This is an open-book, open-resources exam. Explain or show your work for each question. Your grade will be severely deducted if you don’t show your work, even if you get the correct answer.

Name: ______________________________________________

uniqname: ___________________________________________

Honor code: I have neither given nor received any help on this exam.

Signature: __________________________________________

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>/20</td>
</tr>
<tr>
<td>2</td>
<td>/10</td>
</tr>
<tr>
<td>3</td>
<td>/10</td>
</tr>
<tr>
<td>4</td>
<td>/15</td>
</tr>
<tr>
<td>5</td>
<td>/15</td>
</tr>
<tr>
<td>6</td>
<td>/10</td>
</tr>
<tr>
<td>7</td>
<td>/20</td>
</tr>
<tr>
<td>Total</td>
<td>/100</td>
</tr>
</tbody>
</table>
**QUESTION 1: Routing Protocols** *(20 POINTS)*

The first two questions concern a shortest-path, link-state routing protocol running on the following network, where the numbers correspond to link weights:

![Network Diagram](image)

(1a) Suppose the link between nodes k and m fails. Before the failure, what is the shortest path from node i to node j? What is the new path after the failure, when routing-protocol convergence completes? (2 points)

*Before the failure: i-k-m-j (cost 6)*
*After the failure: i-r-n-j (cost 8)*

(1b) (Assuming the failure scenario in 1a): A transient forwarding-loop might occur during routing-protocol convergence. Involving what nodes? List two examples of what would happen to the data packets sent from i to j during this period. (3 points)

*The nodes k and n may experience a forwarding loop, if k learns about the failure first and starts forwarding the packets along the path k-n-j, while n is still forwarding along the (old) path n-k-m-j.*

*Some packets will be discarded when their TTL expires. Others may eventually escape the loop, and experience high delay and arrive out of order.*
The remaining parts of the question focus on interdomain routing using BGP.

(1c) BGP supports flexible routing policies. Internet Service Providers (ISPs) often have a “prefer customer” policy where they prefer to route through a customer, even if a shorter route exists through a peer or provider. Why? How is this policy realized in BGP? (3 points)

Directing traffic through a customer generates revenue, whereas sending through a peer or provider is (at best) revenue neutral and may, in fact, cost money.

The policy is realized in BGP by having an import policy that assigns a higher local-preference value to routes learned from customer ASes.

(1d) A customer AS (like University of Michigan) is not supposed to announce routes learned from one upstream provider (like Sprint) to another (like AT&T). Suppose University of Michigan accidentally advertised all Sprint-learned routes to AT&T, and AT&T applied a “prefer customer” path-selection policy. What would be the consequences, for University of Michigan, AT&T, and the larger Internet? (3 points)

AT&T would direct traffic through Michigan to reach most of the rest of the Internet. This would lead to a heavy load on the AT&T-Michigan and Michigan-Sprint links, and poor performance for many parts of the Internet (particularly AT&T’s customers).

(1e) Suppose two directly-connected routers A and B have a BGP session between them, running over a TCP connection. BGP is used to propagate routing information, yet BGP relies on establishing a TCP connection before exchanging any update messages. TCP, in turn, relies on the routing system to deliver TCP segments. How is this apparently circularity resolved? How do the two TCP end-points know how to reach each other? (3 points)

Since the two routers are directly connected, they have interfaces on the same subnet (i.e., the two BGP speakers have IP addresses in the same subnet). As such, they know how to reach each other, perhaps requiring a simple ARP query to learn the associated MAC address.
(1f) Suppose two directly-connected routers A and B have a BGP session between them, running over a TCP connection with port 179 on both ends. A third party C, several hops away, could conceivably launch a denial-of-service attack on router B by sending unwanted packets to router B on port 179. To defend B from such attacks, the network operators might install a packet filter that discards all packets destined to B on port 179, except for packets sent from IP address A. However, C could easily send “spoofed” packets (with a source IP address that corresponds to A) to B, and get through the packet filter to place unwanted load on router B. The “BGP TTL Security Hack” defends against such attacks by having A sends packet to B with a TTL field of 255, and B discards any BGP packets from IP address A that has a TTL smaller than 254. How does this prevent C from successfully launching the attack? (4 points)

The 8-bit TTL field has a maximum value of 255. C cannot set a value higher than 255, and each hop along the path from C to A decrements the value (discarding when 0 is reached). As such, it is impossible for C to direct a packet to A that will have a TTL value of 254 when it reaches A.

(1g) What other ways could node C disrupt the TCP connection between A and B? How could A and B defend against it? (2 points)

C could send excessive traffic to other destinations reachable via paths that traverse the A-B link. This would lead to congestion on the A-B link that might cause the BGP session’s TCP connection to back off and, in the worst case, even timeout and reset.

A and B could put BGP packets in a separate (high-priority) queue to protect them from congestion induced by other traffic.
QUESTION 2: Ethernet and Wireless (10 points)

(2a) Ethernet bridging relies heavily on flooding. For example, broadcast traffic is flooded. List two protocols that generate broadcast traffic, and explain why broadcasting is done. (2 points)

- ARP: ARP requests are sent to learn the MAC address associated with a particular IP address. The machine sending the request has no idea where the destination machine is located and, as such, sends a broadcast packet to ensure the query reaches the machine with the target IP address.
- DHCP: As part of boot-strapping, a host sends a DHCP request in the hope that a DHCP server will respond to assign an IP address, subnet mask, gateway address, and DNS server address. The host has no idea what machines are serving as DHCP servers and, as such, sends a broadcast traffic to ensure one or more DHCP servers hear the request.

(2b) When (and why) might a unicast frame require flooding? (2 points)

When a node does not know how to reach the destination MAC address, the frame is flooded in the hope of reaching the destination.

(2c) Ethernet switches compute a spanning tree using the spanning-tree protocol. Explain briefly how the spanning tree protocol works. (2 points)

Each switch has an identifier, and these ids impose an ordering on the switches; in particular, the switch with the smallest id will (eventually) become the root. Initially, each switch proclaims to be the root, announcing a distance of 0 to reach the root. The switches repeatedly send messages to their neighbors with (root-id, distance to root, local id), updating as they learn about smaller root-ids and shorter paths to that root. In the end, every switch knows which neighbor(s) to use to forward traffic along the spanning tree rooted at the switch with the smallest id.

(2d) Do the switches learn the network topology (connecting the switches), like routers do in a link-state protocol? Does each pair of switches communicate over a shortest path, like routers do in link-state protocols? (2 points)

No, the switches do not learn the entire topology – only the distances to the root from each neighbor. No, the switches communicate over a (single) spanning tree, rooted at the node with the smallest id; some links are never used, and traffic does not necessarily follow a shortest path.

(2e) Why are acknowledgments used in 802.11 but not in wired Ethernet? (2 points)

In wired Ethernet, the transmitted can sense the wire and decide if the frame was successfully delivered, so no ACK is necessary. In the wireless scenario, the sender has no idea if the frame was successfully delivered, for two reasons. First, fading or the
hidden-terminal problem may mean that interference occurred without the sender knowing. Second, the sender may not be capable of transmitting and listening at the same time, making collision detection impossible. Hence, an ACK is useful.
QUESTION 3: **Source Routing** *(10 POINTS)*

In source routing, the end host or edge router computes the path through the network, and the packet carries the list of hops along the path. The routers, in turn, forward the packet as instructed. This question explores the advantages and disadvantages of source routing.

(3a) List three advantages of source routing, relative to today’s intradomain and interdomain routing protocols. (3 points)

- The sender could exploit knowledge of the performance or reliability of the links.
- The sender could pick a path that matches the application requirements (e.g., low delay vs. high throughput)
- The sender could pick paths that avoid untrusted links or ASes.
- The sender could react quickly to changes in network conditions (e.g., failure) by rerouting to a new path.

(3b) List three disadvantages of source routing, relative to today’s routing system. (3 points)

- The sender would need to perform extra work.
- The packet could not easily adapt its route in mid stream.
- The packets would be larger, because of needing to carry the path information.
- The sender would need to learn the connectivity information for the Internet, which might not be scalable.
- ISPs would lose control over how traffic flows through their networks.
- Denial-of-service attacks would be easier to launch.

(3c) Source routing is implemented in today’s IP routers, but network operators almost always disable the feature. List three reasons why network operators disable source routing. (4 points)

- Otherwise, they would lose control over the flow of traffic, leading to congestion and lost revenue (when customers pick paths that contradict the ISP’s business incentives).
- The ISP would be much more vulnerable to denial-of-service attacks.
- Source routing requires extra processing on the routers, leading to extra overhead.
QUESTION 4: Internet Versus Station Wagon (15 POINTS)

A famous maxim, sometimes attributed to Dennis Ritchie, says “Never underestimate the bandwidth of a station wagon full of tapes.” Suppose you need to deliver a large file between two computers that are 200 km apart and connected by a direct link. This question analyzes when it is faster to drive the data between the two locations, rather than transmit the data?

(4a) Suppose the station wagon drives 100 km/hour and the link has a bandwidth of 800,000 bits/second. And, suppose for simplicity that the data transfer can fully consume the link bandwidth, with no additional overhead (e.g., for headers or the TCP sawtooth). At what file size (in bytes) does the station-wagon solution start delivering the data faster? Show your work.

By car, travel time is 2 hours (i.e., 200 km * 1hr/100km). During two hours, the link could transfer 800,000 bits/sec * 60 sec/min * 60 min/hour * 2hr * 1byte/8bits for 720,000,000 bytes.

(4b) Suppose the sender transmits the data as packets with a 20-byte IP header, and 20-byte TCP header, and a maximum segment size of 512 bytes. How much more time (as a fraction) would the data transfer take on the link? (Ignore TCP congestion control and the link-layer header.)

An MSS of 512 bytes and two 20-byte headers leads to a packet size of 552 bytes. So, only 512/552 of the bandwidth is used to transmit the actual data, so the transfer takes 552/512 of the time, or 40/512 times longer. This reduces to a factor of 5/64 longer time.

(4c) Suppose that, like the path traversed by the car, the link is 200 km long. The speed of electricity in a copper cable is 200,000,000 meters/second. How big does the receive window (used for flow control) need to be to avoid becoming the main constraint on the transfer rate? (Ignore the effects of header sizes, TCP congestion control, and packet loss, and assume that the receiver immediately sends an ACK packet after receiving each data packet and that there is no congestion.)

The receive window needs to be large enough to accommodate a round-trip time of data. The one-way delay is 1sec/200,000km * 200km, or 0.001 seconds (or 1 msec). So, the round-trip time is 0.002 seconds (or 2 msec). Since the link bandwidth is 800,000
bits/sec, the total number of bytes transmitted during a round-trip time is 0.002 sec * 800,000 bits/sec * 1 byte/8 bits, or a grand total of 200 bytes.
QUESTION 5: Sockets *(15 POINTS)*

(5a) Suppose application A is using a stream socket to transfer data to application B on a remote host. Suppose application A writes data into the socket buffer ten times. Why might the underlying TCP implementation transmit more than ten data packets (not including retransmissions of lost packets, or control packets like SYN, ACK, or FIN)?

*If the application writes more than an MSS of data, a single write() call may lead to multiple TCP segments and, hence, multiple packet transmissions.*

(5b) Why might the TCP implementation transmit all of the data in fewer than ten data packets?

*If the application writes less than an MSS of data, the data from multiple write() calls may be combined into a single TCP segment and, hence, a single packet transmission. This is especially true in applications like Telnet, when Nagle’s algorithm is used.*

(5c) Why can application A safely perform a close() on the socket when it is done writing the data, even if application B has not yet received all of the data?

*The TCP implementation (typically in the operating system) buffers the data and continues to (re)transmit the data to the receiver as needed.*

(5d) List two possible explanations for why host A would need to retransmit the SYN packet as part of establishing the TCP connection with B.

*The SYN packet may have been lost in the network, discarded by the receiver due to a checksum error, or discarded because the receiver’s listen queue is full. Or, the SYN-ACK packet may have been lost. Or, the RTO might have been too small (e.g., for a very long-haul link to Mars).*

(5e) Since a datagram socket (i.e., a UDP socket) does not require establishing a connection, why is a port number necessary?

*For demultiplexing the packet to the correct receiving socket.*
QUESTION 6: Cheaters Sometimes Win (10 points)

Many of the protocols underlying the Internet rely on end hosts to faithfully implement the protocols correctly, for the greater good. This question explores what happens when they don’t.

(6a) List one motivation for a host to send an IP packet with the wrong source IP address. List two ways that this can adversely affect the legitimate owner of that IP address.

A host launching a denial-of-service attack may send packets with a “spoofed” source address that corresponds to another host, in order to evade detection. The legitimate owner may be blamed for the attack (and perhaps also blocked from sending legitimate traffic to the victim destination), and may also receive unwanted return traffic (e.g., SYN-ACK or RST packets).

(6b) Consider a multi-access Ethernet where one host has an adapter that does not back off after detecting a collision. Describe how this would affect the communication performance for the other hosts.

When a collision occurs, the other (well-behaved) adapters would back off, while the rogue adapter would continue sending; the well-behaved adapters would not try to send again because the link is already busy. Ultimately, the rogue adapter would have nearly complete control of the link, leaving the other adapters with little or no bandwidth.

(6c) Some implementations of ARP process an ARP reply (by updating the local ARP cache) even when there are no ARP requests pending. Suppose a rogue computer sends an unsolicited ARP reply message, with its own MAC address and the IP address of the LAN gateway router, to another host on the LAN. What will happen when this host (i.e., the host who believed the bogus ARP reply) transmits an IP packet destined to an external Internet address?

The host would send the packet in an Ethernet frame destined to the MAC address of the rogue machine, which may discard the traffic, or may inspect the contents before directing the packet to the legitimate gateway.
QUESTION 7: Home-Network “Box” (20 points)

Consider a home network with multiple hosts plugged in (via Ethernet cables) to a Box that has a link directly to a residential broadband provider (e.g., via a DSL line). Suppose the broadband provider assigns a single public address to each home. This question explores the many functions that the Box implements.

(7a) The Box may, at different times, act as both a DHCP client and a DHCP server. Why would it act as a client? Why would it act as a server?

The Box acts as a DHCP client to the DSL provider’s DHCP server, to get a public IP address. The Box acts as a DHCP server to allocate private IP addresses to the internal hosts.

(7b) The Box serves as a gateway router for the hosts in the home network. How do the hosts in the home network learn the IP address of the gateway? Is this the same address as the single public address the provider allocated to the home? Why or why not?

The hosts in the home network learn the internal-facing address of the gateway via DHCP. This is not the same as the external-facing address assigned by the ISP. Typically, the ISP assigns an address from its own (public) address block, whereas the internal-facing address lies in the (private) address block used to number devices in the home network.

(7c) Suppose a host in the home network sends a TCP SYN packet to a Web server in the external Internet. Explain the role of ARP and NAT in getting the first IP packet from the host through the home network and out the connection to the Internet.

The host recognizes that the destination IP address of the packet falls outside of the local subnet and, as such, directs the IP packet to the gateway router (i.e., the Box). The host uses ARP to determine the MAC address of the gateway, by consulting its ARP cache or, on a cache miss, issuing an ARP query. Then, the host sends the Ethernet frame to the gateway (i.e., the Box). The Box then maps the source address and source port, using a NAT table, before directing the traffic to the Internet. (The Box may also use ARP to learn the MAC address of the DSL provider’s gateway router.)

(7d) Some Web sites on the Internet allow a home user to determine the public IP address the broadband provider has assigned to the home. Why might it be hard for the end user to determine the IP address directly? How does the external Web site know?

The end host learns the private (internally-facing) address of the NAT box, not the public (externally-facing) address. In contrast, the Web server receives the HTTP request on a
TCP connection from the public address of the NAT box and, as such, knows the public address.

(7e) NAT helps slow down the exhaustion of IPv4 address space. However, NAT also poses significant problems for applications that require peer to peer based connection. Explain why that is the case and how it can be overcome.

Peer to peer based applications require peers to connect to each other directly. If hosts are behind NAT, they cannot receive incoming packets without first sending an outgoing packet. It can be overcome if packets go through another host with a public IP address.

(7f) Cellular hosts are often assigned private addresses and thus reside behind NAT boxes. Besides the benefit of not requiring public IP addresses, give another benefit.

Security: arbitrary packets cannot reach these hosts.
Preventing the energy of cellular hosts from being drained due to active network interfaces and thereby saving radio resources.