domain Routing (CIDR)

- A problem with classful addresses was that if a company had more than 254 hosts they would need to be assigned a Class B network
- They would have much less than the 65,534 hosts allocated, so this wasted a huge amount of the global address space
- Classless Inter-Domain Routing (CIDR) was introduced in 1993 to alleviate this problem
- CIDR removed the fixed /8, /16 and /24 requirements for the address classes, and allowed them to be split or ‘subnetted’ into smaller networks
- For example 175.10.10.0/20
- Companies can now be allocated an address range which more closely matches their needs and does not waste addresses

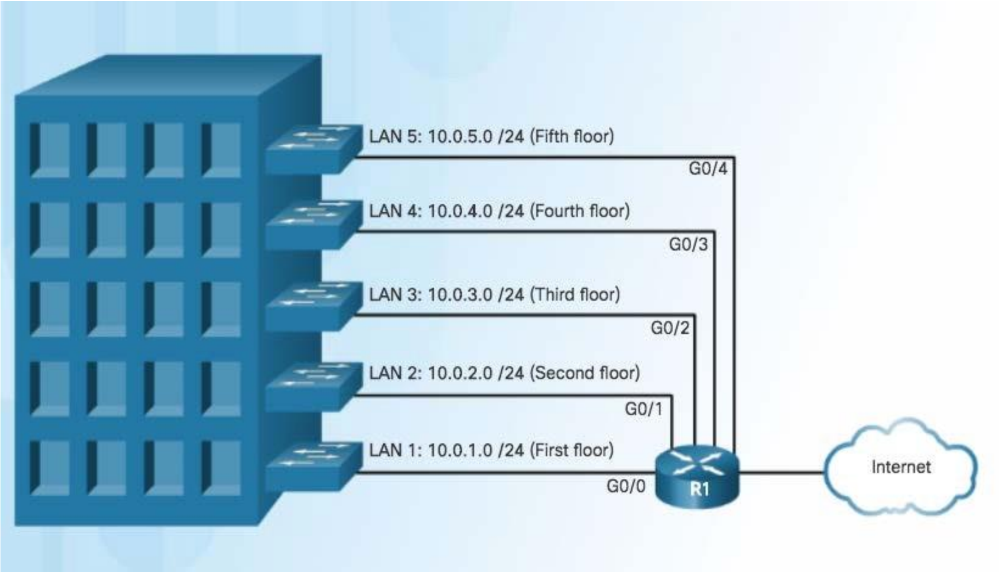


Subnetting an IPv4 Network

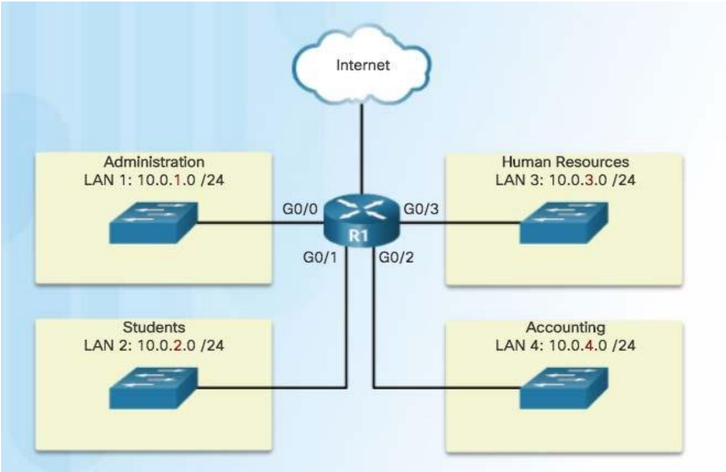
Reasons for Subnetting

- Reduces overall network traffic and improves network performance.
  .
- Enables an administrator to implement security policies such as which subnets are allowed or not allowed to communicate together

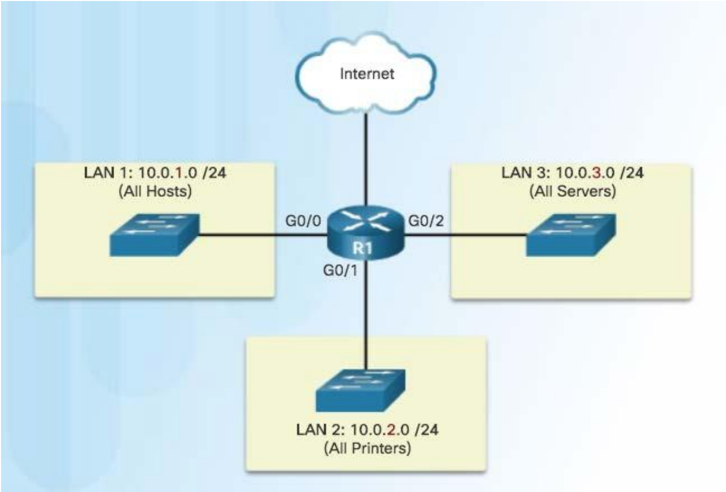
Subnetting by Location



Communicating between Networks



Subnetting by Device Type



Octet Boundaries

Networks are most easily subnetted at the octet boundary of /8, /16, and /24

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

- Prefix length and the subnet mask are different ways of identifying the network portion of an address.
- Subnets are created by borrowing host bits for network bits.
- More host bits borrowed, the more subnets that can be defined.

Subnetting on the Octet Boundary

Subnet Address (256 Possible Subnets)	Host Range (65,534 possible hosts per subnet)	Broadcast
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...	...	...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

- Subnetting Network 10.x.0.0/16
- Define up to 256 subnets with each subnet capable of connecting 65,534 hosts.
- First two octets identify the network portion while the last two octets are for host IP addresses.

Subnetting on the Octet Boundary (Cont.)

Subnet Address (65,536 Possible Subnets)	Host Range (254 possible hosts per subnet)	Broadcast
10.0.0.0/24	10.0.0.1 – 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 – 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 – 10.0.2.254	10.0.1.255
...	...	...
10.0.255.0/24	10.0.255.1 – 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 – 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 – 10.1.1.254	1.1.1.0.255
10.1.2.0/24	10.1.2.1 – 10.1.2.254	10.1.2.0.255
...	...	...
10.100.0.0/24	10.100.0.1 – 10.100.0.254	10.100.0.255
...	...	...
10.255.255.0/24	10.255.255.1 – 10.255.255.254	10.255.255.255

- Subnetting Network 10.x.x.0/24
- Define 65,536 subnets each capable of connecting 254 hosts.
- /24 boundary is very popular in subnetting because of number of hosts.

Classless Subnetting

Subnetting a /24 Network

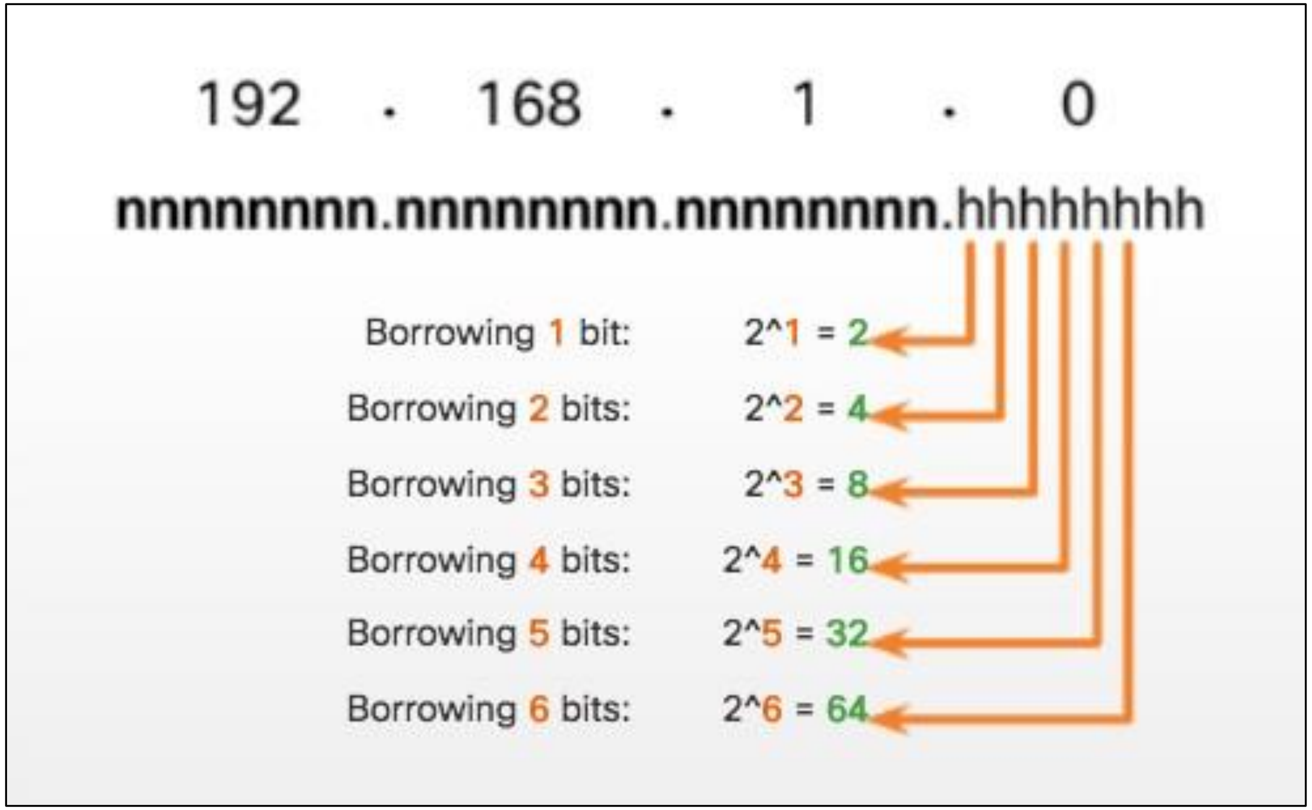
Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

Subnets can borrow bits from *any* host bit position to create other masks.

Subnetting Formulas

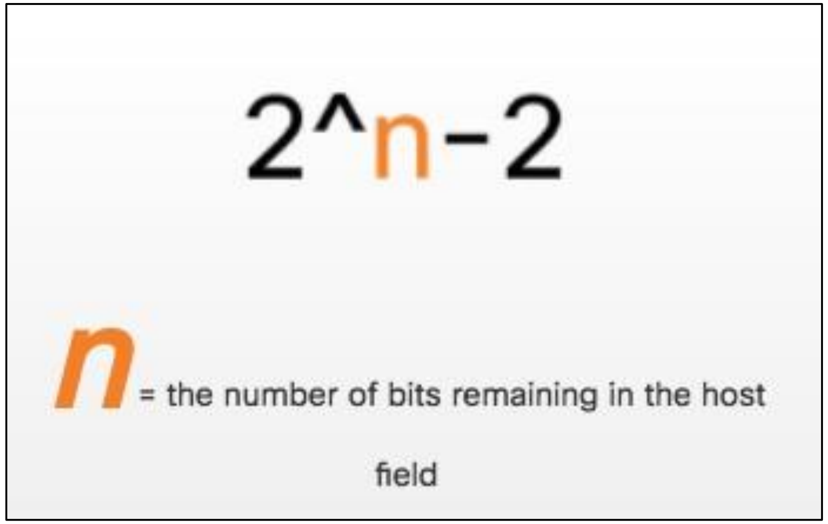
Calculate Number of Subnets Formula

Subnetting a /24 Network

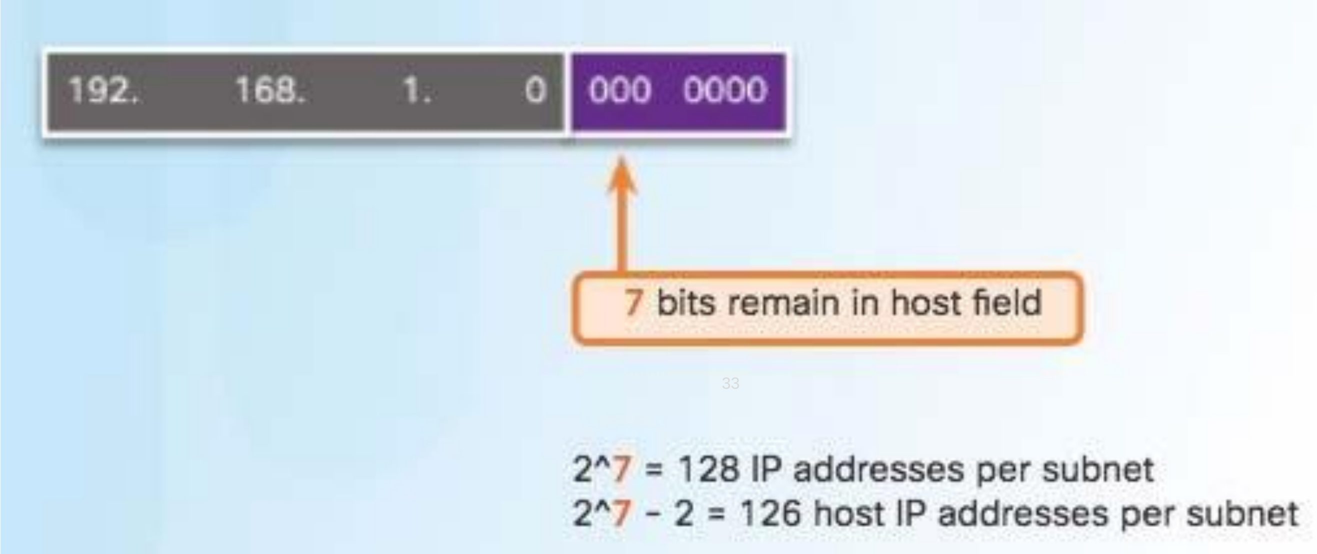


Subnetting Formulas (Cont.)

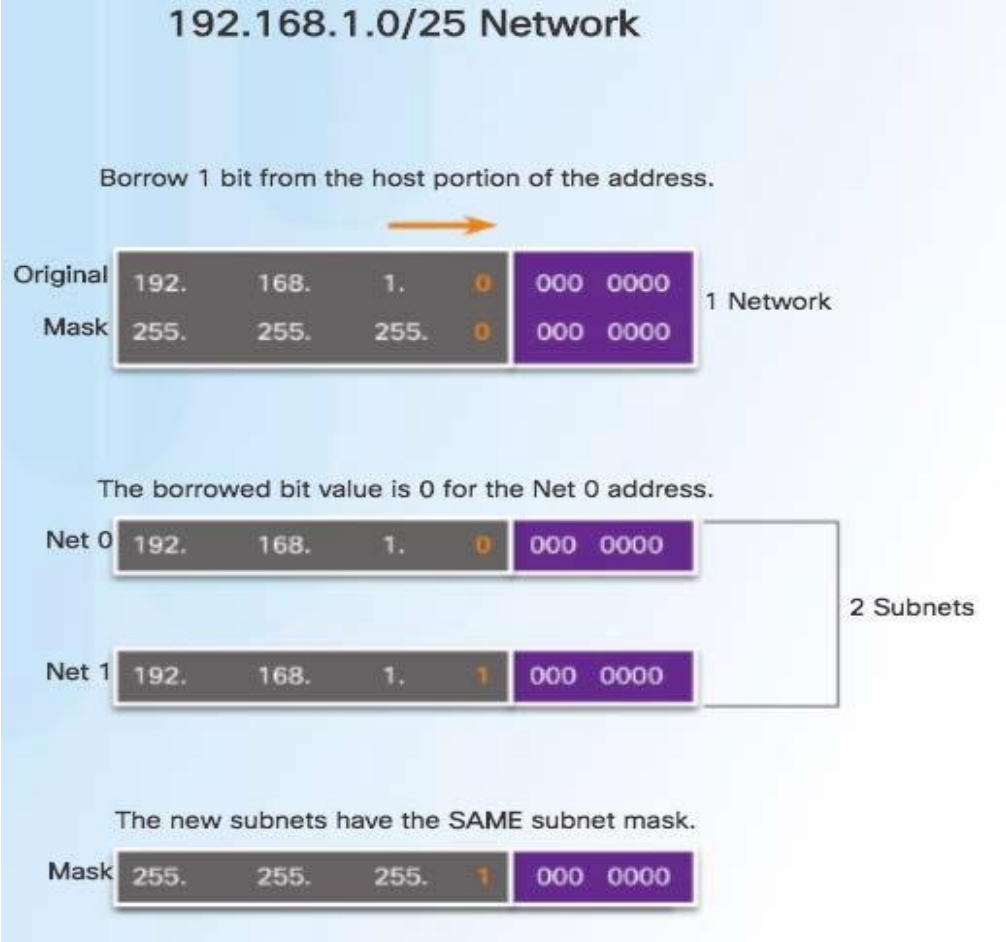
Calculate Number of Hosts Formula

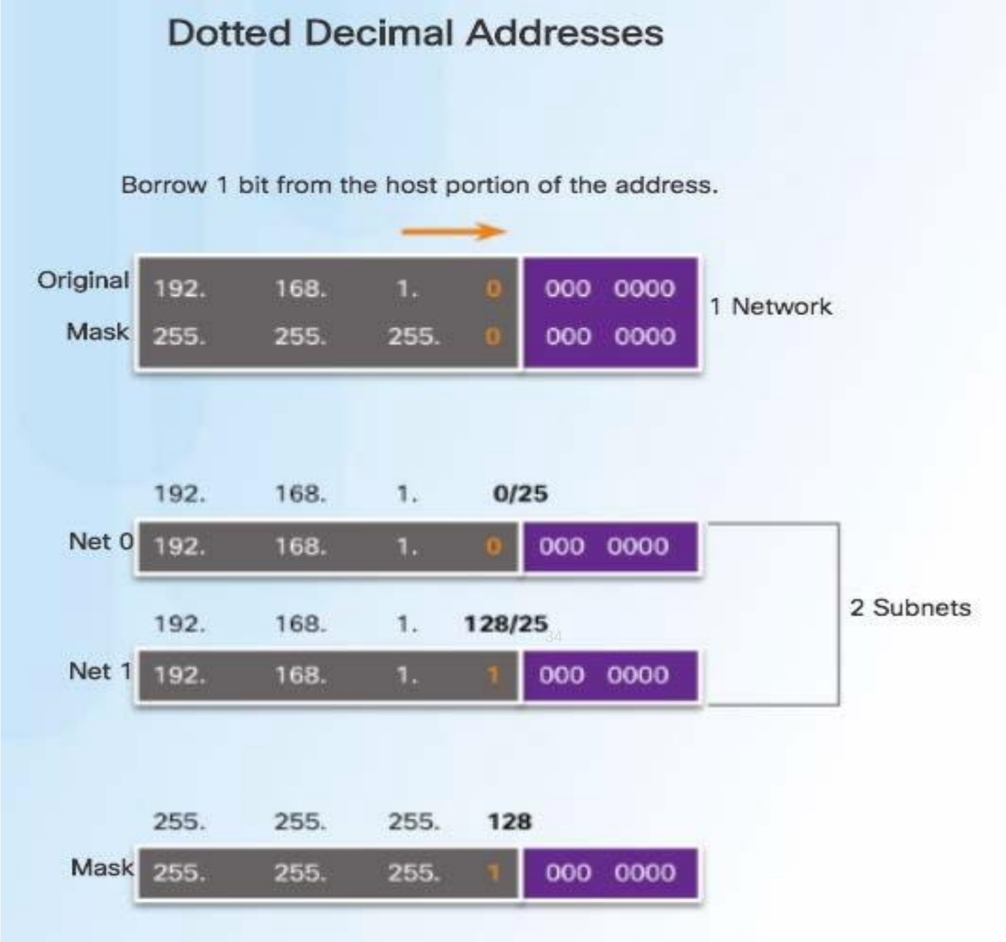


Calculating the Number of Hosts



Classless Subnetting Example





Creating Subnets with a /16 prefix

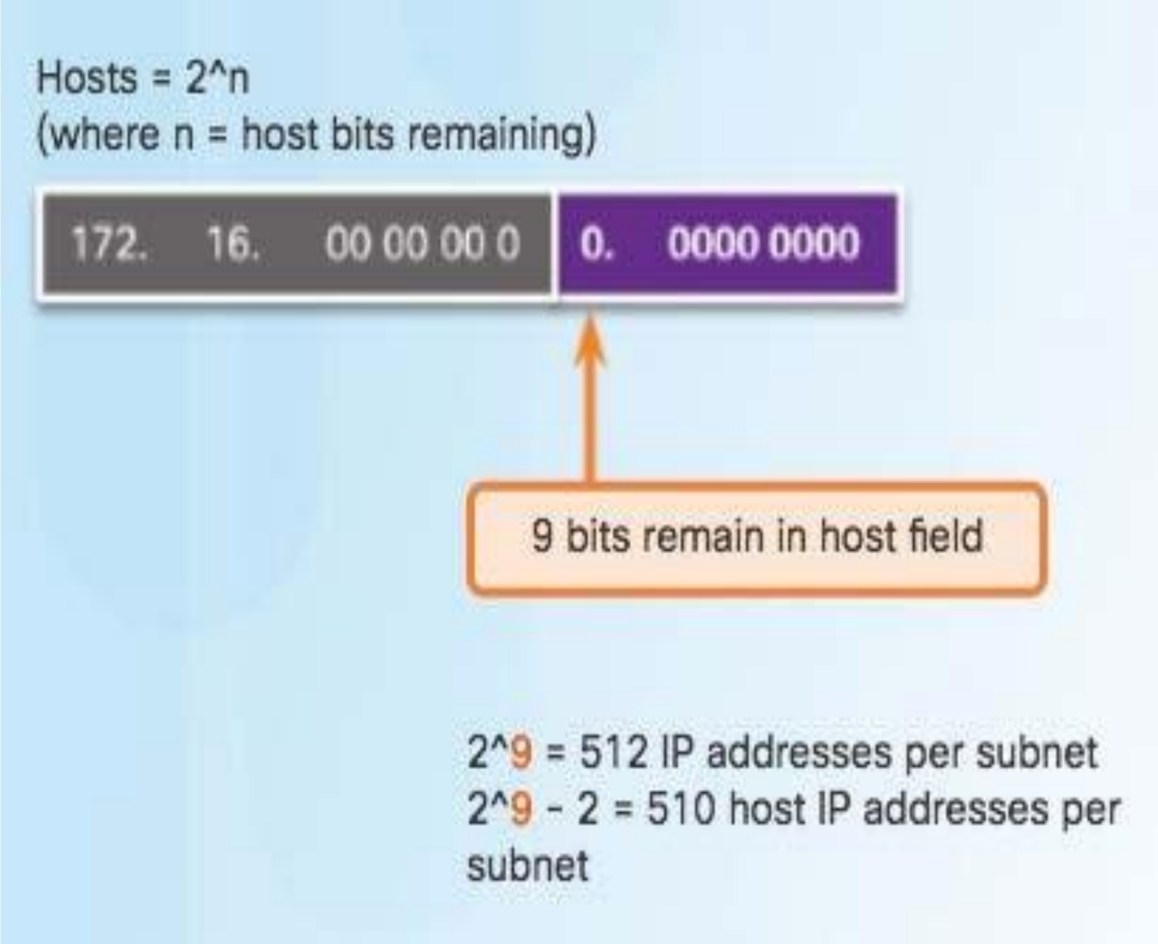
Subnetting a /16 Network

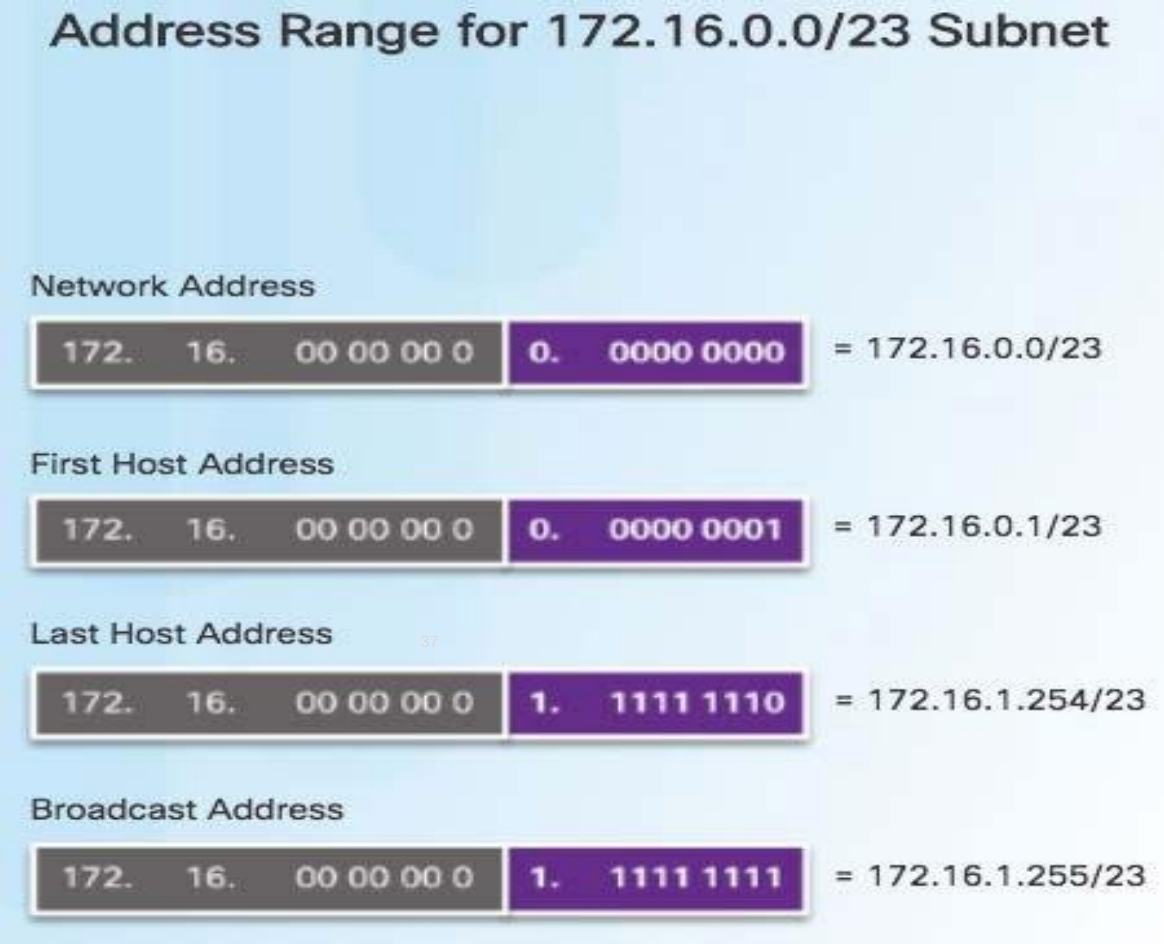
Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	2	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	4	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111100.00000000	64	1022

Creating 100 Subnets with a /16 prefix

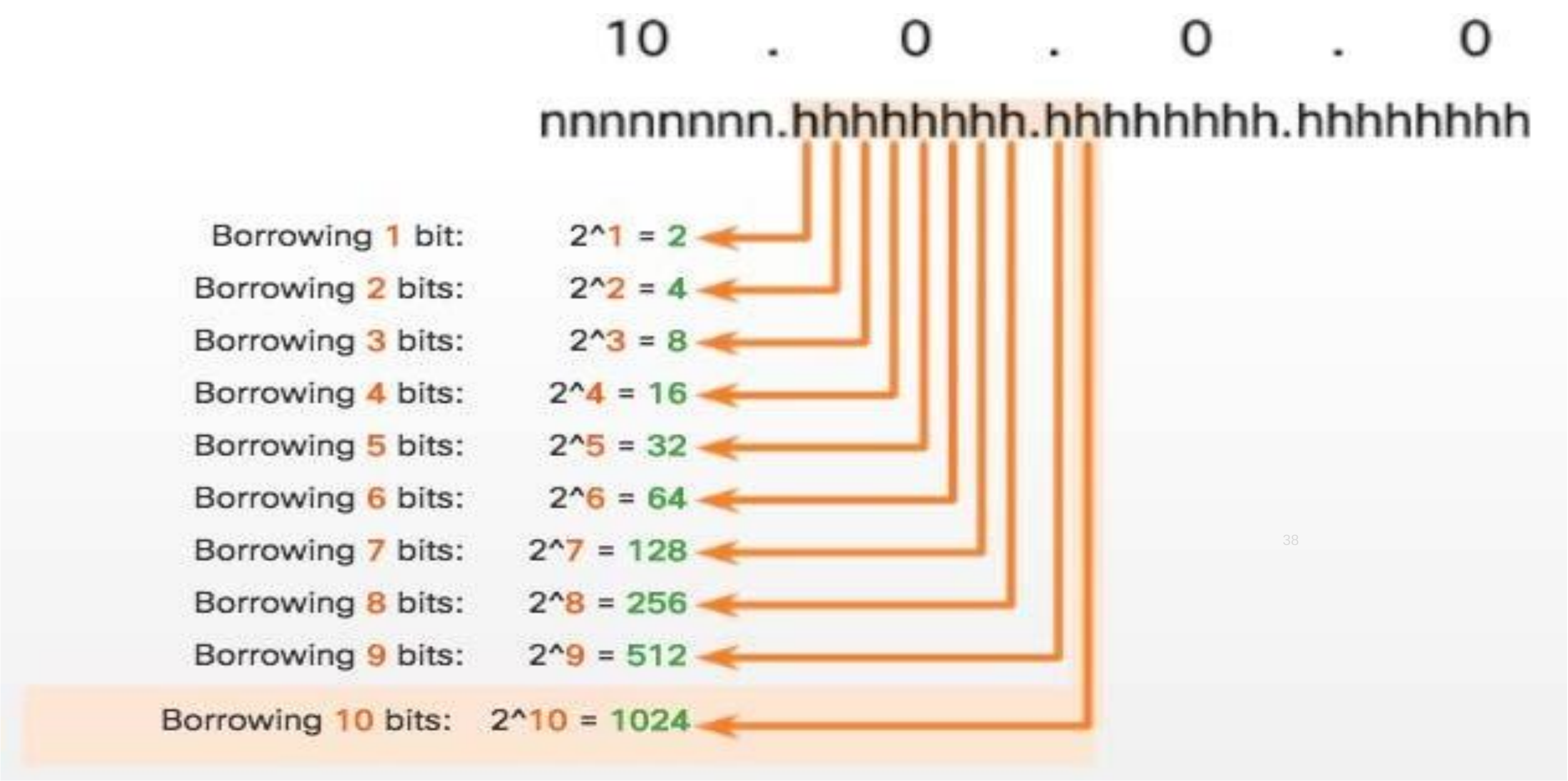
- New Subnet Mask
  - 11111111.11111111.11111110.00000000
- 2^7 = 128 Subnets
- 2^9 = 512 hosts per subnet
- Magic Number = **2**
- 172.16.**0**.0 /23
- 172.16.**2**.0 /23
- 172.16.**4**.0 /23
- 172.16.**6**.0 /23
- …
- 172.16.**254**.0 /23

Calculating the Hosts

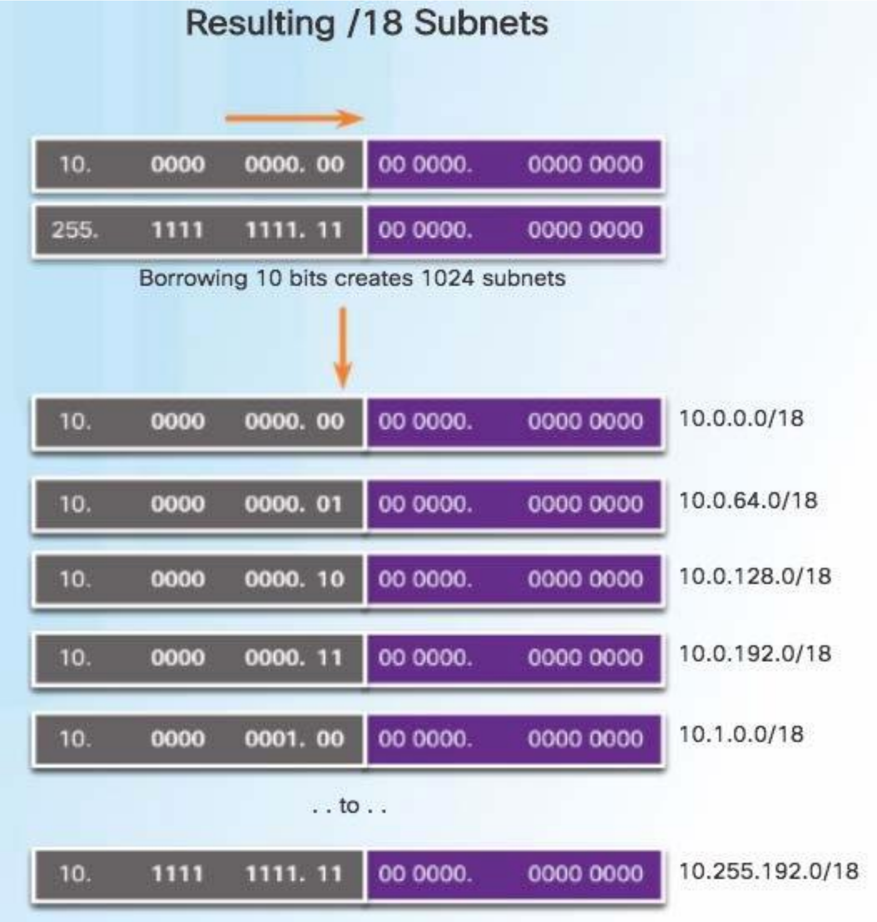


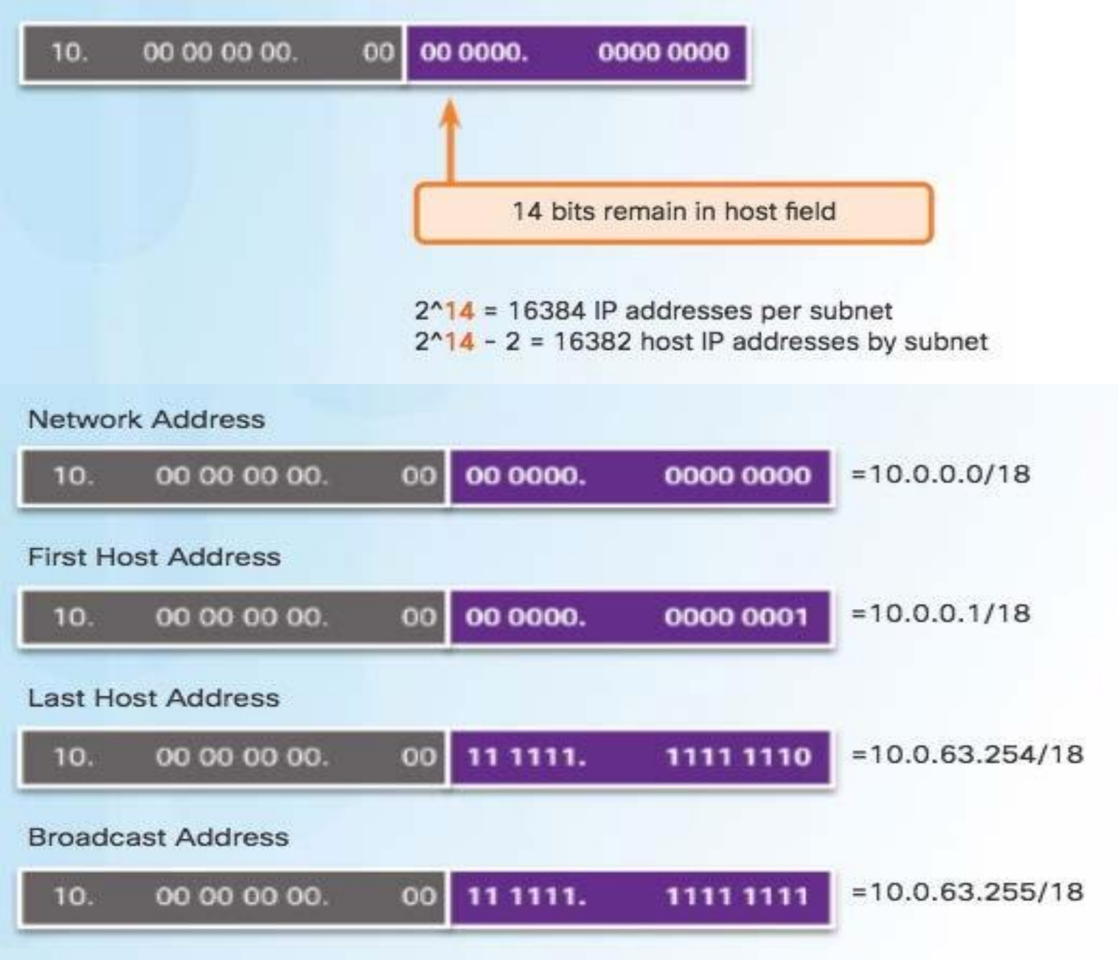


Creating 1000 Subnets with a /8 Network

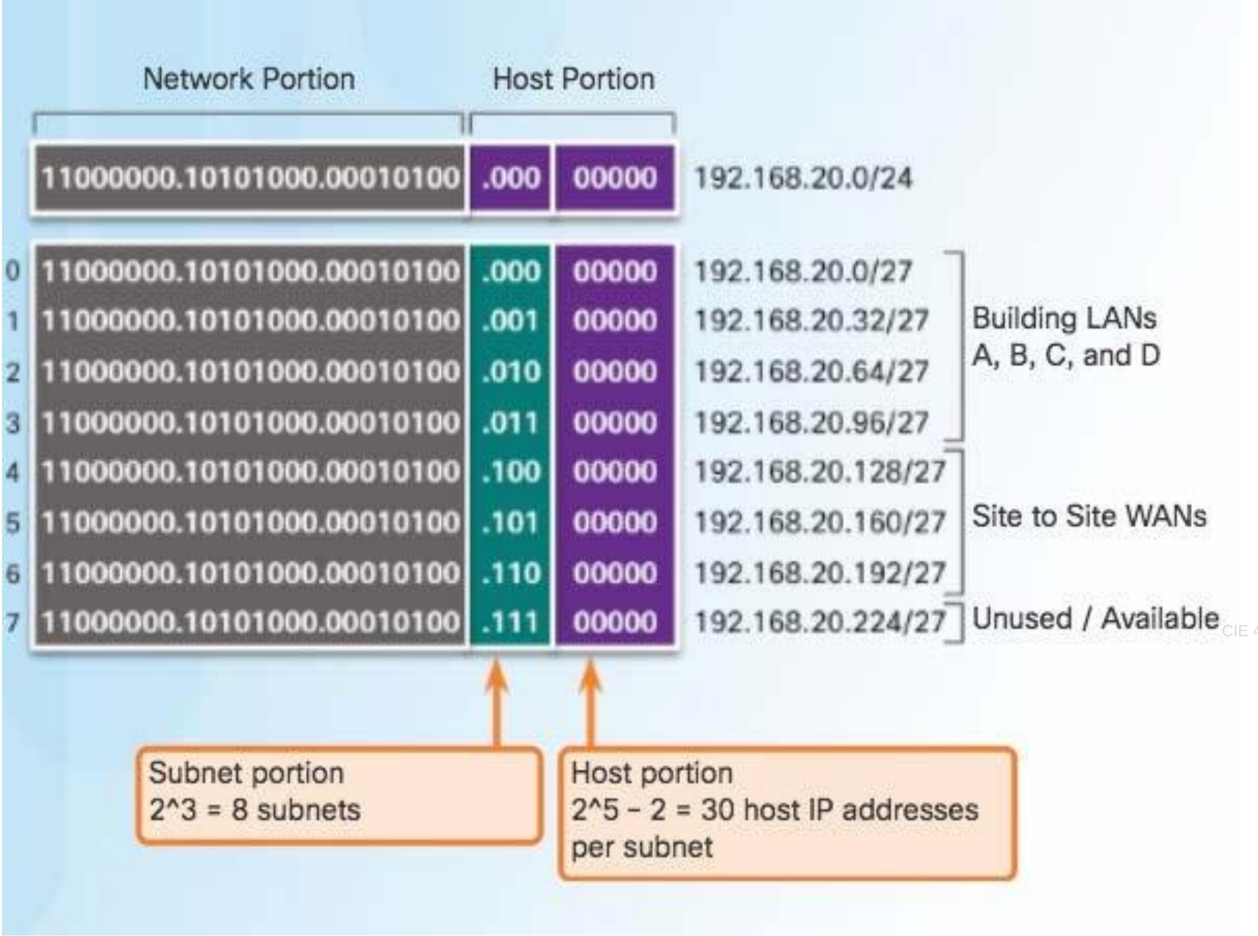


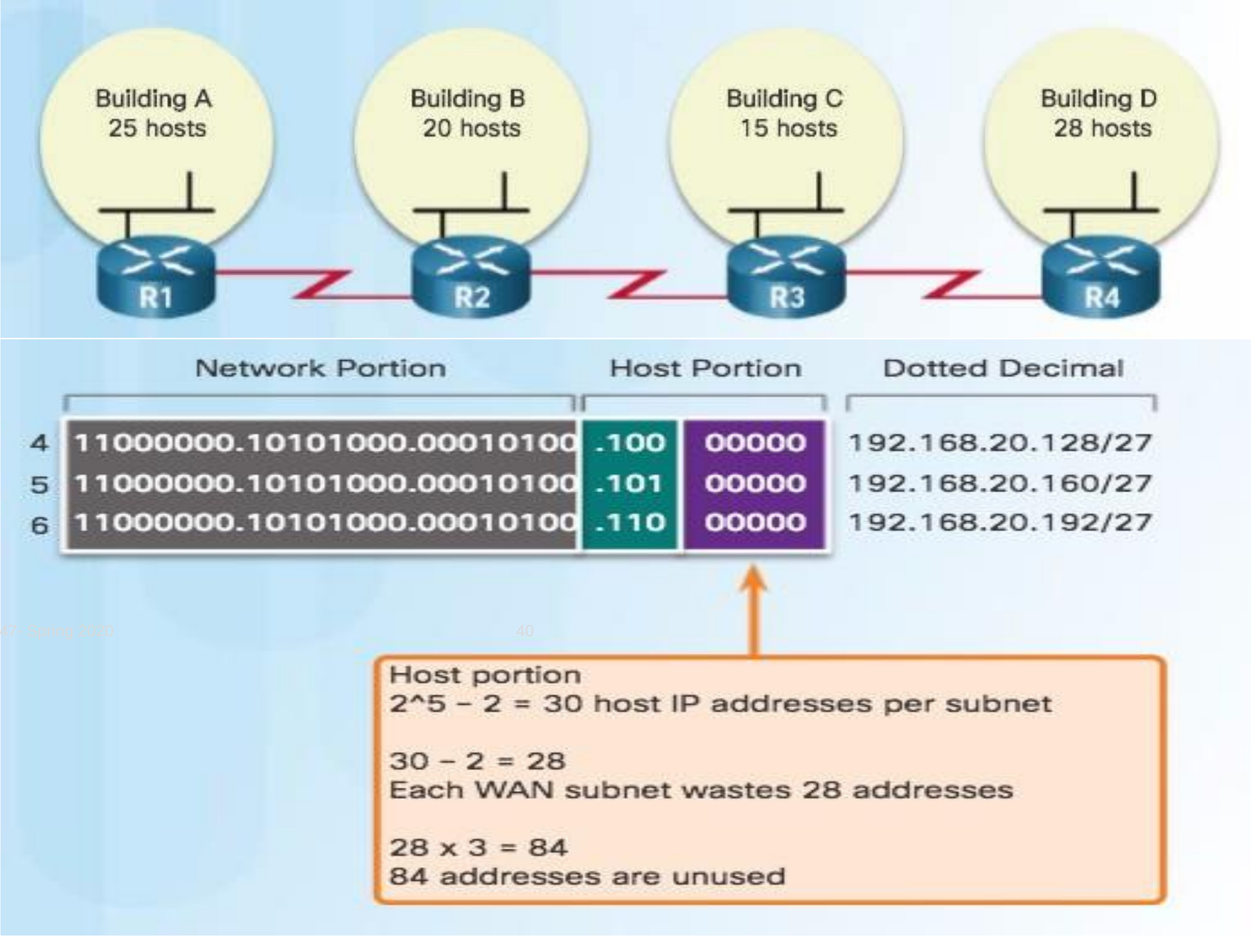
Creating 1000 Subnets with a /8 Network (Cont.)





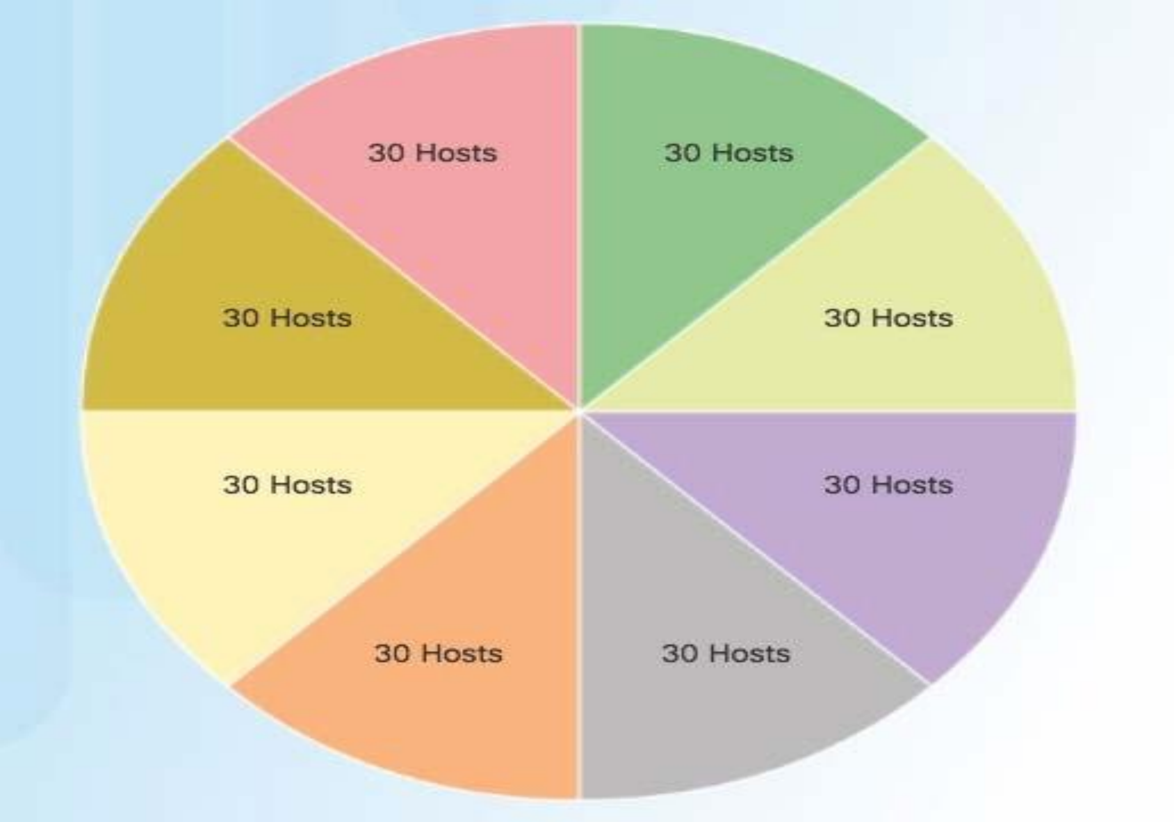
Traditional Subnetting Wastes Addresses



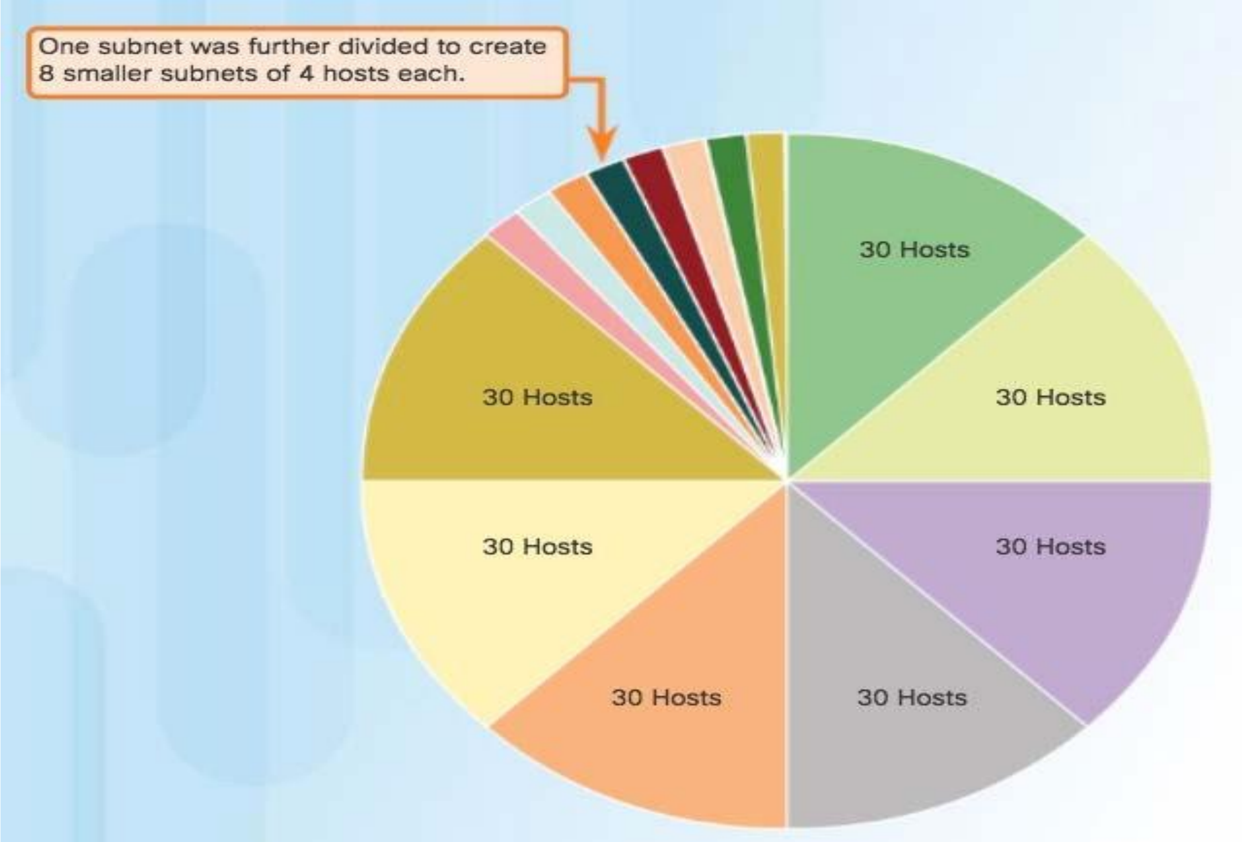


Variable Length Subnet Masks (VLSM)

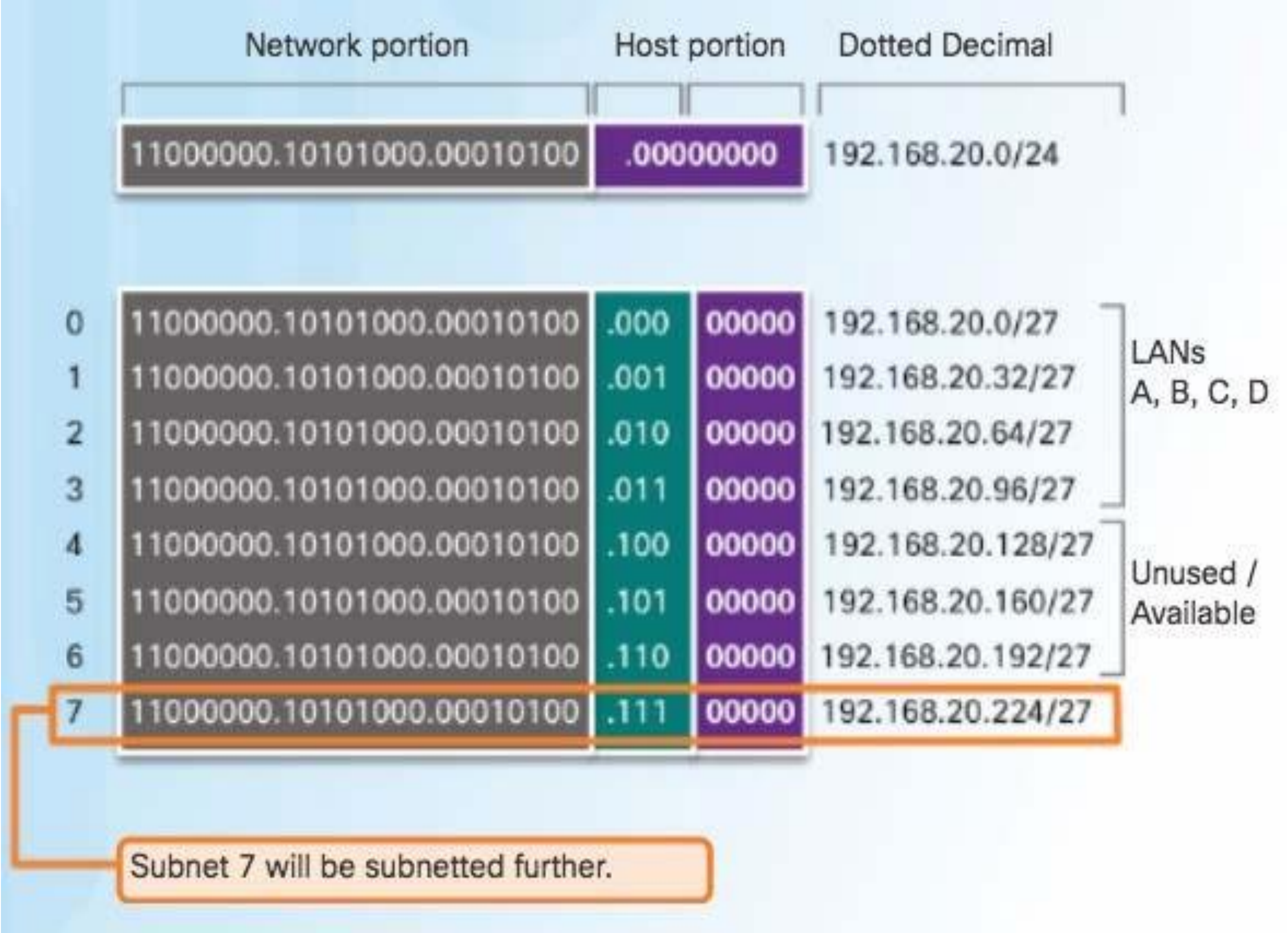
Traditional

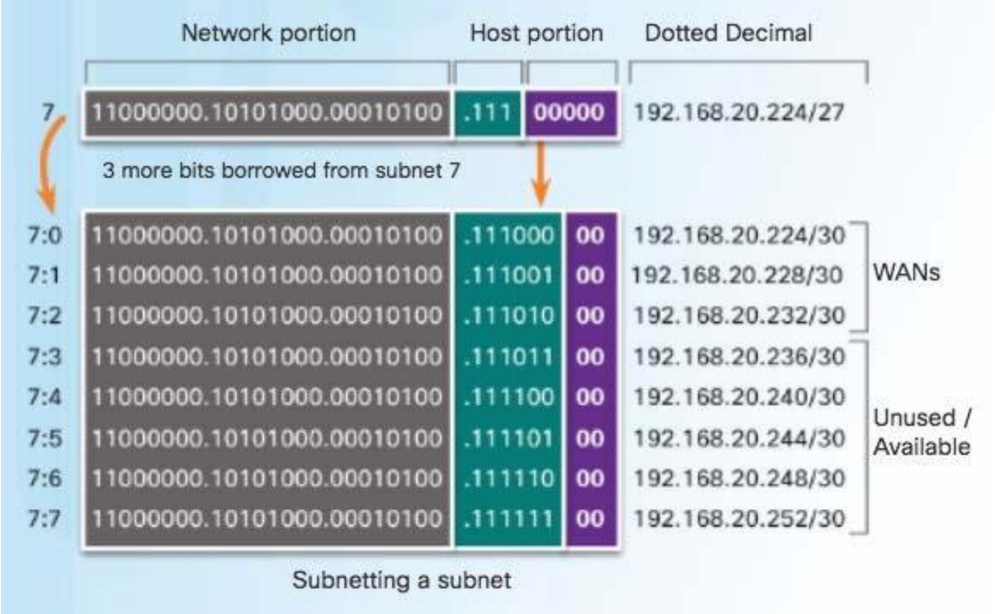


Subnets of Varying Sizes



Basic Variable Length Subnet Masking (VLSM) Basic Subnetting





VLSM Example

- Given the network 172.16.0.0 /23 creates subnets:
  - 1 network for 200 hosts - 256
  - 1 network for 100 hosts - 128
  - 1 network for 50 hosts - 64
  - 1 network for 25 hosts - 32
  - 1 network for 10 hosts - 16
  - 4 point-to-point networks for 2 hosts each – 4x4 = 16

/23 = 2^9 hosts = 512
256+128+64+32+16+16 = 512 hosts needed
Address range 172.16.0.0 – 172.16.1.255

~~172.16.0.0 /23~~
172.16.0.0 /24 (256)
~~172.16.1.0 /24~~
172.16.1.0 /25 (128)
~~172.16.1.128 /25~~
172.16.1.128 /26 (64)
~~172.16.1.192 /26~~
172.16.1.192 /27 (32)
~~172.16.1.224 /27~~
172.16.1.224 /28 (16)
~~172.16.1.240 /28~~
172.16.1.240 /30 (4)
172.16.1.244 /30 (4)
172.16.1.248 /30 (4)
172.16.1.252 /30 (4)

ICMP

Internet Control Message Protocol (ICMP)

- The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that provides message packets to **report errors and other information (Query)** regarding IP packet processing back to the source.
- ICMPs generate several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement.
- If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages.

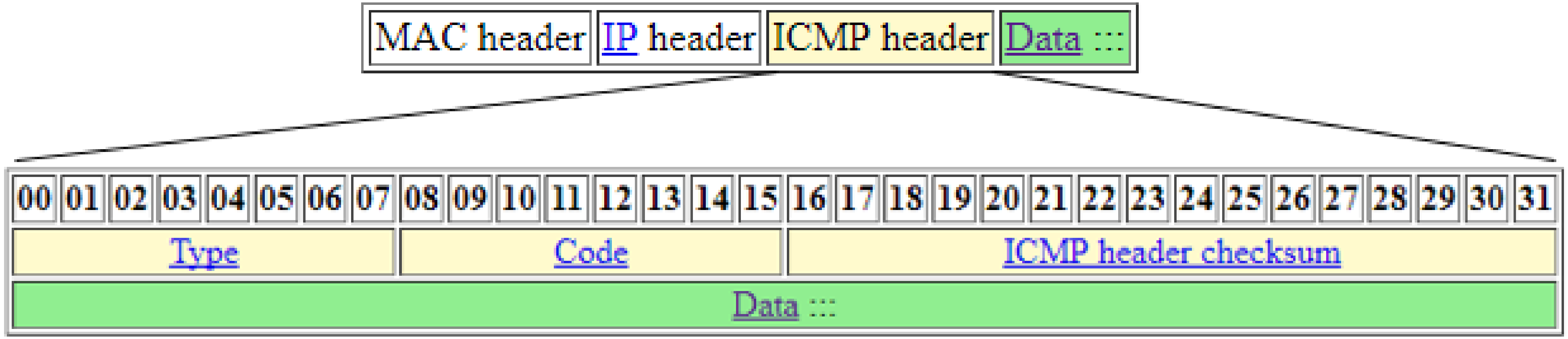
ICMP Frame Format

The ICMP is a 4 byte header:

Type (1 byte): type of ICMP message

Code (1 byte): subtype of ICMP messages

Checksum (2 bytes): This is the 16-bit one's complement of the one's complement sum of the ICMP message starting with the Type field. The checksum field should be cleared to zero before generating the checksum.



ICMP Header-Type -code:

These 8 bits specify the format of the ICMP message, to name few:

Type	Code	description
0	**0**	**echo reply (ping)**
3	0	dest. network unreachable
3	**1**	**dest host unreachable**
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	**0**	**echo request (ping)**
9	0	route advertisement
10	0	router discovery
11	**0**	**TTL expired**
12	0	bad IP header

HOW TO ASSIGN IP…..
Static IP Assignment

- Manually configuring computers with IP addresses:
  - Time consuming
  - Duplicating IP address assignments
  - Incorrect subnet masks

ROUTING PROTOCOLS

IP Routing

- Routing is the process of sending packets from a host on one network to another host on another, remote network.
- A router has two main functions:
  - Determining the best path to available networks
  - Forwarding traffic to those networks
- Routers examine the destination IP address of a packet , determine the next-hop address, and forward the packet
- Routers use **routing tables** to determine a next hop address to which the packet should be forwarded.

Routing table

- Each router maintains a routing table and stores it in RAM.
- A routing table is used by routers to determine a path to a destination network.
- Each routing table consists of the following entries:
  - **Network destination and a network subnet mask**: specifies a range of IP addresses.
  - **Remote router**: IP address of the router used to reach that network
  - **Outgoing interface**: outgoing interface the packet should go out to reach the destination network
  - **Metrics and costs** can include:
    - number of hops (hop count)
    - speed of the path
    - packet loss (router congestion/conditions)
    - latency (delay)
    - path reliability
    - path bandwidth
    - throughput load
    - MTU

```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1   192.168.1.250      20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.1.0    255.255.255.0    192.168.1.250   192.168.1.250      20
    192.168.1.250  255.255.255.255        127.0.0.1       127.0.0.1      20
    192.168.1.255  255.255.255.255    192.168.1.250   192.168.1.250      20
        224.0.0.0        240.0.0.0    192.168.1.250   192.168.1.250      20
  255.255.255.255  255.255.255.255    192.168.1.250   192.168.1.250       1
Default Gateway:       192.168.1.1
```

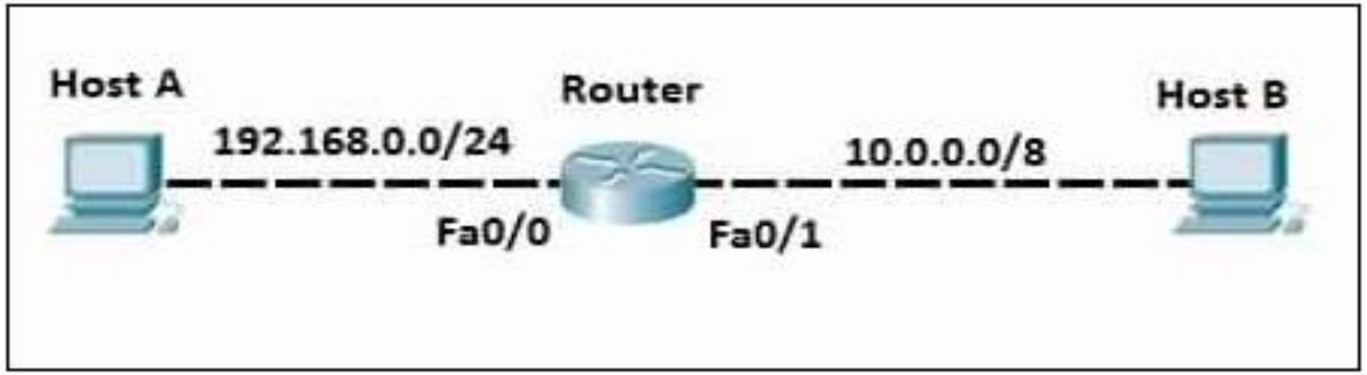
How Routing Tables are Created

There are three different methods for populating a routing table:

- Directly connected subnets
- Static routing
- Dynamic routing

1. Directly Connected Subnets (1/2)

- Host A wants to communicate with host B which is on another network.
- Host A is configured to send all packets destined for remote networks to the router.
- The router receives the packets, checks the routing table to see if it has an entry for the destination address.
- If it does, the router forwards the packet out the appropriate interface port.
- If the router doesn't find the entry, it discards the packet.



1. Directly Connected Subnets (2/2)

- Show ip route
- Router has two directly connected routes to the subnets 10.0.0.0/8 and 192.168.0.0/24.
- The character “C“ in the routing table indicates that a route is a directly connected route. The router will be able to route packets received from host A to host B.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.0.0/24 is directly connected, FastEthernet0/0
Router#
```

STATIC ROUTING

2. Static Routing

- Static routing is the most secure way of routing.
- It reduces overhead from network resources.
- Manually add routes in routing table. By adding static routes, a router can learn a route to a remote network that is not directly connected to one of its interfaces.
- It is useful where numbers of route are limited.

2. Static Routing

- Router A is directly connected to router B.
- Router B is directly connected to the subnets (10.0.1.1/24. and 10.0.2.1/24)
- Since that subnet is not directly connected to Router A,
- the router doesn’t know how to route packets destined for that subnet.
- You have to configure that route manually.

```
ip route 10.0.1.0 255.255.255.0 10.0.0.1
ip route 10.0.2.0 255.255.255.0 10.0.0.1
```


```
ip route 10.1.0.0 255.255.255.0 10.0.0.2
```

2. Static Routing

First, consider the router A's routing table before adding the static route:

```
A#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
C       10.1.0.0 is directly connected, FastEthernet1/0
A#
```

2. Static Routing

- Use *static route* command to configure router A to reach the subnet 10.0.1.0/24.
- The router now has the route to reach the subnet:

ip route DESTINATION_NETWORK SUBNET_MASK NEXT_HOP_IP_ADDRESS

```
A#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 3 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
C       10.1.0.0 is directly connected, FastEthernet1/0
S       10.0.1.0 [1/0] via 10.0.0.1
A#
```

Pros and Cons of Static Routing

Pros:

- It is easy to implement.
- It is most secure way of routing, since no information is shared with other routers.
- It puts no overhead on resources such as CPU or memory.

Cons:

- It is suitable only for small network.
- If a link fails it cannot reroute the traffic.

Cisco Packet Tracer

Switch

Switch Basic Commands (1/2)

Command	Purpose
1-Configure Terminal Example: Switch> enable Switch# configure terminal (or config t) Switch(config)#	Enters global configuration mode, when using the console port.
2-Hostname Name Example: Switch (config)# hostname S1 S1(config)#	Specifies the name for the switch.
3-Interface Type Number Example: Switch(config)# **interface vlan 1** Switch(config-if)#	Enters the configuration mode for Vlan interface on the Switch. **Must be in enabled configuration Mode**

Switch Basic Commands (2/2)

Command	Purpose
4-IP Address IP-Address Mask Example: Switch(config-if)# ip address 192.168.12.1 255.255.255.0 Switch (config-if)#	Sets the IP address and subnet mask for the specified vlan interface.
5-No shutdown Example: Switch(config-if)# no shutdown Switch(config-if)#	Enables the vlan interface, changing its state from administratively down to administratively up **Wait 2 seconds after that command**
6-Exit Example: Switch(config-if)# exit Switch(config)#	Exits configuration mode for vlan interface and returns to global configuration mode

Verifying Your Configuration

Switch# show running-config

Switch# show ip interface brief

Save Switch Configuration

Exit from configuration mode

S1#write memory (or wr)

- This command write your configuration in memory

S1# copy running-config startup-config

- This command will take your current configuration and save it to the startup configuration file

Router

Router Basic Commands (1/2)

Command	Purpose
1-Configure Terminal Example: Router> enable Router# configure terminal (or config t) Router(config)#	Enters global configuration mode, when using the console port.
2-Hostname Name Example: Router(config)# hostname MyRouter MyRouter(config)#	Specifies the name for the router.
3-Interface Type Number Example: Router(config)# interface fastethernet 4 (or int f0/4) Router(config-if)#	Enters the configuration mode for a Fast Ethernet WAN interface on the router. **Must be in enabled configuration Mode**

Router Basic Commands (2/2)

Command	Purpose
4-IP Address IP-Address Mask Example: Router(config-if)# ip address 192.168.12.1 255.255.255.0 Router(config-if)#	Sets the IP address and subnet mask for the specified Fast Ethernet interface.
5-No shutdown Example: Router(config-if)# no shutdown Router(config-if)#	Enables the Ethernet interface, changing its state from administratively down to administratively up **Wait 2 seconds after that command**
6-Exit Example: Router(config-if)# exit Router(config)#	Exits configuration mode for the Fast Ethernet interface and returns to global configuration mode

Configuration Example

R1

```
*Mar  1 00:00:04.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down
*Mar  1 00:00:04.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to down
*Mar  1 00:00:04.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to down
*Mar  1 00:00:04.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
*Mar  1 00:00:04.547: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to down
*Mar  1 00:00:04.551: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/2, changed state to down
*Mar  1 00:00:04.551: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/3, changed state to down
R1#
R1#enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
```

Save Router Configuration

Exit from configuration mode

R1#write memory (or wr)

- This command write your configuration in memory

R1# copy running-config startup-config

- This command will take your current configuration and save it to the startup configuration file

```
R1(config-if)#exit
R1(config)#exit
R1#wr
*Mar  1 00:01:44.095: %SYS-5-CONFIG_I: Configured from console by console
R1#copy runnin
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Verifying Your Configuration

Router# show ip route

Router# show ip interface brief

R1

```
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#wr
*Mar  1 00:01:44.095: %SYS-5-CONFIG_I: Configured from console by console
R1#copy runnin
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.12.0/24 is directly connected, FastEthernet0/0
R1#
```

Lab5- NETWORK LAYER

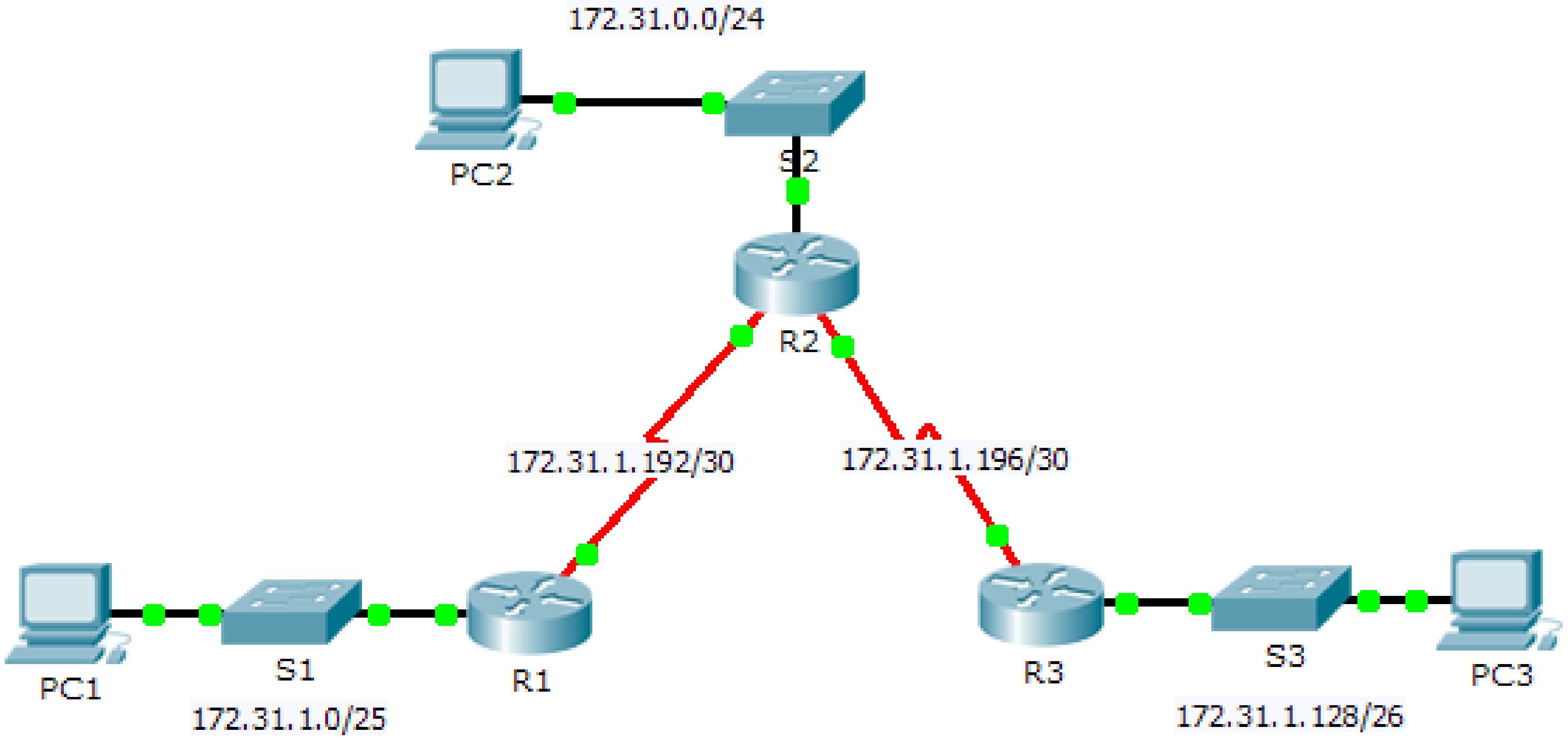
Lab Setup

Objectives

Part 1: Examine the Network and Evaluate the Need for Static Routing

Part 2: Configure Static and Default Routes

Part 3: Verify Connectivity



Addressing table

create the preceding topology and configure the devices as per the values mentioned in the following table. **First of all, configure the IP addresses on each device ,**

On switches ; only configure their hostname.

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.1.1	255.255.255.128	N/A
	S0/0/0	172.31.1.194	255.255.255.252	N/A
R2	G0/0	172.31.0.1	255.255.255.0	N/A
	S0/0/0	172.31.1.193	255.255.255.252	N/A
	S0/0/1	172.31.1.197	255.255.255.252	N/A
R3	G0/0	172.31.1.129	255.255.255.192	N/A
	S0/0/1	172.31.1.198	255.255.255.252	N/A
PC1	NIC	172.31.1.126	255.255.255.128	172.31.1.1
PC2	NIC	172.31.0.254	255.255.255.0	172.31.0.1
PC3	NIC	172.31.1.190	255.255.255.192	172.31.1.129

Part 1:Examine the Network and Evaluate the Need for Static Routing

Looking at the topology diagram,

Q1: how many networks are there in total?

Q2: How many networks are directly connected to R1, R2, and R3?

Q3:Test connectivity to the R2 and R3 LANs by pinging PC2 and PC3 from PC1. Save screenshots

Q4:Why were you unsuccessful?

Q5: How many static routes are required by each router to reach networks that are not directly connected?

Part 2:Configure Static and Default Routes

Step 1: Configure recursive static routes on R1.

Configure a recursive static route to every network not directly connected to R1, including the WAN link between R2 and R3.

ip route 172.31.0.0 255.255.255.0 172.31.1.193

ip route 172.31.1.196 255.255.255.252 172.31.1.193

ip route 172.31.1.128 255.255.255.192 172.31.1.193

Q6: Test connectivity to the R2 LAN and ping the IP addresses of PC2 and PC3. Why were you unsuccessful? **Save screenshots**

Part 2:Configure Static and Default Routes

Step 2: Configure recursive static routes on R2.

Configure a recursive static routes from R2 to every network not directly connected.

ip route 172.31.1.0 255.255.255.128 172.31.1.194

ip route 172.31.1.128 255.255.255.192 172.31.1.198

Step 3: Configure a default route on R3.

Configure a default route on R3 so that every network not directly connected is reachable.
ip route 0.0.0.0 0.0.0.0 172.31.1.197

Part 3:Verify static route configurations and Verify Connectivity

Use verification commands to check your interface configurations.

- Use the **show ip interface brief** command on both **R1 , R2 and R3** to quickly verify that the interfaces are configured with the correct IP address and active.

Q7 : How many interfaces on R1 , R2 and R3 are configured with IP addresses and in the "up" and "up" state? Save screenshots

Q8: What part of the interface configuration is NOT displayed in the command output?

Use the **show ip route** command on both **R1 , R2** and **R3** to view the current routing tables and answer the following questions: Save screenshots

Q9: How many connected routes (uses the C code) do you see on each router?

Q10: Does this number match the number of C and D routes shown in the routing table?

Part 3:Verify static route configurations and Verify Connectivity

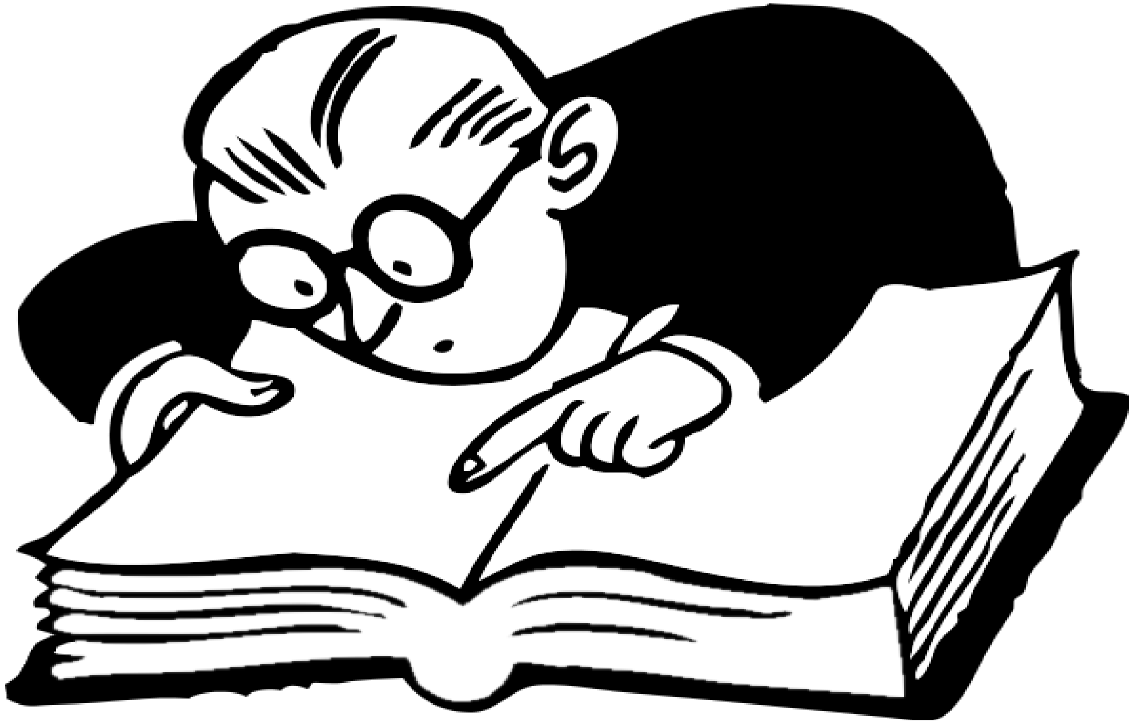
Test end-to-end connectivity across the network.

You should now be able to ping from any PC to any other PC on the network. In addition, you should be able to ping the active interfaces on the routers. For example, the following should tests should be successful:

Q11: From the command line on PC1, ping PC2 and PC3.

Q12: From the command line on R1, ping PC3.

Task



- ❑ Post your **pdf-format** explanation report on the Google classroom **due two days after lab.**
- ❑ All answers should be contained in **one explanation report**. DO NOT create a separate answer report for each question
- ❑ Don't forget to provide your project as appendices for **full credit.**


Questions

Thank you.....!