HO CHI MINH CITY UNIVERSITY OF SCIENCE
FACULTY OF ELECTRONICS AND TELECOMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS AND NETWORKS

COURSE

COMPUTER NETWORKS

Chapter 04

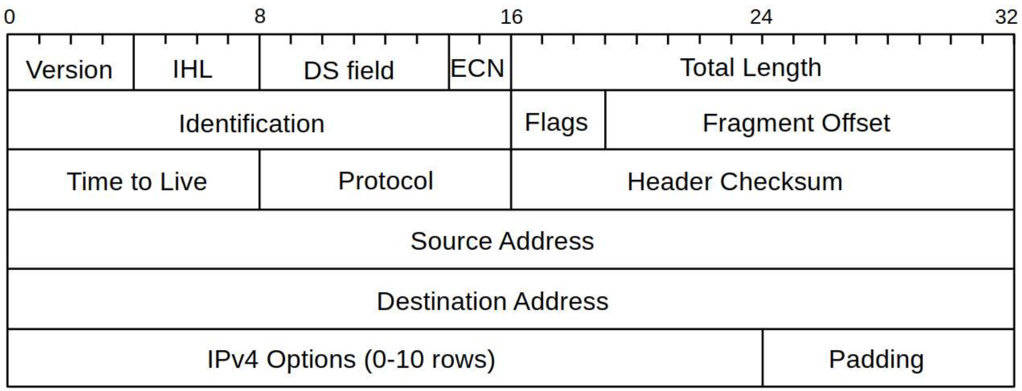
IP VERSION 4

Reference: Peter L Dordal, "An Introduction to Computer Networks," Jul 26, 2019

Lecturer: Nguyen Viet Ha, Ph.D. Email: nvha@fetel.hcmus.edu.vn

1 The IPv4 Header

1. The IPv4 Header



1. The IPv4 Header

- **Version:** Contains a 4-bit binary value identifying the IP packet version. For IPv4 packets, this field is always set to 0100.
- **Differentiated Services (DS)** (Type of Service - ToS) field: 8-bit field used to determine the priority of each packet.
  - The first 6 bits identify the Differentiated Services Code Point (DSCP) value that is used by a quality of service (QoS) mechanism.
  - The last 2 bits identify the explicit congestion notification (ECN) value that can be used to prevent dropped packets during times of network congestion.

1. The IPv4 Header

❖ **Time-to-Live (TTL):** Contains an 8-bit binary value that is used to limit the lifetime of a packet (referred to as hop count).

- ➢ Decreased by one each time the packet is processed by a router, or hop. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address.

❖ **Protocol:** This 8-bit binary value indicates the data payload type (upper-layer).

- ➢ ICMP (0x01), TCP (0x06), and UDP (0x11)….

❖ **Source IP Address -** Contains a 32-bit binary value that represents the source IP address of the packet.

❖ **Destination IP Address -** Contains a 32-bit binary value that represents the destination IP address of the packet.

1. The IPv4 Header

❖ **Internet Header Length (IHL) -** Contains a 4-bit binary value identifying the number of 32-bit words in the header. The IHL value varies due to the Options and Padding fields.

- ➢ Minimum: 5 -> Maximum: 15

❖ **Total Length –** (Packet Length), this 16-bit field defines the entire packet (fragment) size, including header and data, in bytes.

- ➢ Minimum: 20 -> Maximum: 65,535 bytes.

❖ **Header Checksum -** The 16-bit field is used for error checking of the IP header.

- ➢ If the values do not match, the packet is discarded.

1. The IPv4 Header

❖A router may have to **fragment a packet** when forwarding it from one medium to another medium that has a smaller MTU.

❖ **Identification -** This 16-bit field uniquely identifies the fragment of an original IP packet.

❖ **Flags -** This 3-bit field identifies how the packet is fragmented. It is used with the Fragment Offset and Identification fields to help reconstruct the fragment into the original packet.

- ➢ DF**: D**on't **F**ragments flag, MF: **M**ore **F**ragments flag

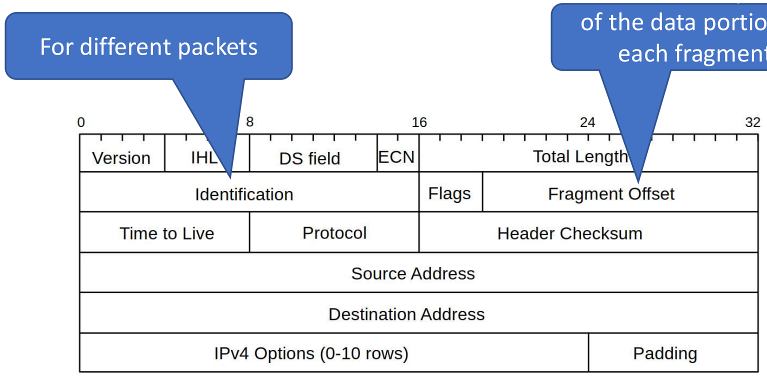
❖ **Fragment Offset -** This 13-bit field identifies the order in which to place the packet fragment in the reconstruction of the original unfragmented packet.

2 Fragmentation

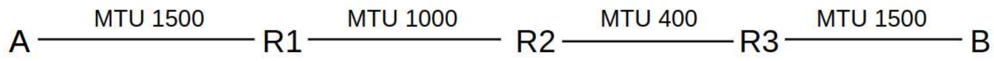
2. Fragmentation

❖MTU is smaller than the packet that needs forwarding.

→Fragmentation (vs. reassembly)



2. Fragmentation



❖Suppose **A** addresses a packet of 1500 bytes to **B**, and sends it via the LAN to the first router **R1**. The packet contains 20 bytes of IPv4 header and 1480 of data.

A→R1	FragOffset
1st Fragment	
2nd Fragment	
3rd Fragment	
4th Fragment	

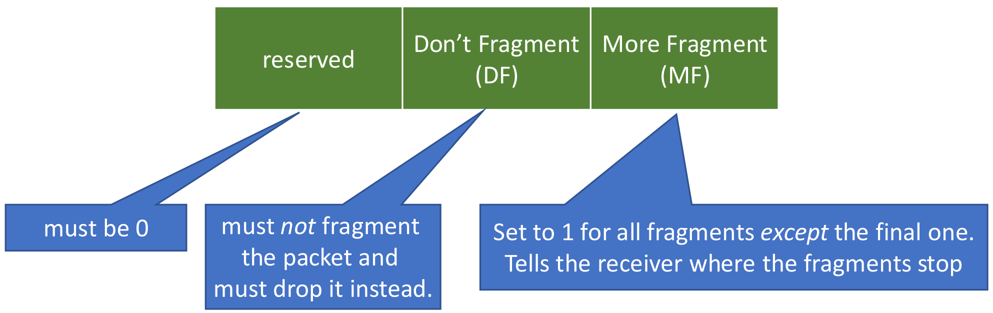
R1→R2	FragOffset
1st Fragment	
2nd Fragment	
3rd Fragment	
4th Fragment	

R2→R3	FragOffset
1st Fragment	
2nd Fragment	
3rd Fragment	
4th Fragment	

R3→B	FragOffset
1st Fragment	
2nd Fragment	
3rd Fragment	
4th Fragment	

2. Fragmentation

❖**Flag (3 bits)**



❖The fragments may not arrive in order.

➢The reassembler must identify when different arriving packets are fragments of the same original, and must figure out how to reassemble the fragments in the correct order.

2. Fragmentation

❖**Reassembly timer**

➢If a fragment arrives, a buffer is allocated.

- Because of the ***FragOffset*** field, the fragment can then be **stored** in the buffer **in the appropriate position**.

➢Reassembly timer is started.

➢When all fragments have arrived, the packet is sent on up as a completed IPv4 packet.

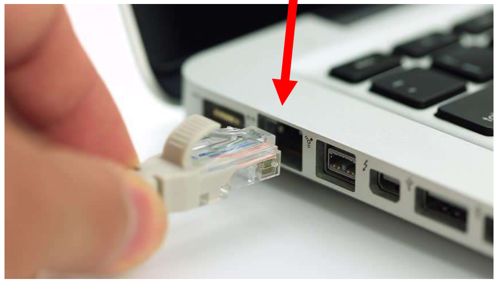
➢On the other hand, if the **reassembly timer expires**, all the pieces received so far are **discarded**.

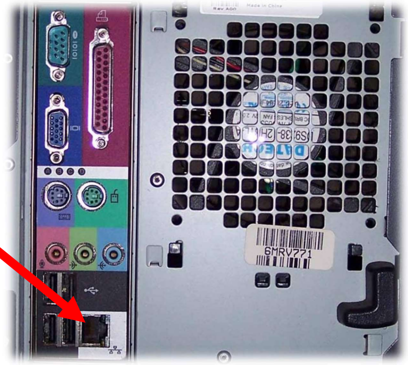
3 Interfaces

3. Interfaces

❖ IP addresses are assigned not to hosts or nodes, but to **interfaces**.

➢ E.g., LAN interface in PC.





3. Interfaces

❖ **Loopback** interface

➢ Providing a way to deliver IP packets to other processes on the same machine.

- IPv4 loopback address: "127.0.0.1"
- IPv6 loopback address: "::1"

➢ Client/server testing.

➢ Check the processes in current host.

❖ **Virtual** interface

➢ VPN connections.

➢ Virtual machine

3. Interfaces

❖ **Multihomed hosts**

➢ A non-router host with multiple non-loopback network interfaces is often said to be **multihomed**.

- Interfaces are been used simultaneously, with different IP addresses assigned to each.
- E.g., Laptops have both an Ethernet interface and a Wi-Fi interface.

4 Special Addresses

❖ **Private addresses**

- IPv4 addresses intended only for site internal use.
- If a packet shows up at any non-private router (e.g., at an ISP router), with a private IPv4 address as either source or destination address, the packet should be dropped.

- 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

❖ **Broadcast addresses**

- Used in conjunction with LAN-layer broadcast.
  - Sending a packet from one host to all hosts in the network.

❖ **Multicast addresses**

- The address with first byte beginning **1110**.
  - 224.0.0.0 to 239.255.255.255.
- Delivering to a specified set of addresses.
  - Examples:
    - Video and audio broadcasts
    - Routing information exchange by routing protocols
    - Distribution of software
    - Remote gaming

❖ **Broadcast addresses**

- Used in conjunction with LAN-layer broadcast.
  - Sending a packet from one host to all hosts in the network.

❖ **Multicast addresses**

- The address with first byte beginning **1110**.
  - 224.0.0.0 to 239.255.255.255.
    - **Link local** - 224.0.0.0 to 224.0.0.255 (E.g., routing information exchanged by routing protocols)
    - **Globally scoped addresses** - 224.0.1.0 to 238.255.255.255 (E.g., 224.0.1.1 has been reserved for Network Time Protocol)

4. Special Addresses

❖**Public Addresses:**

➢These addresses are designed to be used in the hosts that are publicly accessible from the Internet.

5 The Classless IP Delivery Algorithm

5. The Classless IP Delivery Algorithm

❖**Classful** (discontinuation)

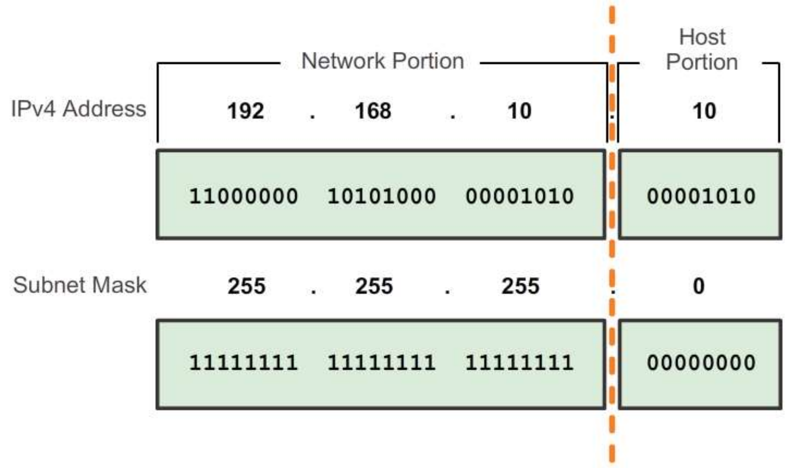
➢Fixed the network portion and host portion

Class	High Order Bits	First Octet Range	Number of Network Bits	Number of Host Bits	Number of Networks	Number of Hosts per Network
A	0	0-127	8	24	128	16,777,216
B	10	128-191	16	16	16,384	65,536
C	110	192-223	24	8	2,097,152	256
D	1110	224-239	Used for Multicasting to multiple hosts.			
E	1111	240-255	Reserved for research and development.			

5. The Classless IP Delivery Algorithm

❖**Classless**

➢Dynamic network portion and host portion



5. The Classless IP Delivery Algorithm

❖**Classless**

➢Dynamic network portion and host portion

IPv4 Address

11000000 10101000 00001010	00001010

Subnet Mask

11111111 11111111 11111111	00000000

Network Address

11000000 10101000 00001010	00000000

prefix length = 24 → 192.168.10.0/24

5. The Classless IP Delivery Algorithm

❖**IP Destination**

➢**Local**

- The host delivers the packet to its final destination via the LAN connected to the corresponding interface.

➢**Non-Local**

- The host **lookup** the forwarding table and sends the packet to the associated next_hop.

❖The forwarding table may also contain a ***default entry for the next_hop***, which it may return in cases when the destination does not match any known network. (**0.0.0.0/0**)

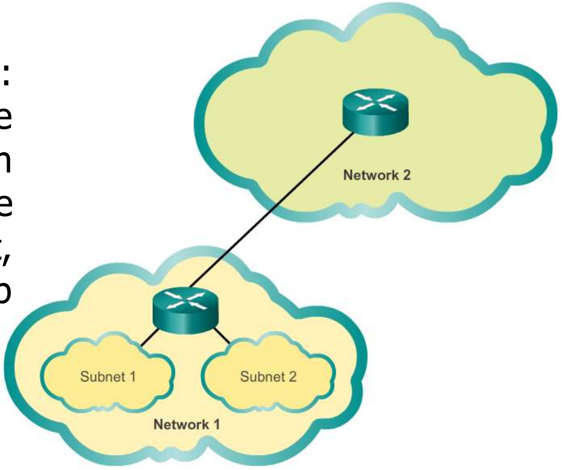
6 IPv4 Subnets

6. IPv4 Subnets

❖**Subnet**

➢Idea: A site to appear to the outside world as a single IP network, but for further IP-layer routing to be supported inside the site.

➢**Hierarchical routing**: first we route to the primary network, then inside that site we route to the subnet, and finally the last hop delivers to the host.



6. IPv4 Subnets

❖ Borrowing Bits (of Host portion) to create Subnets

➢ *EX: Borrowing 1 bit 2^1 = 2 subnets*

192.168.1.0/24 Network

Address	192	168	1	0000	0000
Mask	255	255	255	0000	0000
	Network Portion			Host Portion	

Net 0	192.	168.	1.	0	000	0000
Net 1	192.	168.	1.	1	000	0000
Mask	255.	255.	255.	1	000	0000

The borrowed bit value is **1** for the Net 1 address.

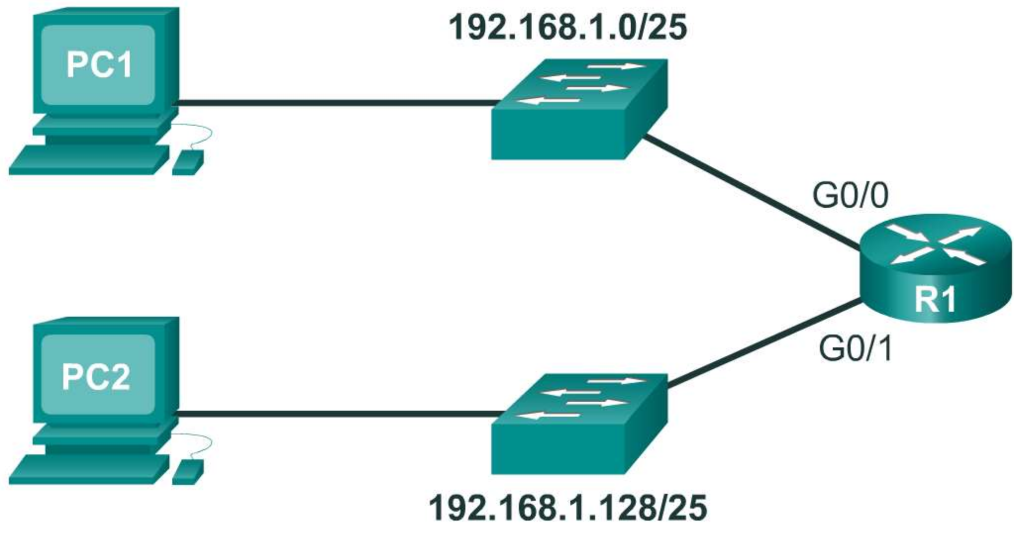
2 Subnets

The new subnets have the **SAME** subnet mask.

Network: 192.168.1.**0/25**
Mask: 255.255.255.**128**

Network: 192.168.1.**128/25**
Mask: 255.255.255.**128**

6. IPv4 Subnets



6. IPv4 Subnets

Address Range of **192.168.1.0/25** subnet

Network Address	192.	168.	1.	0	000	0000	= 192.168.1.0
First Host Address	192.	168.	1.	0	000	0001	= 192.168.1.1
Last Host Address	192.	168.	1.	0	111	1110	= 192.168.1.126
Broadcast Address	192.	168.	1.	0	111	1111	= 192.168.1.127

6. IPv4 Subnets

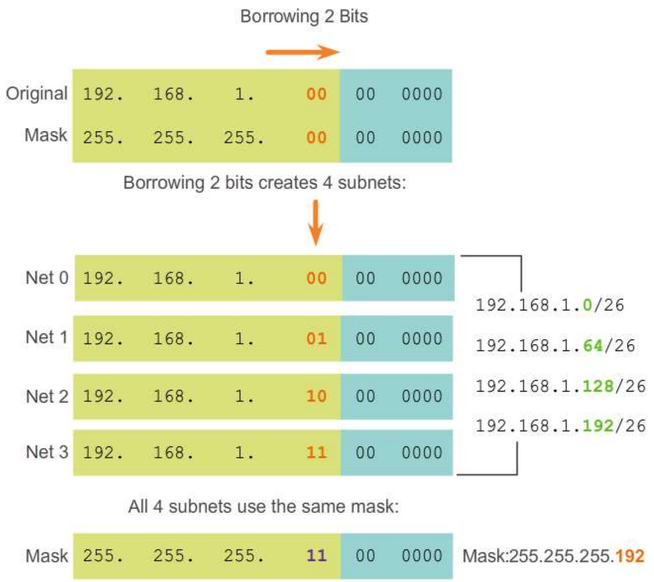
Address Range of **192.168.1.128/25** subnet

Network Address	192.	168.	1.	1	000	0000	= 192.168.1.128
First Host Address	192.	168.	1.	1	000	0001	= 192.168.1.129
Last Host Address	192.	168.	1.	1	111	1110	= 192.168.1.254
Broadcast Address	192.	168.	1.	1	111	1111	= 192.168.1.255

6. IPv4 Subnets

❖**Need 4 Subnets?**

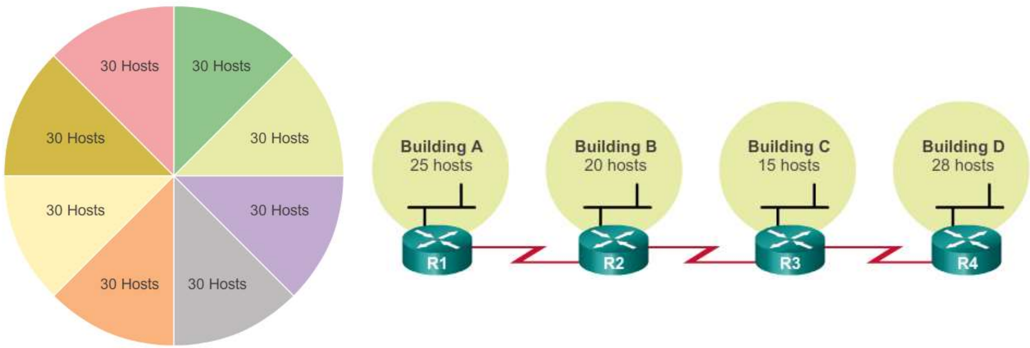
➢Borrowing 2 bits to create 4 subnets. **2^2 = 4 subnets**



7 VLSM (Variable Length Subnet Masking)

7. VLSM

❖Traditional subnetting - same number of addresses is allocated for each subnet.



❖Subnets that require fewer addresses have unused (**wasted**) addresses.

➢For example, WAN links only need 2 addresses.

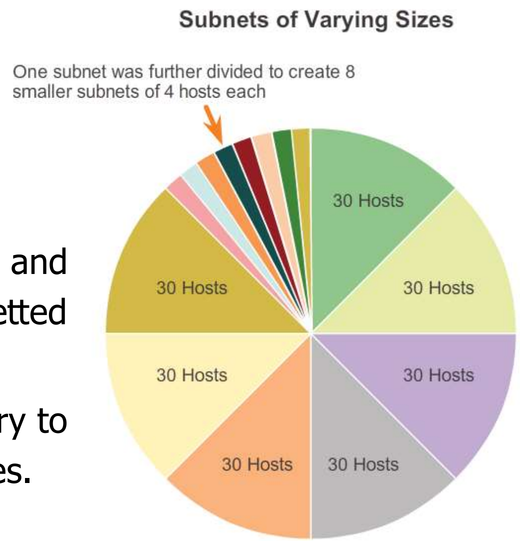
7. VLSM

❖**Variable Length Subnet Mask (VLSM)** or subnetting a subnet provides more efficient use of addresses.

❖ VLSM enables a network number to be configured with different subnet masks on different interfaces.

❖ Network is first subnetted, and then the subnets are subnetted again.

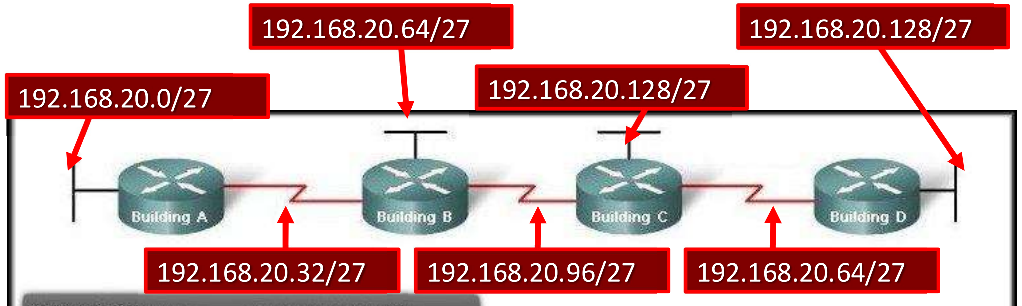
❖ Process repeated as necessary to create subnets of various sizes.



7. VLSM

10.0.0.0/8	Subnet	using /16		
Subnet	1st Host	Last Host	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	Subnet	1st Host	Last Host	Broadcast
Sub-subnet Using /24	**10.2.0.0/24**	**10.2.0.1**	**10.2.0.254**	**10.2.0.255**
	10.2.1.0/24	**10.2.1.1**	**10.2.1.254**	**10.2.1.255**
	10.2.2.0/24	**10.2.2.1**	**10.2.2.254**	**10.2.2.255**
	Etc.			
	10.2.255.0/24	**10.2.255.1**	**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	
Etc.				
10.255.0.0/16	10.255.0.1	10.255.255.254	10.255.255.255	

7. VLSM

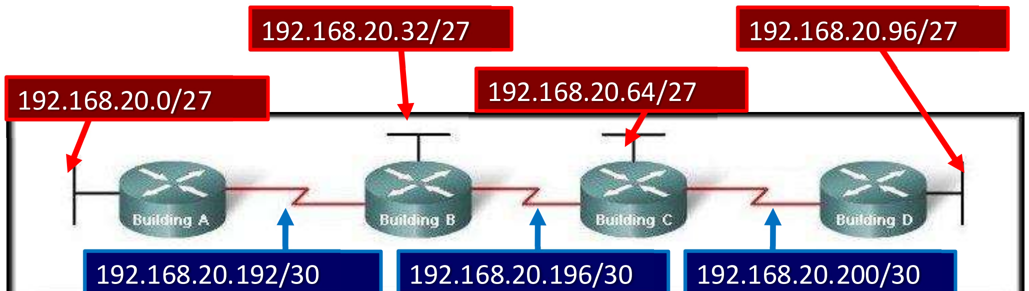


Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

7 Networks with 30 usable addresses for each network

Wasted 28 addresses on each WAN link

7. VLSM



Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.220/30

7. VLSM

❖Steps for VLSM:

1. List the number of hosts required per network beginning with the largest to the smallest.
2. Convert the subnet mask to binary.
3. Draw a line where the network portion ends.
4. Ask yourself the question… *How many bits do I need to support the required number of hosts?*
5. Move the line to show your new network portion.
6. Determine your new magic number.
7. Finish subnetting using the new magic number.

❖The starting address is always the first network.

❖You cannot go past the *next* network of the *previous level*.

8

Address Resolution Protocol: ARP

8. Address Resolution Protocol: ARP

❖ If a host finds that the destination IP address matches the network address of one of its interfaces, it is to deliver the packet via the LAN.

➢ Looking up the LAN address (MAC address).

→ARP

❖ **ARP cache:** Storing of <IPv4,LAN> address pairs for other hosts on the network.

➢ ARP-cache entries eventually expire. The timeout interval used to be on the order of 10 minutes, but Linux systems now use a much smaller timeout (~30 seconds observed in 2012).

8. Address Resolution Protocol: ARP

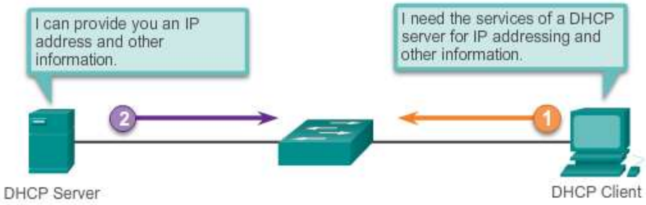
<VIDEO>

9

Dynamic Host Configuration Protocol (DHCP)

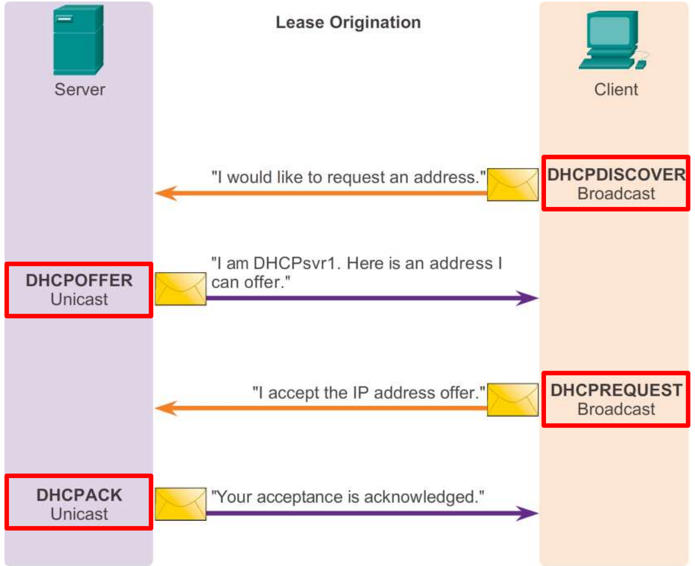
9. Dynamic Host Configuration Protocol (DHCP)

- DHCP works in a client/server mode.
  - When the client connects, the server assigns or leases an IP address to the device.
  - The device connects to the network with that leased IP address until the lease period expires.
  - The host must contact the DHCP server periodically to extend the lease.
  - The leasing of addresses assures that addresses that are no longer used are returned to the address pool for use by other devices.



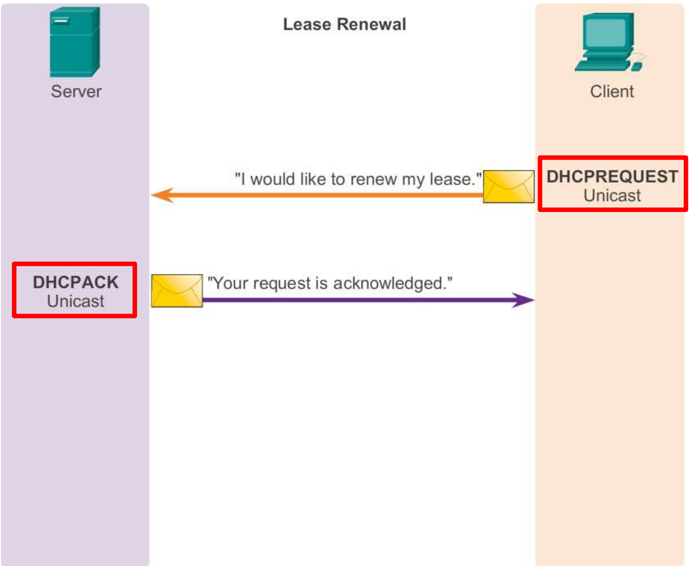
DHCPv4 Operation

❖**Lease Origination:** 4 Step Process.



9. Dynamic Host Configuration Protocol (DHCP)

❖**Lease Renewal:** 2 Step Process



10 Internet Control Message Protocol

10. Internet Control Message Protocol

❖ICMP is a protocol for sending IP-layer error and status messages.

❖ICMP messages are identified by an 8-bit type field.

Type	Description
Echo Request	`ping` queries
Echo Reply	`ping` responses
Destination Unreachable	Destination **network** unreachable
	Destination **host** unreachable
	Destination **port** unreachable
	Fragmentation required but DF flag set
	Network administratively prohibited
Source Quench	Congestion control
Redirect Message	Redirect datagram for the **network**
	Redirect datagram for the **host**
	Redirect for TOS and network
	Redirect for TOS and host
Router Solicitation	Router discovery/selection/solicitation
Time Exceeded	TTL expired in transit
	Fragment reassembly time exceeded
Bad IP Header or Parameter	Pointer indicates the error
	Missing a required option
	Bad length
Timestamp Timestamp Reply	Like `ping`, but requesting a timestamp from the destination

Queries sent by one host to another

Error sent by a router to sender

10. Internet Control Message Protocol

❖The **Destination Unreachable** type has a large number of subtypes:

- ➢**Network unreachable:** some router had no entry for forwarding the packet, and no default route
- ➢**Host unreachable:** the packet reached a router that was on the same LAN as the host, but the host failed to respond to ARP queries
- ➢**Port unreachable:** the packet was sent to a UDP port on a given host, but that port was not open. TCP, on the other hand, deals with this situation by replying to the connecting endpoint with a reset packet. Unfortunately, the UDP Port Unreachable message is sent to the host, not to the application on that host that sent the undeliverable packet, and so is close to useless as a practical way for applications to be informed when packets cannot be delivered.

10. Internet Control Message Protocol

❖The **Destination Unreachable** type has a large number of subtypes:

- ➢**Fragmentation required but DF flag set:** a packet arrived at a router and was too big to be forwarded without fragmentation. However, the Don't Fragment bit in the IPv4 header was set, forbidding fragmentation.

- ➢**Administratively Prohibited:** this is sent by a router that knows it can reach the network in question, but has configure intro to drop the packet and send back Administratively Prohibited messages. A router can also be configured to blackhole messages: to drop the packet and send back nothing.

10. Internet Control Message Protocol

❖**Traceroute and Time Exceeded**

- ➢The traceroute program uses ICMP Time Exceeded messages.

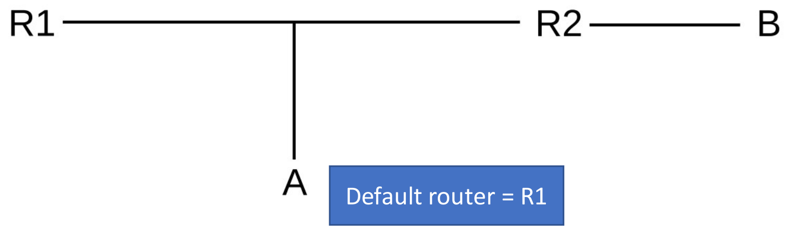
- ➢A packet is sent to the destination with the **TTL** set from **1** until the ICMP query reaches to the destination.
  - Router drops packet having TTL = 0 and returns ICMP Time Exceeded.

10. Internet Control Message Protocol

❖**Redirects**

➢Most non-router hosts start up with an IPv4 forwarding table consisting of a single (default) router.

➢ICMP Redirect messages help hosts learn of other useful routers.



❖**Router Solicitation**

➢These ICMP messages are used by some router protocols to identify immediate neighbors.

QA

Lecturer: Nguyen Viet Ha, Ph.D.
Ho Chi Minh City University of Science
Faculty of Electronics and Communications
Department of Telecommunication and Networks
Email: nvha@fetel.hcmus.edu.vn