PROGRAMME: BACHELOR OF SCIENCE IN COMPUTER SCIENCE

DEPARTMENT: COMPUTING & INFORMATION TECHNOLOGY

FACULTY: MANAGEMENT SCIENCES

COUESE UNIT: COMPUTER NETWORKS AND DATA
COMMUNICATION

LECTURER: BAHITYA PATRICK

STUDENT NAME: ABARIKURUNGI BUDGET

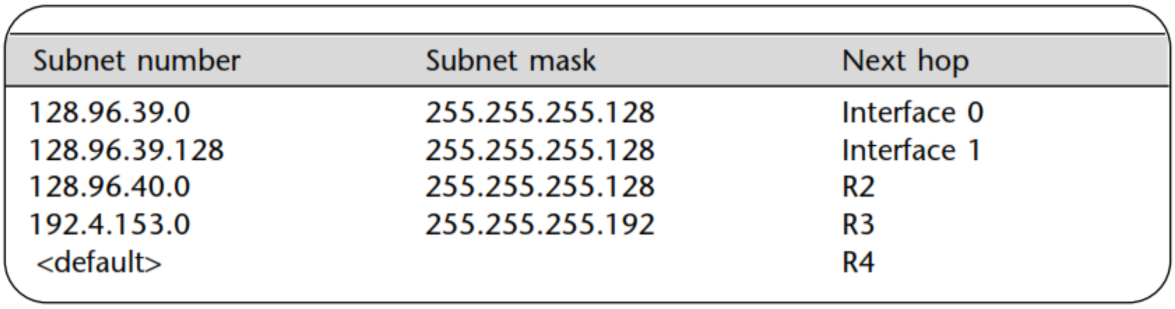
REG NO:19/U/0076/LCS

COURSEWORK II LCS 3201

YEAR III **SEMETSTER II**

Questions:

1. A router has built the routing table shown in the table below. The router can route packets directly to Ethernet interfaces 0 or 1, or it can forward packets to routers R2, R3 or R4. Describe what the router does with a packet addressed to each of the following destinations:
   (a) 128.96.39.10
   (b) 128.96.40.12
   (c) 128.96.40.151
   (d) 192.4.153.17
   (e) 192.4.153.90



Subnet number	Subnet mask	Next hop
128.96.39.0	255.255.255.128	Interface 0
128.96.39.128	255.255.255.128	Interface 1
128.96.40.0	255.255.255.128	R2
192.4.153.0	255.255.255.192	R3
<default>		R4

2. With reference to IP version 4:
   (a) What are the three main classes of IP addresses?
   (b) How are the bits distributed between host and network in each of these classes?
   (c) What is the purpose of the time-to-live field in an IP header?
   (d) What happens when time-to-live reaches zero?
3. Briefly outline the CSMA/CA medium access technique used in wireless LANs.
b. Explain why the earlier CSMA/CD LAN protocol does not lend itself to use in WLANs.
4. What is Mobile IP and how does it work?

Question 1:

The router applies each subnet mask on the address and if the subnet number matches any entry in the subnet number entry, then it uses the entry in the next hop column to send the data packets.

a) 128.96.39.10

Given the host IP address and the subnet mask, we can obtain the network address to which that host is connected and thus identify the next hop. The network address can be obtained by ANDing the subnet mask with the host IP address. The next hop is the device/interface through which the router can send data packets towards the destination.

For a)

With Subnet Mask 1

Host IP 128.96.39.10 = 10000000 01100000 00100111 00001010
AND
Subnet mask 1 255.255.255.128 = 11111111 11111111 11111111 10000000
Network Address = 10000000 01100000 00100111 00000000 = 128.96.39.0

With Subnet Mask 2

Host IP 128.96.39.10 = 10000000 01100000 00100111 00001010
AND
Subnet mask 2 255.255.255.192 = 11111111 11111111 11111111 10000000
Network Address = 10000000 01100000 00100111 00000000 = 128.96.39.0
Since ANDing the host IP address with each subnet mask gives the same network address as 128.96.39.0, the router will send the data packets to this host through **Ethernet interface 0** as the next hop.

For b)
With Subnet Mask 1
Host IP 128.96.40.12 = 10000000 01100000 00101000 00001100
AND
Subnet mask 1 255.255.255.128 = 11111111 11111111 11111111 10000000
Network Address = 10000000 01100000 00101000 00000000 = 128.96.40.0
With Subnet Mask 2
Host IP 128.96.40.12 = 10000000 01100000 00100111 00001010
AND
Subnet mask 2 255.255.255.192 = 11111111 11111111 11111111 10000000
Network Address = 10000000 01100000 00101000 00000000 = 128.96.40.0
Since ANDing the host IP address 128.96.40.12 with each subnet mask gives the same network address as 128.96.40.0, the router will send the data packets to this host through **router R2** as the next hop.

For c)
With Subnet Mask 1
Host IP 128.96.40.151 = 10000000 01100000 00101000 10010111
AND
Subnet mask 1 255.255.255.128 = 11111111 11111111 11111111 10000000
Network Address = 10000000 01100000 00101000 10000000 = 128.96.40.128
With Subnet Mask 2
Host IP 128.96.40.151 = 10000000 01100000 00100111 10010111
AND
Subnet mask 2 255.255.255.192 = 11111111 11111111 11111111 11000000
Network Address = 10000000 01100000 00101000 10000000 = 128.96.40.128
Since ANDing the host IP address 128.96.40.151 with each subnet mask gives the same network address as 128.96.40.128, the router will send the data packets to this host using the default route through **R4** as the next hop since there is no corresponding subnet address.

For d)
With Subnet Mask 1
Host IP 192.4.153.17 = 11000000 00000100 10011001 00010001
AND
Subnet mask 1 255.255.255.128 = 11111111 11111111 11111111 10000000
Network Address = 11000000 00000100 10011001 00000000 = 192.4.153.0
With Subnet Mask 2
Host IP 192.4.153.17 = 11000000 00000100 10011001 00010001
AND
Subnet mask 2 255.255.255.192 = 11111111 11111111 11111111 11000000
Network Address = 11000000 00000100 10011001 00000000 = 192.4.153.0

Since ANDing the host IP address 192.4.153.17 with each subnet mask gives the same network address as 192.4.153.0, the router will send the data packets to this host through **router R3** as the next hop.

For e)
With Subnet Mask 1
Host IP 192.4.153.90 = 11000000 00000100 10011001 01011010
AND
Subnet mask 1 255.255.255.128 = 11111111 11111111 11111111 10000000
Network Address = 11000000 00000100 10011001 01000000 = 192.4.153.64
With Subnet Mask 2
Host IP 192.4.153.90 = 11000000 00000100 10011001 01011010
AND
Subnet mask 2 255.255.255.192 = 11111111 11111111 11111111 11000000
Network Address = 11000000 00000100 10011001 01000000 = 192.4.153.64

Since ANDing the host IP address 192.4.153.90 with each subnet mask gives the same network address as 192.4.153.64, the router will send the data packets to this host through the default route using **router R4** as the next hop since there is no matching network address.

2a) What are the three main classes of IP addresses?

The table below shows the main three classes of the IP address

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.

2b) How are the bits distributed between host and network in each of these classes?

Network Classes

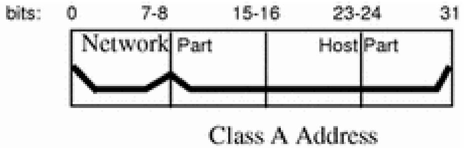
The first step in planning for IP addressing on your network is to determine which network class is appropriate for your network. After you have done this, you can take the crucial second step: obtain the network number from the InterNIC addressing authority.

Currently there are three classes of TCP/IP networks. Each class uses the **32-bit IP address** space differently, providing more or fewer bits for the network part of the address. These classes are class A, class B, and class C.

Class A Network Numbers

A class A network number uses the first **8 bits** of the IP address as its "network part." The remaining **24 bits** comprise the host part of the IP address, as illustrated below. Figure 3-2 graphically illustrates a class A address.

Figure 3-2 Byte Assignment in a Class A Address

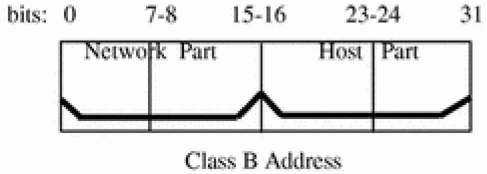


The values assigned to the first byte of class A network numbers fall within the range 0-127. Consider the IP address 75.4.10.4. The value 75 in the first byte indicates that the host is on a class A network. The remaining bytes, 4.10.4, establish the host address. The InterNIC assigns only the first byte of a class A number. Use of the remaining three bytes is left to the discretion of the owner of the network number. Only 127 class A networks can exist. Each one of these numbers can accommodate up to 16,777,214 hosts.

Class B Network Numbers

A class B network number uses **16 bits** for the network number and **16 bits** for host numbers. The first byte of a class B network number is in the range 128-191. In the number 129.144.50.56, the first two bytes, 129.144, are assigned by the InterNIC, and comprise the network address. The last two bytes, 50.56, make up the host address, and are assigned at the discretion of the owner of the network number. Figure 3-3 graphically illustrates a class B address.

Figure 3-3 Byte Assignment in a Class B Address

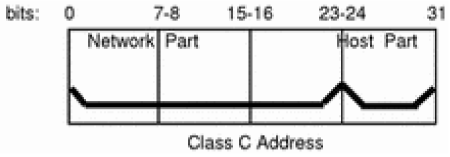


Class B is typically assigned to organizations with many hosts on their networks.

Class C Network Numbers

Class C network numbers use **24 bits** for the network number and **8 bits** for host numbers. Class C network numbers are appropriate for networks with few hosts--the maximum being 254. A class C network number occupies the first three bytes of an IP address. Only the fourth byte is assigned at the discretion of the network owners. Figure 3-4 graphically represents the bytes in a class C address.

Figure 3-4 Byte Assignment in a Class C Address



The first byte of a class C network number covers the range 192-223. The second and third each cover the range 1- 255. A typical class C address might be 192.5.2.5. The first three bytes, 192.5.2, form the network number. The final byte in this example, 5, is the host number.

2c) What is the purpose of the time-to-live field in an IP header?

Time-to-live in networking refers to the time limit imposed on the data packet to be in-network before being discarded. It is an **8-bit binary value** set in the header of Internet Protocol (IP) by the sending host.

The purpose of the TTL field is **to avoid a situation in which an undeliverable datagram keeps circulating on an Internet system**, and such a system eventually becoming swamped by such "immortals". **The maximum TTL value is 255.** The value of TTL can be set from 1 to 255 by the administrators.

2d) What happens when time-to-live reaches zero?

When the TTL count is 0, after the final subtraction, **the packet is discarded by the router**. This triggers an Internet Control Message Protocol (ICMP) message that's sent back to the originating host.

So, when a packet begins its journey from the origin to its destination, a TTL (time to live) count is put into the packet. (This is for IPv4 - IPv6 have a ‘hop limit’)

Every time on the way a router receives the packet, it subtracts one from the TTL count and passes it on to the next hop. At some point, the TTL field for a given packet may reach zero, at which point that router doesn’t forward the packet any more. Rather, it returns an ICMP packet back to tell the source that the TTL expired. It’s a reasonable way of stopping packets circulating forever

3a) Briefly outline the CSMA/CA medium access technique used in wireless LANs

CSMA/CA which is an acronym of Carrier sense multiple access/collision avoidance is **a protocol for carrier transmission in 802.11 networks**. It was developed to minimize the potential of a collision occurring when two or more stations send their signals over a data link layer. The basic idea behind CSMA/CA is the “**Listen Before Talk**” (LBT) principle. This means that the line has to be checked to see if it’s free (“idle”) before the station can start a transmission.

- ❖ Distributed coordination function (DCF)
- ❖ Request to send and clear to send (RTS/CTS)
- ❖ Network allocation vector (NAV)
- ❖ The CSMA/CA procedure at a glance

Distributed coordination function (DCF)

Within CSMA/CA, the distributed coordination function (DCF) controls the time a station waits before initiating transmission in a free medium. DCF also assigns certain time slots to network participants for further actions, creating a **binding time structure**. This procedure is the focus of collision avoidance: a complex time structure that makes it possible to avoid collisions. DCF takes various intervals into account when creating the time structure.

DCF interframe space (DIFS): In the first step, participants must monitor the network for the duration of the DIFS to determine whether it’s currently free. For CSMA/CA, this means that no other station within range is sending out a transmission at the same time. The DIFS results from the SIFS almost double the slot time, which is between 28 and 50 µs long.

- **Contention window**: If participants determine that the channel is free, they wait a random amount of time before they start sending. This duration corresponds to the contention window. This time window doubles with each collision and corresponds to the binary exponential backoff (BEB) that is familiar from CSMA/CD.

- **Short interframe space** (SIFS): After sending the data packet, the recipient node sends a notification – if the RTS/CTS procedure is also utilized. However, this station also waits for a fixed time before sending.

SIFS is the time it takes to process a data package. The duration depends on the IEEE-802.11 standard and is between 10 µs and 16 µs.

Request to send and clear to send (RTS/CTS)

The frames "Request to Send" (RTS) and "Clear to Send" (CTS) are part of the optional extension CSMA/CA RTS/CTS. This procedure is **upstream of the actual data transmission**. If a participant determines that the transmission medium is free, the device first sends an RTS frame to the participant that is to receive the data. With this, the output computer makes it clear that it wants to start a transmission and will occupy the transmission medium for a certain time.

The receiver, in turn, sends a CTS frame to the original sender. As with the RTS frame, all other participants in the range are informed that the transmission is currently occupied and the transmitter is enabled for transmission. Only then does the original device start transmitting the data. Now it is not possible for the participants in a wireless network to detect collisions or other interference during transmission. For this reason, the receiving station needs to send an **acknowledgement** (ACK) when the data packet has arrived correctly.

If the ACK frame doesn't appear, the sender of the data assumes that a complication has occurred and resends the data packet. The station has a **preferential right** to use the medium and doesn't have to wait again for the channel to be free. The three frame types each consist of several fields.

- **Frame control**: the FC field contained in each 802.11 frame is 2 bytes (16 bits) and again divided into several elements:

    - Protocol version: specifies the version of the protocol used
    - Type: specifies whether it is a control frame (as with RTS/CTS and ACK), data frame, or management frame
    - Sub-type: specifies the type of frame by defining one of the 25 sub categories
    - To distribution system: is set when the frame goes to a distribution system
    - From distribution system: is set if the frame comes from a distribution system
    - More fragments: only has content if more frames follow (only relevant for data frames and management frames)
    - Retry: specifies whether and how often the frame has already been sent
    - Power management: shows the power saving mode
    - More data: specifies that more data should be sent
    - WEP: indicates whether the data is encrypted with WEP
    - Order: tells the recipient whether the data is sent in the correct order

- **Duration**: specifies the time the transmitter needs for data transmission (this information is crucial for the network allocation vector and has a size of 2 bytes)
- **Receiver address**: contains the MAC address of the receiver (6 bytes)
- **Transmitter address**: contains the MAC address of the sender (6 bytes); only required for RTS, not for CTS, and ACK
- **Frame check sequence**: the 4-byte block check sequence is a checksum that enables the receiving station to determine whether the data frame has arrived as planned. The sender calculates the checksum from the data of the frame. The same process also takes place on the receiver's side when the frame has arrived. If the receiver's result matches what the sender attached to the frame as FCS, the transmission was successful.

Network allocation vector (NAV)

Before a device in the network starts a transmission, it first sends information (in the duration field of the RTS frame) to all other participants. The station reveals how long the network will be occupied by the transmission. Every other device enters this information in its very personal **network allocation vector** (which is not really a vector from a mathematical point of view). This is managed internally and specifies the time when a delivery attempt is possible again. The network allocation vector (NAV) counts down continuously and is only replenished by new information from other stations.

The CSMA/CA procedure at a glance

If participants in a wireless network follow Carrier Sense Multiple Access with Collision Avoidance, certain steps must be adhered to. First, the stations monitor the transmission medium. When it comes to WLAN, this means that carrier sense **monitors the radio channel** and checks whether other network participants.

If it turns out that the transmission medium is currently occupied, a **random backoff** is initiated: the station waits a random amount of time until a new check starts. All other stations, which are not busy with sending or receiving, experience the same.

If the network is free, the station initiates **DCF**. First, the channel is checked more thoroughly for the duration of DIFS.

As this happens, all other participants are informed that the network is currently in use. This causes them to raise their network allocation vector again and wait to try again to see if the channel is free. Then **the station starts the transmission**. When this is finished, the receiver waits for the duration of an SIFS and then responds with an ACK frame to confirm to the sender that everything has been fully received and to set the network allocation vector to 0, showing that the network is free for a new transmission.

3b). Explain why the earlier CSMA/CD LAN protocol does not lend itself to use in WLANs.

CD doesn’t work on a wireless network, because the antenna can only transmit or receive at any given time, so it cannot listen for a collision *while* it’s sending data. Instead, wireless networks use CSMA/CA (Collision Avoidance), which send an RTS signal (Ready to Send) before transmitting actual data. When other devices hear that RTS, they know someone’s about to send, so they wait.

Why do they use it? Because today, Wi-Fi is probably the only common implementation of Ethernet that actually still requires it. It’s the only one that still uses a multi-access model. Most wired Ethernet, today, is switched, and full-duplex, so there is never any contention.

Remember, on a multi-access network, only one speaker is allowed at a time. You can’t have everyone talking at once, because it’s all going across the same carrier. That was true in old bus or hub Ethernet. It’s still true with Wi-Fi. And since only one device can talk at a time, you have to listen first to hear if anyone else is speaking before you try to talk. If someone is, you back off and try again soon.

4a. What is Mobile IP and how does it work?

Mobile IP is an internet engineering task force standard communication protocols designed to allow mobile device users to move from one network to another without changing their IP address.

how does it work?

There are three main phases for mobile IP

- ❖ Agent Discovery
- ❖ Registration
- ❖ Tunneling

Agent Discovery

A mobile node discovery its current location (Home agent and foreign agent) during agent discovery.

This process is done by either the Agent Advertisement or Agent Solicitation communication process.

Agent Advertisement

- Home Agent and Foreign Agent advertises their presence periodically on the network to which they are attached by using ICMP (internet control message protocol)
- The FA periodically broadcasts the Internet Router Discovery Protocol (IRDP) message RFC 1256 in its own network to let the visited MN know the FA is here and what services the FA provides (Agent Advertisement). Thus, the MN knows which network it belongs to.

Agent Solicitation

Foreign agents are expected to issue agent advertisement messages periodically. In case the MN does not receive information from agent advertisement, it can request the service by sending a solicitation message to inform the FA directly (Agent Solicitation)

If there is no answer back during a limited time, the MN attempts to use the Dynamic Host
Configuration Protocol (DHCP) to acquire a new IP address. Both the advertisement and the solicitation protocols are the same as the IRDP. A destination address in the IRDP packet can be used as either a multicast address or a broadcast

REGISTRATION

After a discovery phase, the MN has to send a registration or deregistration request message with its updated COA back to the HA. After that, a registration reply message will be sent back to the MN to confirm the registration process.

Mobile node registration takes place in two phases.

When the COA is at FA, the mobile node sends its registration request containing COA to the FA which forwards the request to HA. The HA then sets a mobility binding containing the mobile node home IP address, the current COA and registration lifetime negotiated during registration process. Registration expires automatically after the lifetime and is eventually deleted. The HA the send back a reply message to FA which finally forwards it to MN.

When COA is co-located. In this situation the mobile node sends request directly to HA and vice versa.

In case the MN returns to its home network, the MN still sends the registration message to
deregister it from the HA.

TUNNELING

Is used to forward IP datagrams from a home address to a Care-of Address

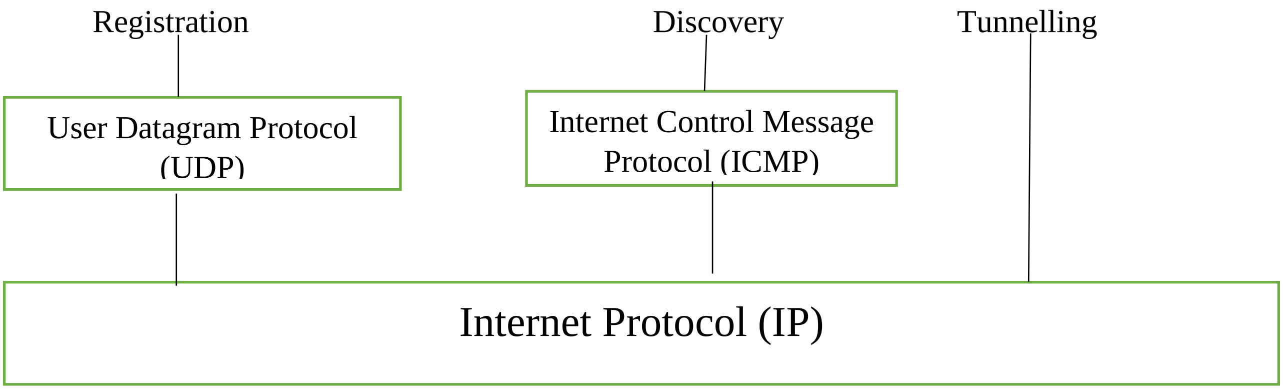
Home agent intercepts IP datagrams sent to mobile node's home address

Home agent informs other nodes on home network that datagrams to mobile node should be delivered to home agent

Datagrams forwarded to care-of address via tunnelling

Datagram encapsulated in outer IP datagram

DIAGRAM SHOWING INTERACTION BETWEEN PHASES


Registration
Discovery
Tunnelling
User Datagram Protocol (UDP)
Internet Control Message Protocol (ICMP)
Internet Protocol (IP)

REFERENCES:

https://docs.oracle.com/cd/E19504-01/802-5753/planning3-78185/index.html

https://www.geeksforgeeks.org/what-is-time-to-live-ttl/

https://www.quora.com/What-is-the-purpose-of-the-time-to-live-field-in-the-IP-header

https://www.quora.com/What-happens-when-TTL-expires

https://www.ionos.com/digitalguide/server/know-how/csmaca-carrier-sense-multiple-access-with-collision-avoidance/

https://www.quora.com/Why-is-CSMA-CD-used-in-wireless-LAN-What-can-be-the-problem-if-CSMA-CD-is-used-in-the-above