Closed book. Closed notes. No electronic device.

1.

For each description below, give **one** term that *best* describes it. In many cases, but not all, the term will be in the table at left. In each case, give only **one** answer of **at most** 4 words (otherwise you get zero).

Anonymity
Sender k-anonymity
Receiver k-anonymity
Authoritative nameserver
Autonomous system
BGP
DHCP
DNS query
DNS zone
Dining cryptographers
Forwarding
Internetwork
IP address
IPsec
Link
MAC address
Mitnick attack
MixNet
Nameserver
Protocol
Router
Routing
SYN cookie
SYN flooding
Time-to-live
TCP
Tor
Transport
UDP

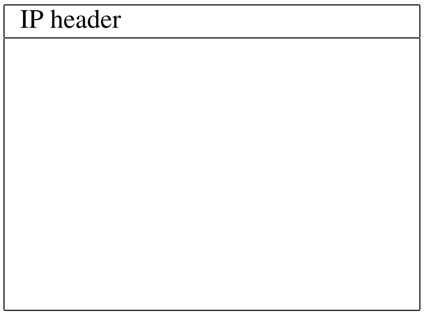
1. The activity of a router when it transfers incoming packets to outgoing links.
2. The activity by which routers select paths to destination addresses.
3. IP resides in this layer of the Internet.
4. BGP resides in this layer of the Internet.
5. TCP and UDP reside in this layer of the Internet.
6. 802.11 (WiFi) resides in this layer of the Internet.
7. The field of an IP packet indicating the maximum number of hops it can traverse.
8. Routers forward an IP packet based on this field of the packet.
9. The transport protocol used for voice and video transfer.
10. The transport protocol used by SSH.
11. An independently-administered part of the Internet.
12. The protocol for selecting routes between ASes.
13. This protocol provides "best-effort" packet transfer.
14. What a router does when it drops any IP packet whose source address does not belong to the router's AS.
15. The standard protocol for sending encrypted integrity-protected IP packets.
16. This provides the mapping of domain names to IP addresses.
17. A server that can provide the IP address of any node in its zone.
18. A server that knows the IP addresses of the top-level-domain nameservers.
19. The protocol by which a new host in a network obtains IP addresses for itself, DNS server, etc.
20. An attack in which a TCP server is overwhelmed with spurious connect requests.
21. A defense against SYN flooding.

2. What information does a host acquire from a DHCP server.

3. A local-area network that uses DHCP has an attacker that can eavesdrop and send messages. A new host, say A, joins the network and later attempts to access `https://a.com`. How can the attacker arrange to have A's attempt go instead to `https://b.com`.

4.

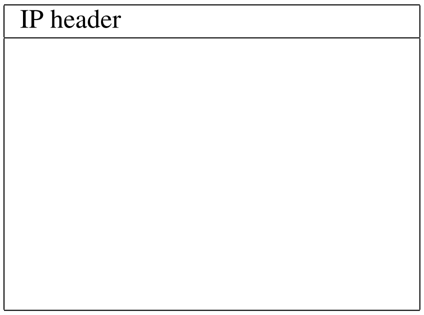
a. The IP packet at right carries data of an application that uses TCP. Indicate the parts of the packet occupied by IP data, TCP header, TCP data and TCP sequence numbers.



b. Can an attacker stop the application after it is connected by tampering with just one packet. Explain briefly.

5.

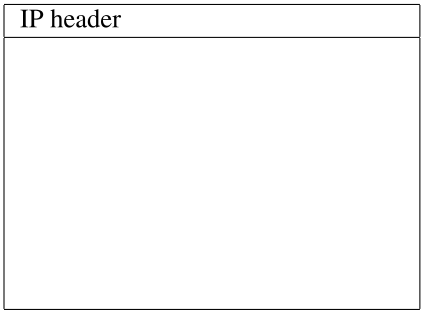
a. The IP packet at right carries data of an application that uses UDP. Indicate the parts of the packet occupied by IP data, UDP header and UDP data.



b. Can an attacker stop the application after it is connected by tampering with just one packet. Explain briefly.

6.

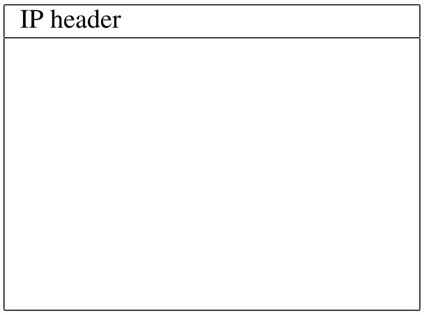
a. The IP packet at right carries data of an application that uses UDP and IPsec in tunnel mode. Indicate the parts of the packet occupied by UDP header, UDP data, IPsec header and IPsec data.



b. Can an attacker stop the application after it is connected by tampering with just one packet. Explain briefly.

7.

a. The IP packet at right carries data of an application that uses SSL. Indicate the parts of the packet occupied by all the headers and data upto (and including) the SSL data.

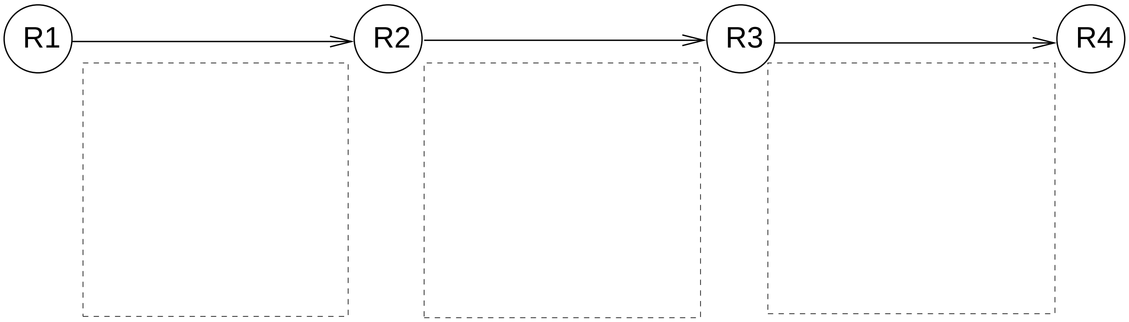


b. Can an attacker stop the application after it is connected by tampering with just one packet. Explain briefly.

8. What is DNS cacheing?

9. Can a DNS attack succeed in the absence of DNS cacheing?

10. Below is one circuit of a MixNet. Let pk_i be the public key of node Ri Node R1 wants to send message m to node R4. In the box below each link, give the message that is actually sent bover the link.



11. Give the steps to set up a hidden service X on host D in a Tor network.

12. TCP uses a 3-way handshake for connection establishment:

- client sends SYN
- server receives SYN, responds with SYN+ACK
- client receives SYN+ACK, becomes open, responds with ACK.
- server receives ACK, becomes open.

Why does TCP not use a 2-way handshake as follows:

- client sends SYN
- server receives SYN, becomes open, responds with SYN+ACK
- client receives SYN+ACK, becomes open, responds with ACK.

12. What is congestion control. How is this achieved with ACKs in TCP.

13. Why does a SYN cookie include a slow-moving timestamp.

14. Give the steps of the Mitnick attack.

15. What is a defense against the Mitnick attack.

16. Give the steps of the opt-ack attack.

15. What is a defense against the opt-ack attack.