دانشگاه صنعتی اصفهان

IT Fundamentals

Assignment 1

Author: Melvin Mokhtari

Student ID: 9831143

Instructor: **Dr. Mohammad Hossein Manshaei**

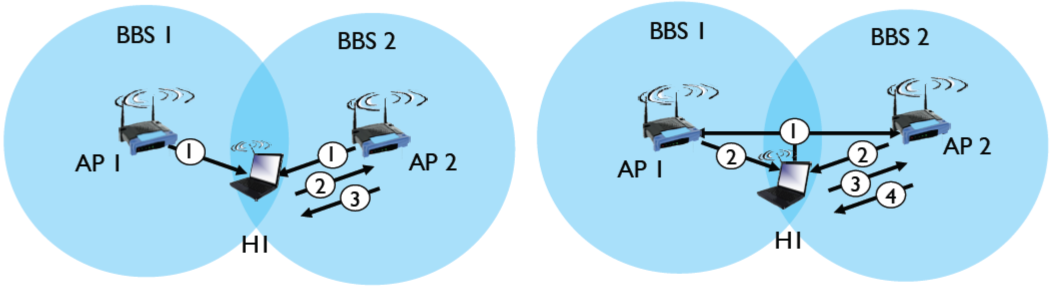
Date Last Edited: March 12, 2022

Problem 1
Answer the following questions briefly:

- Describe the role of beacon frames and probe frames in 802.11.
- What is the relation between BER and SNR?
- What are the differences between a master device in a Bluetooth network and a base station in an 802.11 network?

Solution

• The access points (APs) have to broadcast the beacon frames periodically over one of the 11 channels, according to the 802.11 standard. A beacon frame carries the SSID and MAC address of an AP. When a wireless station enters a Wi-Fi jungle (which is formed by two or more APs), it scans 11 channels and seeks beacon frames from different APs. A wireless station can be associated with one of the available APs after knowing about them through beacon frames. Therefore, the role of a beacon frame is to help a wireless station discover and identify a nearby access point to associate with it.



passive scanning:
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

active scanning:
(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

• There is an inverse relationship between SNR (Signal to Noise Ratio) and BER (Bit Error Rate). When BER rises, the SNR falls, and when BER falls, the SNR rises. Because a sender can raise SNR by increasing transmission power, it can also lower the likelihood that a frame is received incorrectly by increasing transmission power.

• There are mainly three differences between a master device in a Bluetooth network and a base station in an 802.11 network. These are listed below:

1. A master device is used in a Bluetooth network (an ad-hoc network), but a base station is used in infrastructure networks such as 802.11 networks.

2. The master device sets up the Bluetooth network and manages all communications in the network. Simply, it rules the network. On the other hand, the base station is responsible only for sending and receiving data to and from a wireless host associated with that base station.

3. Moreover, any ordinary Bluetooth node (smartphone, PDA, etc.) can be a master node in a Bluetooth network, but special devices such as access points act as base stations in 802.11 networks. Access points cannot be used by standard wireless devices such as laptops, cell phones, and PDAs.

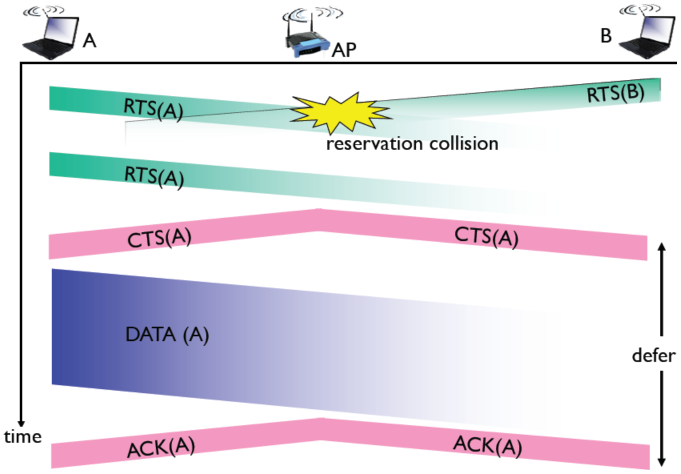
Problem 2
How can you activate RTS/CTS transmission in your WiFi devices? Explain which condition a station will check before sending a packet; when you activate RTS/CTS mode, why?

Solution
RTS/CTS (Request To Send / Clear To Send) helps prevent problems when wireless clients can receive signals from more than one access point on the same channel. The problem is known as ”hidden node”. By default, 802.11 relies on physical carrier sensing only, which is known to suffer from this problem.
Generally, it is not recommended to change the default RTS threshold but when the RTS Threshold is set to the default of 2346, RTS/CTS is disabled. If we lower this value incrementally, we can introduce more latency into the network. After each change, we have to decide whether the change in network performance is positive before making it again.
However, there are some issues to consider in this process:

- If there are a large number of collisions and users are far apart, then it is best to activate the RTS/CTS. After an RTS frame is received from a user, the access point will respond with a CTS frame.
- A highly mobile user can remain hidden for a short time period during testing, then get closer to other stations most of the time. If collisions occur between users within range of each other, the issue may be the result of RF interference or high network utilization.
- In several instances, enabling RTS/CTS in the access point is useless if the hidden station issue does not exist. All stations with valid associations are in range and not hidden from the access point; forcing the access point to implement the RTS/CTS connection will reduce throughput. So, if there is no hidden node problem, changing the threshold may not improve performance.

NOTE For activating RTS/CTS on access points, the user configuration interface needs to set a specific packet size threshold. The threshold range is around 0 – 2347 bytes; if the packet transmitted by the access point is larger than the threshold, the RTS/CTS function will be initiated. If the packet size is less than the threshold or below average, the function will not initiate.

When we activate RTS/CTS on a station, it refrains from sending a data frame until that particular station completes the connection with another station. The access point will transfer a CTS frame after receiving the RTS frame. The CTS features a time value that will alert other stations to hold access to the medium while the station that initiates the RTS transmits the data.
In other words, a transmitter raises its RTS line, which causes an interrupt on the receiver, i.e., ”Hey, can I send some data”? If the receiver is in a position to receive the data, it will assert its CTS line, i.e., ”Yes, you can start sending.” The raising and lowering of these lines allows device drivers to maintain a reliable data connection between transmitter and receiver, and bad data in transit does not affect flow control mechanism.



Problem 3
Describe the main differences between the three versions of SNMP (i.e., SNMP v1, v2 and v3), by reading the related RFCs.

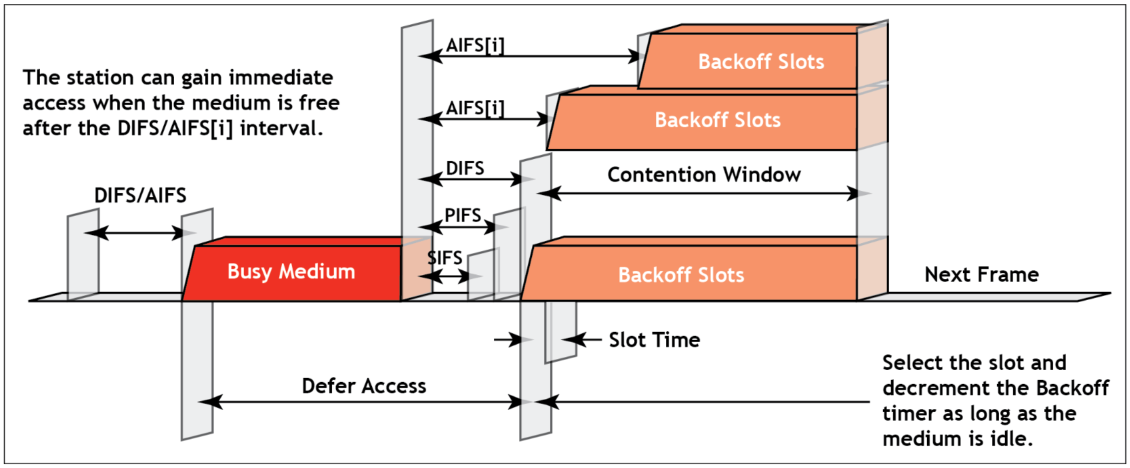
Solution
SNMPv2 and v3 are improved versions of the SNMP protocol, but SNMPv3 is more secure and performs better than version 2. However, SNMPV2 is a more widely used protocol version, but some people now consider version 2 obsolete. Version 2 was introduced with informed features that acknowledged the receipt of messages by the manager, while version 3 authenticates each message and ensures privacy.
Moreover, GetBulk and the TRAP2 and INFORM commands are missing from SNMPv1. SNMPv2c is a minor change to SNMPv1 that only adds these three commands.
In the table below, we'll find a more detailed comparison:

Cotent	SNMPv1	SNMPv2	SNMPv3
Standards	RFC-1155.1157.1212	RFC-1441.1452 RFC-1901 to 1910	RFC-1902 to 1908, 2271 to 2275
Version	SNMPv1 was the first version of SNMP	SNMPv2 currently exist in SNMPv2c, SNMPv2u, SNMPv2	SNMPv3 is the newest version of SNMP
Protocol Operations	Simple request / response protocol. Protocol operations: Get, GetNext, Set, and Trap	Similarity: Get, GetNext, Set Changes: Trap, New: GetBulk and Inform	SNMPv3 uses SNMPv2 protocol operations and its PDU message format
Security	No security from someone in the network	SNMPv2 failed to improve security	Its primary feature is enhanced security
Complexity	Performance and security limitations	More powerful but more complex than SNMPv1	SNMPv3 focuses on improving security aspects
Message Format	Five messages (GetRequest, GetNextRequest, SetRequest, Trap, Response)	Seven messages instead of five (inform-request, get-bulk-request)	Implements SNMP v1 and v2 specifications along with proposed new features
Protocol	An open, standard, streamlined protocol	Simple request / response protocol	The "EngineID" Identifier in SNMPv3 uniquely identifies each SNMP entity
MIB	Defines limited, implemented MIB of scalar variables and two dimensional tables	Defines general framework with which MIB defined and constructed	Can configure agents to provide a number of levels of access to MIB
Plaintext community strings	Yes	Yes	No
Detection of malformed packets	No	Yes	Yes
Susceptible to injection attacks	Yes	No	No
Susceptible to replay attacks	Yes	No	No
Susceptible to sniffing of session keys	Yes	No	No
Default / known passwords	Yes	Yes	No

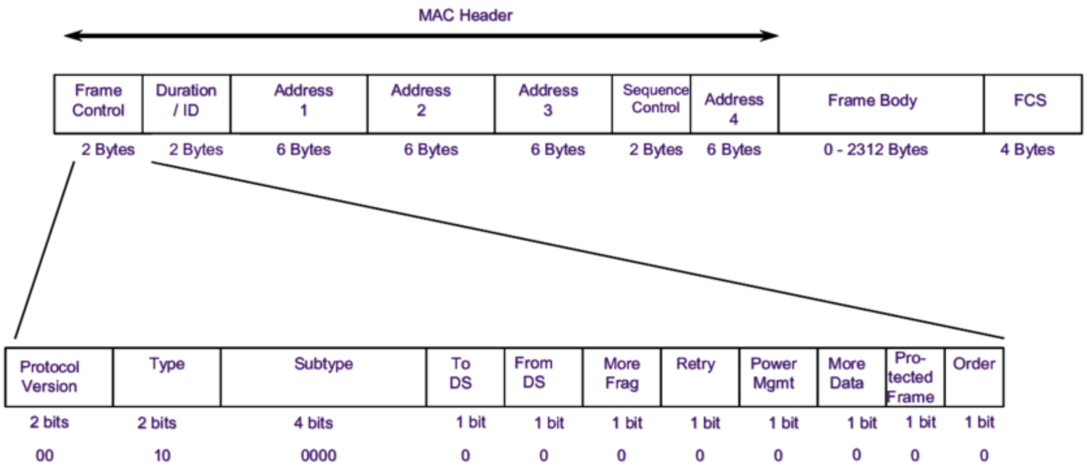
Problem 4
Consider the frame format of 802.11 presented in the lectures. Let us assume that the transmission rate for header and payload are R_H and R_P, respectively. How much time do we need to transmit this frame in 802.11? How do we compute the duration field given these rates? Now consider that you should use RTS and CTS packets. Explain how the duration field must be calculated in the MAC header of 802.11 packets, i.e., for all RTS, CTS, Data, and ACK packets.

Solution

This question is a little vague. For instance, in the sentence ”How much time do we need to transmit this frame in 802.11?”, ”this” is ambiguous! If it means an 802.11 frame, what does it mean to transfer an 802.11 frame into an 802.11 frame? And definitely, ”this” was not referred to as a header or payload because they are part of the 802.11 frame. I think something was missing here, and I imagine this ”this” refers to ”data,” and the whole question aims to calculate the data transmission time or in other words, the average time per packet in two different scenarios: with RTS/CTS and without RTS/CTS!
The 802.11 currently defines at least three interframe spaces, as shown in figure below:


The station can gain immediate access when the medium is free after the DIFS/AIFS[i] interval.
DIFS/AIFS
Busy Medium
AIFS[i]
AIFS[i]
DIFS
PIFS
SIFS
Backoff Slots
Backoff Slots
Contention Window
Backoff Slots
Next Frame
Slot Time
Defer Access
Select the slot and decrement the Backoff timer as long as the medium is idle.

Interframe allow 802.11 to control which traffic gets first access to the channel after carrier sense declares the channel to be free. The Short InterFrame Spacing (SIFS) value is used for acknowledgments that must directly follow the previous data frame; DCF InterFrame Spacing (DIFS) is used for non-QoS data frames; Arbitrated InterFrame Spacing (AIFS) is used for QoS data frames and is variable based on the WMM Access Category (AC) to which the frame is assigned.
We also know that the 802.11 frame is formed like the figure below:



Before discussing the formula to find the time per packet in 802.11, I must first declare some other variables and their procedures:

- DIFS Time = The amount of time a wireless station waits to send after sensing channel is clear
- SIFS Time = The amount of time required for a wireless interface to process a received frame and to respond with a response frame
- Preamble Time = The amount of time that takes to synchronize transmission timing between two or more systems
- Backoff Time = The waiting time that a station waits before attempting retransmission of the frame = (Slot Time * Minimum Backoff Window Size) / 2
- Packet Transmission Time = Transmission Time of the PHY preamble + Transmission Time of the PHY header (R_H) + Transmission Time of MAC overhead (header + FCS) + Transmission Time of data payload (R_P)
- ACK Transmission time = Transmission Time of ACK frame + Transmission Time of the PHY preamble + Transmission Time of the PHY header (R_H)

Now let's come back to final formula. As I mentioned before, we have two main scenarios: with RTS/CTS and without RTS/CTS. Let's go forward and indicate each scenario's formula to calculate the average time per packet:

- Without RTS/CTS:
  - Average Time Per Packet = DIFS + Average Backoff Time + Packet Transmission Time + SIFS + ACK Transmission Time
- With RTS/CTS:
  - Average Time Per Packet = DIFS + RTS Packet Transmission Time+ CTS Packet Transmission Time + Average Backoff Time + Packet Transmission Time + SIFS + ACK Transmission Time

Problem 5

Consider the scenario shown in the figure of the problem, in which there are four wireless nodes A, B, C, D. the radio coverage of the four nodes is shown via the shaded ovals, all nodes share the same frequency.

• Let us assume that D wants to send data to C, C wants to send data to B, and B wants to send data to A. Explain how we can choose channels, activate RTS/CTS, and use other 802.11b features to maximize the throughput of this network. Note that all stations have only one wireless card interface and can send or receive at a specific time.

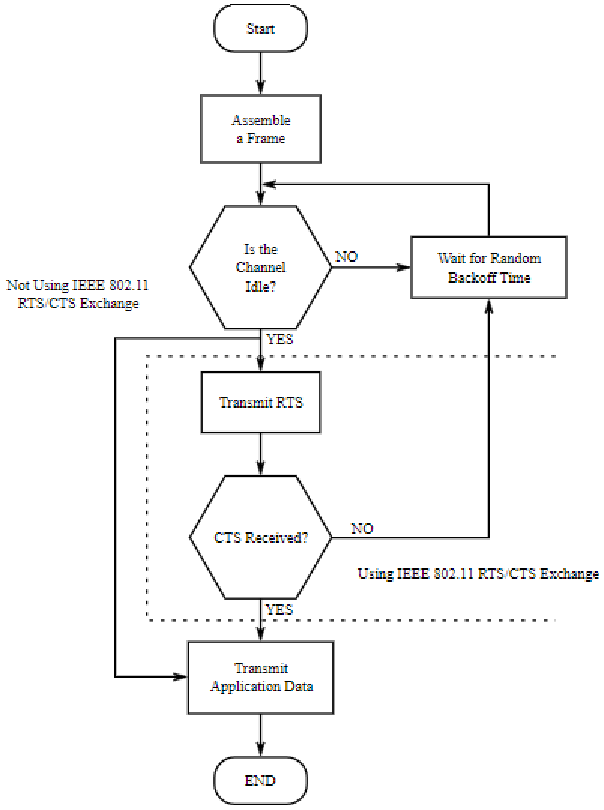
• Answer the previous question when node A wants to send data to B and D to C, simultaneously.

Solution

• Node C is in the radio coverage of both B and D, and since a node can receive only one message at a timeslot, C will receive either D's message or B's message (collision occurs).

In other words, D can send a packet to C, C can also send a packet to B, but the problem is that the same wireless card interface makes these connections happen simultaneously, so a packet collision occurs. This scenario is also true for B when C wants to send a packet to B and B simultaneously wants to send a packet to A. So we have to activate RTS/CTS mode to introduce a delay in this process to make it possible for these nodes to transmit packets without collision. The CSMA/CA feature is also a factor that can help us prevent this collision.

NOTE Actually, to overcome this problem, request-to-send/clear-to-send (RTS/CTS) handshaking (IEEE 802.11 RTS/CTS) is implemented at the access point in conjunction with the Carrier sense multiple access with collision avoidance (CSMA/CA) scheme. In the figure below, we can see a simplified algorithm of CSMA/CA. We also use the same trait to reach a more stable situation and maximize the throughput of this network:


Start
Assemble a Frame
Is the Channel Idle?
NO
Wait for Random Backoff Time
Not Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit RTS
CTS Received?
NO
Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit Application Data
END

• Since the transmission radius of A and D are not overlapping, B and C will receive their messages as planned, and as a result, we do not need to activate any extra mode of 802.11 for this scenario.

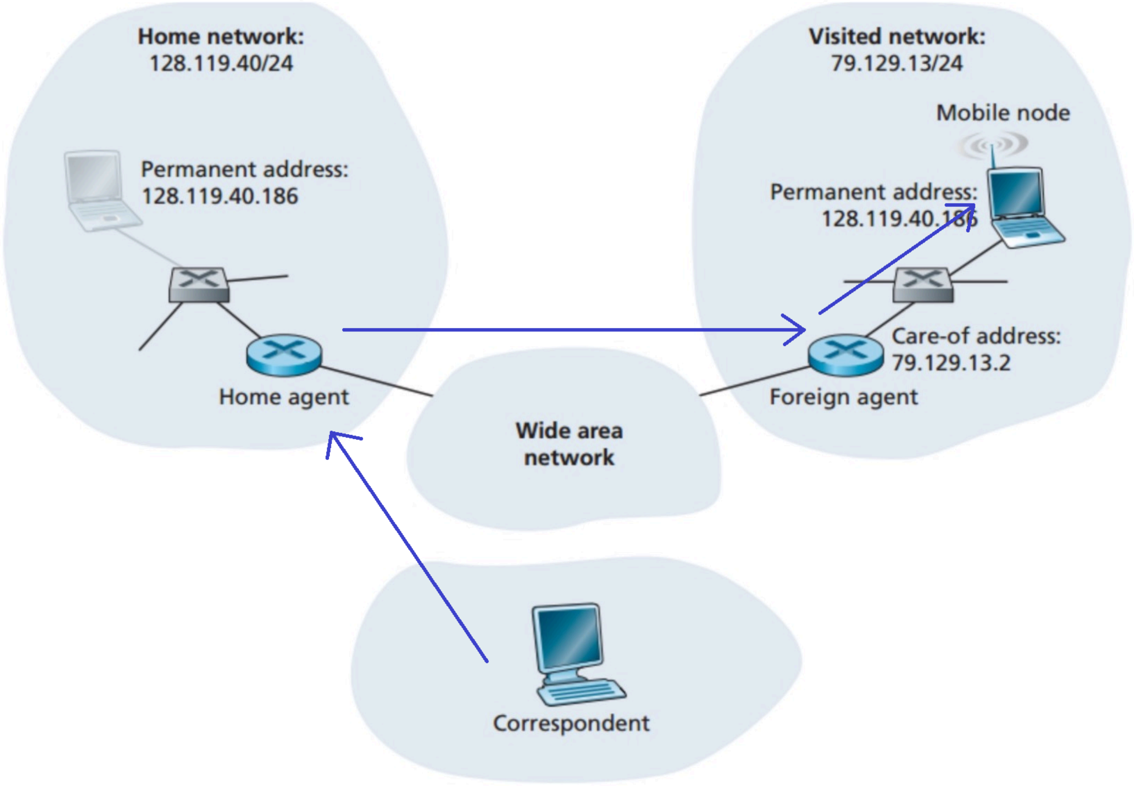
Problem 6
Consider the scenario shown in figure of the problem. Suppose that the correspondent wants to send data to mobile node, and vice versa.
• Explain the packet flow in the aforementioned scenario. (for both direct routing and indirect routing)
• What would be the source and destination IP address in each stage? (for both direct routing and indirect routing)

Solution

•

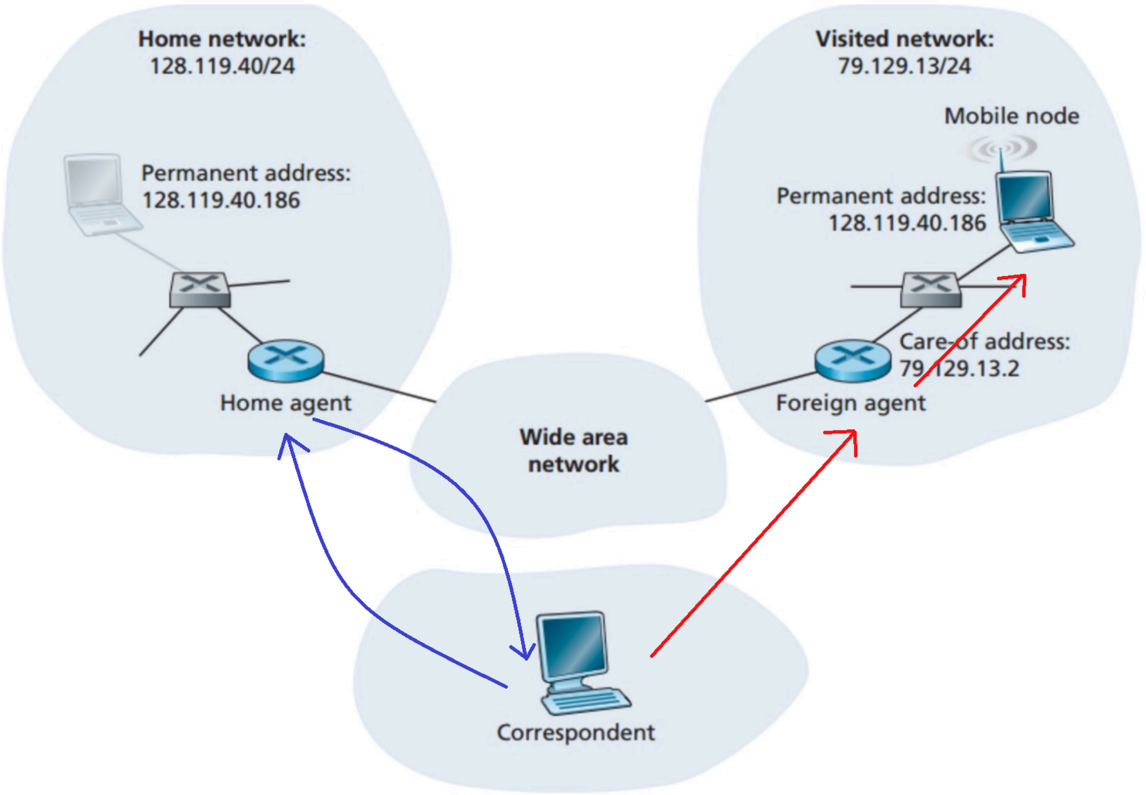
∗ Indirect Routing:

- The correspondent simply addresses the datagram to the mobile node's permanent address and sends it into the network, unaware of whether the mobile node is resident on its home network or is visiting a foreign network. Such datagrams are first routed, as usual, to the mobile node's home network.
- The home agent intercepts these datagrams and then forwards them to the foreign agent, using the mobile node's COA.
- It is subsequently forwarded to the mobile node by the foreign agent.
- For a response, the mobile node can directly address its datagram to the correspondent (using its permanent address as the source and the correspondent's address as the destination address). Since the mobile node knows the correspondent's address, there is no need to route the datagram back through the home agent.



∗ Direct Routing:

- A correspondent agent in the correspondent's network first learns the COA of the mobile node. This is done by sending a control message about the mobile node's COA to the home agent.
- The home agent then returns the information about the COA via a control message.
- The correspondent agent then tunnels datagrams straight to the COA of the mobile node, which is similar to the tunneling performed by the home agent, first to the foreign agent and then to the mobile node.



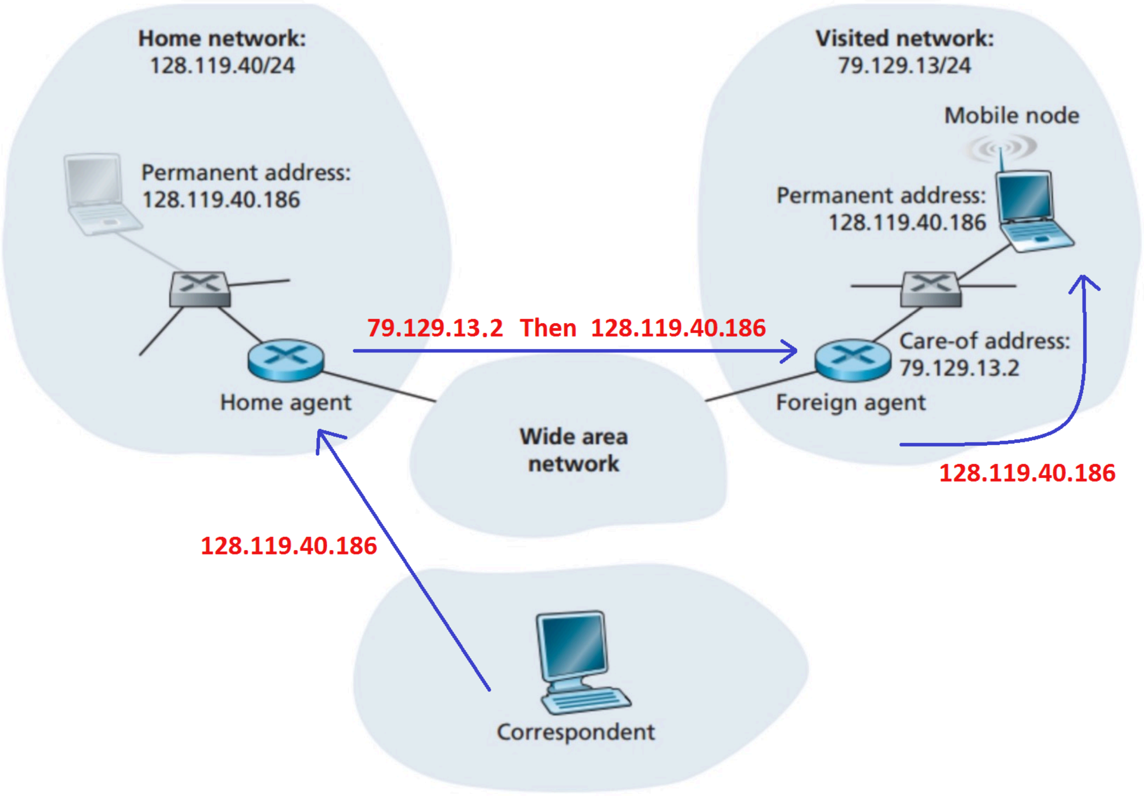
-

  - ∗ Indirect Routing:

  - The datagram from the correspondent to the home agent's destination IP address: 128.119.40.186

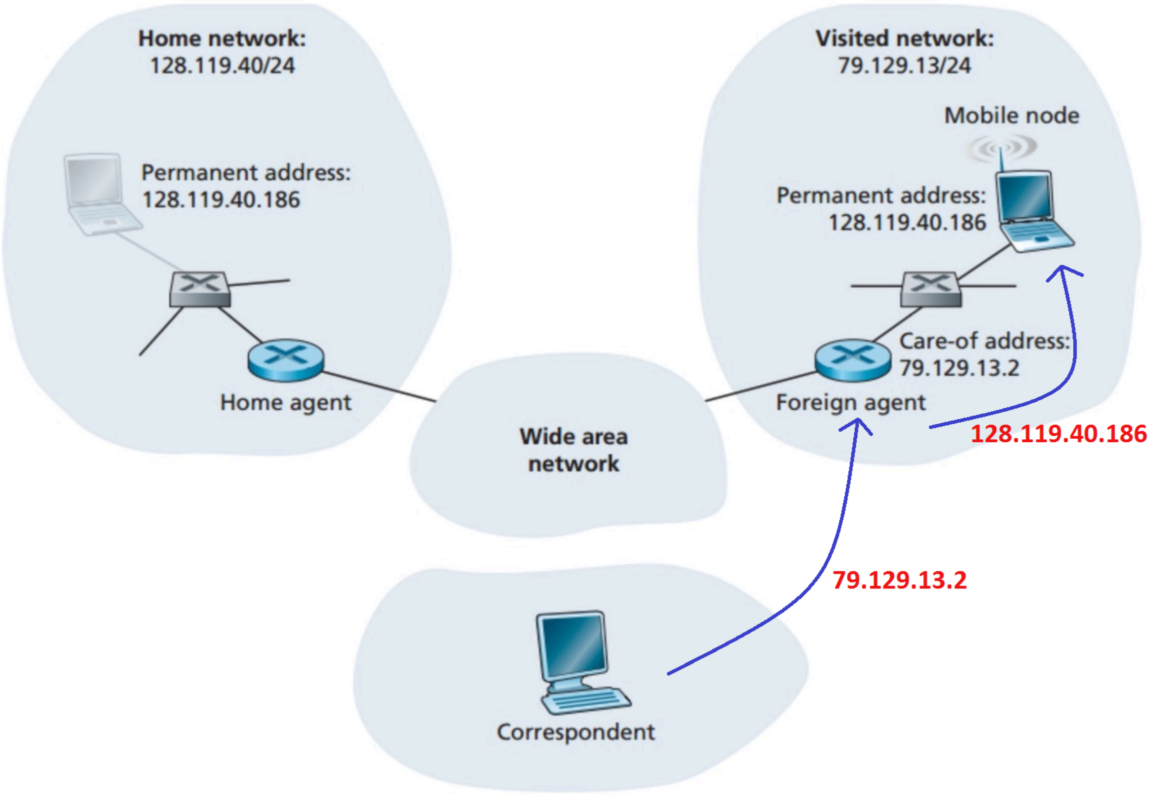
  - The datagram is forwarded from the home agent to the foreign agent's IP address: 79.129.13.2
    The datagram includes the message's IP address: 128.119.40.186

  - The datagram is forwarded from the foreign agent to the mobile node's IP address: 128.119.40.186



∗ Direct Routing:

- The datagram from the correspondent to the foreign agent's destination IP address: 79.129.13.2
  The datagram includes the message's IP address: 128.119.40.186
- The datagram is forwarded from the foreign agent to the mobile node's IP address: 128.119.40.186



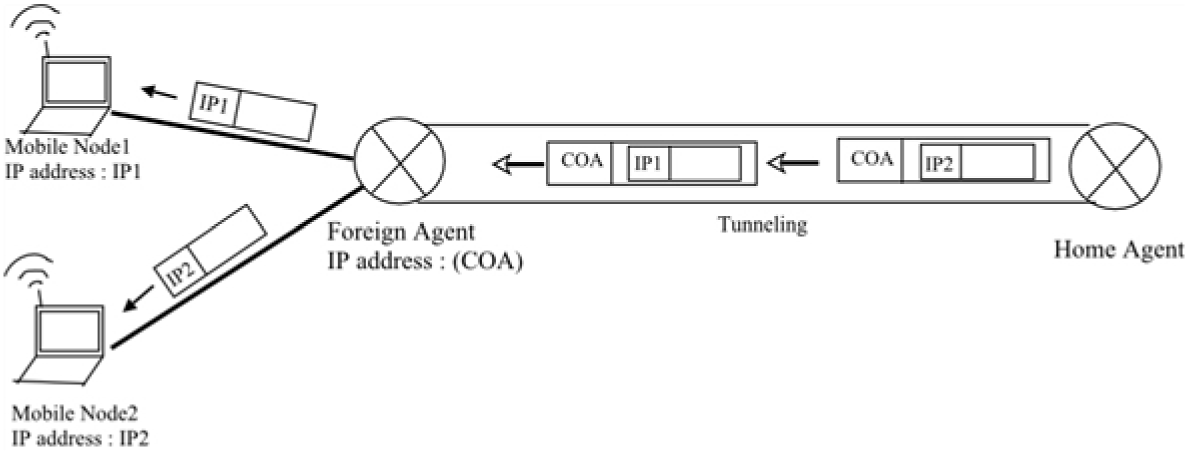
Problem 7
Consider two mobile nodes in a foreign network having a foreign agent. Is it possible for the two mobile nodes to use the same care-of address in mobile IP? Explain your answer.

Solution

On the same visited network, two mobiles may surely have the same care-of-address. Indeed, if the care-of-address is the foreign agent's address, then this address is the same. Once the foreign agent decapsulates the tunneled datagram and determines the mobile address, then separate addresses would need to send the datagrams separately to their different destinations (mobiles) within the visited network.

That is to say, care-of-address refers to the IP address of a foreign agent. When a mobile node visits a foreign network, a care-of address (COA) is assigned to that mobile node. It is also registered at the home agent to redirect the mobile node data to the foreign agent encapsulating the original packet. The foreign agent decapsulates the packet and sends the original packet to a particular mobile node. If two mobile nodes visit the same foreign network and have the same foreign agent, the same COA is assigned to the two mobile nodes. Respective home agents send their mobile node's data to the same COA by encapsulating the original packet for the foreign agent. Then a foreign agent encapsulates the packets and sends the data to a particular mobile node.

The picture below shows an example scenario of two mobile nodes from the same home network visiting the same foreign network (the two mobile nodes do not need to be from the same home network).


IP1
Mobile Node1
IP address : IP1
IP2
Mobile Node2
IP address : IP2
Foreign Agent
IP address : (COA)
COA
IP1
COA
IP2
Tunneling
Home Agent