ECE/CS 4984: Wireless and Mobile Systems Design ◆

Final Exam

Instructions

The exam is open book and open notes. You may use a computer to view notes and documentation. You may not run a compiler, network configuration program, or any other programs except to view PDF files, Word files, text files, or source code.

This exam consists of 20 questions on 10 pages. Check now to be sure that you have all pages.

Questions on pages 5, 8, and 9 refer to the network diagram that appears on the last page of the exam. You can remove the page with the diagram for easy reference.

You have 2 hours to complete the exam.

Part I: Multiple Choice Questions [42 points total, 3 points for each question]. For each question below, circle the letter associated with the single ***best*** answer.

1. Suppose all stations in an 802.11 WLAN enable virtual carrier sensing. Station A senses the medium and overhears a CTS transmitted by station B (station A did not hear the RTS that prompted this response from node B). Which of the following is the correct procedure to be followed by station A?
   (a) Station A assumes it is outside the range of the sender in this exchange and, therefore, it can transmit immediately without causing a collision.
   (b) Station A waits for SIFS and then sends an ACK to inform station B that it has correctly received the CTS.
   (c) Station A waits for SIFS, then senses the medium again. Since it did not hear the RTS, station A cannot set its Network Allocation Vector (NAV).
   (d) Station A waits for DIFS, then senses the medium again. Since it did not hear the RTS, station A cannot set its Network Allocation Vector (NAV).
   (e) Station A sets its Network Allocation Vector (NAV) according to information in the CTS frame and it need not sense the medium again until that period is over.

2. A friend comes to you for advice on whether to activate the exchange of RTS/CTS messages in the 802.11 WLAN she set up at home. You should tell your friend…
   (a) To activate virtual carrier sensing because, otherwise, her WLAN will not be in compliance with the IEEE 802.11 standard.
   (b) To activate virtual carrier sensing, as it will always increase aggregate throughput.
   (c) To activate virtual carrier sensing if she has been observing a large number of collisions.
   (d) To activate virtual carrier sensing if she wants to increase the security of the network.
   (e) Not to activate virtual carrier sensing, as any device that does not support RTS/CTS will no longer be able to associate with her access point.

3. Typically, you can activate the exchange of RTS/CTS by an access point (AP) by selecting…
   (a) a frame size threshold: data frames larger than that threshold will be preceded by an RTS.
   (b) a frame size threshold: data frames smaller than that threshold will be preceded by an RTS.
   (c) a set of devices: when communicating with those devices, the AP will issue an RTS.
   (d) a threshold for the number of devices associated with the AP: when this threshold is exceeded, the AP will precede all data frames by an RTS.
   (e) a threshold for the number of devices associated with the AP: while this threshold is not reached, the AP will precede all data frames by an RTS.

4. In an 802.11 WLAN in ad hoc mode, station A has RTS/CTS disabled. It receives an RTS from station B. What happens?

   (a) Station A does not respond; eventually, station B will timeout and will attempt to send its frame without an explicit CTS from station A.

   (b) Station A does not respond; communication between the two stations is not possible.

   (c) Station A sends a management frame to inform station B that they should communicate without the exchange of RTS/CTS.

   (d) Station A responds with a CTS.

   (e) Station A displays an error message to the user, telling him/her to enable virtual carrier sensing.

5. Transmission by Bluetooth devices may interfere with…

   (a) IEEE 802.11a transmissions, but not 802.11b, as both 802.11a and Bluetooth use OFDM.

   (b) IEEE 802.11g transmissions, but not 802.11b, as both 802.11g and Bluetooth use FHSS.

   (c) IEEE 802.11b transmissions, but not 802.11a, as both 802.11b and Bluetooth use DSSS.

   (d) IEEE 802.11b transmissions, but not 802.11a, as both 802.11b and Bluetooth operate in the same frequency band.

   (e) IEEE 802.11b transmissions, but not 802.11g, as both 802.11b and Bluetooth use FHSS.

6. Adaptive Frequency Hopping (AFH) is a solution proposed for coexistence between Bluetooth and 802.11 devices. Which of the following is true?

   (a) 802.11 hardware (NICs) must support AFH for this solution to be effective.

   (b) 802.11 device drivers require a (software) upgrade for this solution to be effective.

   (c) This solution requires specific support by Bluetooth devices, but no changes to 802.11 devices.

   (d) One drawback of the solution is that Bluetooth devices that do not support AFH will no longer be able to operate in the same piconet as those that do support AFH.

   (e) Both Bluetooth and 802.11 devices must undergo a firmware upgrade for the solution to be effective.

7. The major challenge in adapting Policy-based QoS management for use in mobile ad hoc networks is that…

   (a) It is difficult to guarantee quality of service in a MANET, due to the dynamic topology.

   (b) It is difficult to authenticate nodes in a MANET.

   (c) Policy-based QoS management only works with proactive routing protocols.

   (d) Policy based network management was originally envisioned as a centralized solution, and must be adapted to the distributed environment that is characteristic of MANETs.

   (e) It requires modifications to the IEEE 802.11 specification.

8. Which ad hoc routing protocol(s) is (are) adopted in the IEEE 802.11 specification?
   (a) OLSR and AODV.
   (b) OLSR, AODV, DSR and TBRPF.
   (c) It is not decided yet. The 802.11 specification will be modified to support whichever routing protocol(s) is(are) chosen by the IETF.
   (d) A large number of proactive, reactive and hybrid routing protocols.
   (e) The 802.11 specification only covers the physical and link layers and, therefore, does not define routing protocols.

9. Suppose the instructors decide to upgrade the access points used in the experiments to the Linksys® WirelessG WAP54G access point hub, supporting data rates up to 54 Mbps. Which of the following is true?
   (a) Student notebook computers would be able to associate with this access point using their IEEE 802.11a cards.
   (b) Student notebook computers would be able to associate with this access point using their IEEE 802.11b cards.
   (c) We would need to buy IEEE 802.11g NICs for the notebook computers to be able to associate with this AP.
   (d) Even if the NICs loaned to students are not upgraded, we should see a significant increase in throughput in our experiments.
   (e) The lab exercises dealing with medium access control would need to be modified, since the MAC adopted in IEEE 802.11g is different from that adopted in the IEEE 802.11b specification.

10. Hot spot services…
   (a) are a good example of pervasive computing.
   (b) are a good example of location-aware computing.
   (c) typically support instantaneous operation, but not physical integration, and therefore are not a good example of pervasive computing.
   (d) use the Service Location Protocol (SLP) for clients to identify coverage areas.
   (e) are a good example of support for nomadic computing, but not of pervasive computing.

11. Which of the following IEEE 802.11 security vulnerabilities is <u>not</u> addressed by the Temporal Key Integrity Protocol?
   (a) The relatively small number of unique initialization vectors.
   (b) The relatively weak integrity check based on a cyclic redundancy check.
   (c) Asymmetric authentication where a station cannot authenticate an access point.
   (d) None of the above – all of the vulnerabilities (a) through (c) are addressed.
   (e) All of the above – none of the vulnerabilities (a) through (c) are addressed.

Refer to the network diagram provided on the last page of this exam to answer multiple choice questions 12, 13, and 14.

12. When does Device A perform a proxy ARP to support Mobile IP for Host D?
    (a) Any time an ARP request is received for Host D (assuming Host D has registered a care-of address on the foreign network).
    (b) Just one time when Host D sends a registration request for a care-of address on the foreign network.
    (c) When Host D returns to the home network and de-registers the foreign network care-of address.
    (d) Any time a foreign agent (Device B) sends a registration request to Device A.
    (e) Any time a foreign agent (Device B) sends a tunneled datagram to Device A.

13. Suppose "iptables" is used to create a firewall at Device C. Which chain and table will be used to process (accept, reject, deny, etc.) packets sent by host F to the DHCP server running on Device C?
    (a) The FORWARD chain and the NAT table.
    (b) The INPUT chain and the NAT table.
    (c) The OUTPUT chain and the NAT table.
    (d) The FORWARD chain and the FILTER table.
    (e) The INPUT chain and the FILTER table.
    (f) The OUTPUT chain and the FILTER table.
    (g) None of the above.

14. Suppose Host F and Host G both open TCP connections to an HTTP server running at port 80 on Host H. Also, the web browsers on Host F and Host G both use port 9000 for their local TCP port number for their connection. Which of the following is true? Note that Device C implements NAT using iptables as in Project P11.
    (a) This cannot work since packets from both sessions coming into Device C from the WAN will have the same source and destination IP addresses and the same source and destination port numbers.
    (b) This will work only if Device C has at least two different 10.0.1.*x* IP addresses on the WAN. Device C can assign different source IP addresses for packets sent from the different hosts.
    (c) Device C must create a tunnel to Host H. Device C can encapsulate the different packets directly in the tunnel instead of doing traditional NAT.
    (d) Device C must translate both the IP address and the port number for outgoing packets. It can assign different source port numbers for packets sent from the different hosts.
    (e) Device C must use a NAT application-level gateway for HTTP so that it can interpret application requests to distinguish between packets belonging to the different connections.

Part II: Other Questions [points are noted for each]. Provide your answer in the space provided. Do not continue answers elsewhere.

15. MANET Routing [25 points]. Nodes in an ad hoc network maintain the following routing tables. For simplicity, we identify nodes by the last byte in their IP addresses (rather than the full IP address).

At node 1			*At node 2*			*At node 3*		
Dest.	**Next hop**	**Number of hops**	**Dest.**	**Next hop**	**Number of hops**	**Dest.**	**Next hop**	**Number of hops**
2	2	1	1	1	1	1	2	2
3	2	2	3	3	1	2	2	1
4	2	2	4	4	1	4	4	1
5	5	1	5	4	2	5	4	2
6	5	3	6	4	2	6	4	2

At node 4			*At node 5*			*At node 6*		
Dest.	**Next hop**	**Number of hops**	**Dest.**	**Next hop**	**Number of hops**	**Dest.**	**Next hop**	**Number of hops**
1	5	2	1	1	1	1	4	3
2	2	1	2	1	2	2	4	2
3	3	1	3	4	2	3	4	2
5	5	1	4	4	1	4	4	1
6	6	1	6	4	2	5	4	2

(a) [4 points] Draw the topology of the network.

(b) [3 points] Node 6 generates a packet with destination address node 1. What route will the packet follow?

(c) [12 points] Suppose OLSR is adopted as the routing protocol. Complete the table below with the *optimal* Multipoint Relay Set (MPR) and the *optimal* Multipoint Relay Selector Set (MS) for each node. (Note: Whenever there is a tie, assume that the node with the higher ID is chosen as a multipoint relay.)

Node j	***MPR(j)***	***MS(j)***
1		
2		
3		
4		
5		
6		

(d) [3 points] Node 2 detects a new link to node 7 and generates a new topology control (TC) message, which it sends to its neighbors. Which of these neighbors will forward the TC message?

(e) [3 points] Give one reason why a protocol such as OSPF, used for intra-domain routing in wired networks, would not be a good choice for a MANET. Your answer should be brief. Use only the space provided below.

Refer to the network diagram provided on the last page of this exam to answer questions 16-20.

16. [3 points] Is Host F considered a "mobile host" or a "nomadic host"? Briefly justify your answer. Use only the space provided below.

17. [3 points] What is the care-of address registered at Device A by Host D?

18. [12 points] Suppose Host E sends a datagram to Host D.

    (a) [2 points] What are the source and destination IP addresses of the datagram sent by Host E?

        Source IP: _____

        Destination IP: _____

    (b) [2 points] What are the source and destination IP addresses of the datagram as received at interface 10.0.1.3 at Device B?

        Source IP: _____

        Destination IP: _____

    (c) [4 points] Specify the path followed by the datagram. You can use the host and device designations (A through H) specified in the network diagram.

    (d) [4 points] Specify all tunnels used to deliver the datagram from Host E to Host D. For each tunnel, specify the originating tunnel endpoint and the final tunnel endpoint using the host and device designations (A through H) specified in the network diagram.

19. [5 points] Which pair(s) of nodes must have security associations according to the Mobile IP standard? Use the host and device designations (A through H) specified in the network diagram.

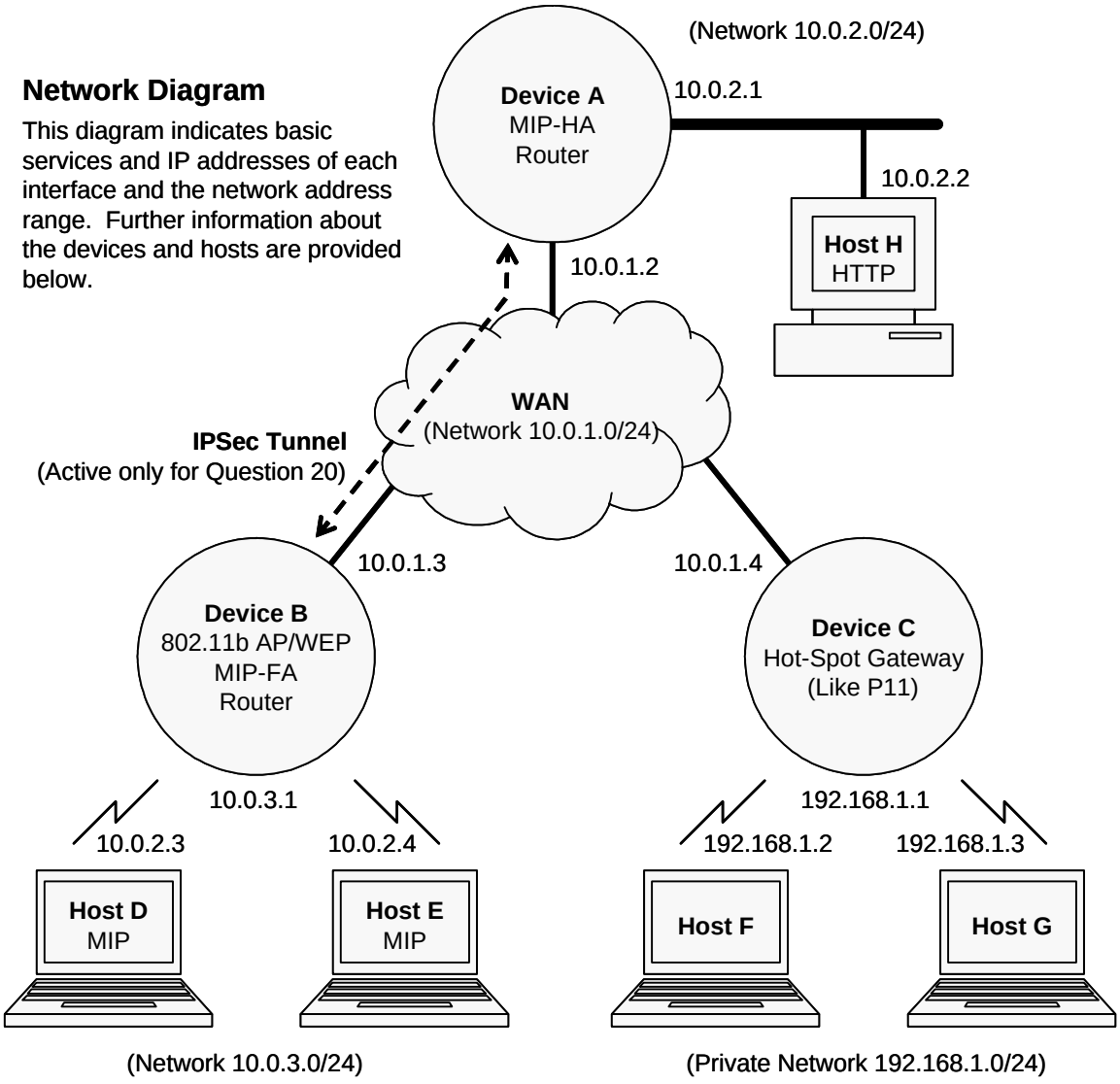
20. [10 points] Suppose that an IPsec tunnel is created between Device B (specifically, interface 10.0.1.3) and Device A (specifically, interface 10.0.1.2). The tunnel uses IPsec ESP in tunnel mode. AES is used. All packets to be delivered between interface 10.0.1.3 and interface 10.0.1.2 are carried via this IPsec tunnel.

    (a) [5 points] A packet sent from Host H to Host D is captured as it traverses the IPsec tunnel. Specify all IP headers in this packet. Specify the source and destination IP addresses in each header. Do not show any other fields except for the source and destination IP addresses. (Assume that we can fully decrypt the packet for this analysis.)

    (b) [5 points] With this configuration, what is the single greatest security vulnerability that threatens the privacy of datagrams sent between Host D and Host H? Briefly justify your answer. Use only the space provided below.

Network Diagram

This diagram indicates basic services and IP addresses of each interface and the network address range. Further information about the devices and hosts are provided below.



Description of Devices and Hosts

- Device A performs routing and Mobile IP (MIP) home agent functions
- Device B performs routing and MIP foreign agent functions. It also serves as an IEEE 802.11b access point using WEP with a 128-bit key. Device B does not provide a firewall. The IP routing function at Device B does not examine the source IP address.
- Device C is a wireless hot spot gateway with the same functionality as the gateway from project P11.
- Hosts D and E are MIP mobile hosts attached to foreign network 10.0.3.0/24. The home network for Hosts D and E is 10.0.2.0/24 and both mobile hosts are registered with the HA on Device A using the FA on Device B.
- Hosts F and G are hot-spot users. Hosts F and G use DHCP. They do not use Mobile IP.
- Host H attached to network 10.0.2.0/24 and is assigned a static IP address. Host H runs an HTTP server.