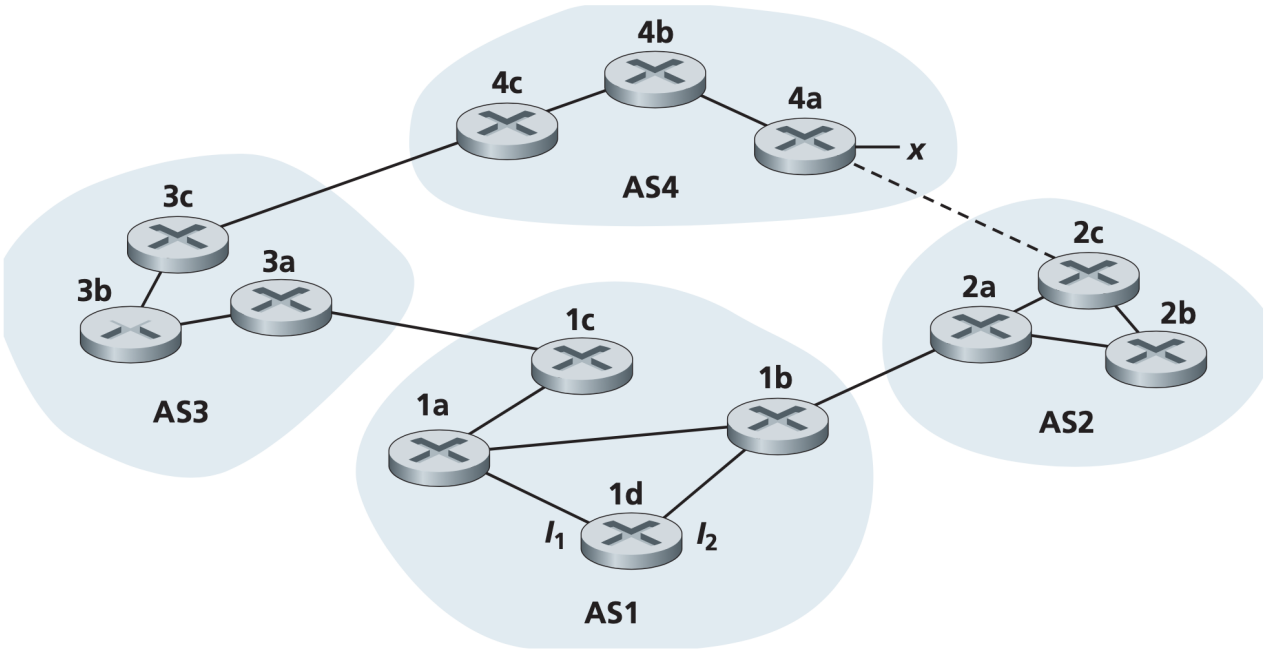
Final Practice

All questions need to be answered.

Qn1. For each of the statements/questions, circle the number if it is TRUE or cross the number if it is FALSE.

1. The DHCP protocol uses TCP for communication. (F)
2. The IPv6 header does not contain a fragmentation field. (T)
3. The Time-to-live (TTL) field helps reduce the extent of packet flooding in the network. (T)
4. In BGP, a host in one AS uses hot-potato routing to route packets to a destination in another AS. (F)
5. MAC addresses are 47 bits long. (F)
6. OSPF is used for inter-AS routing. (F)

Qn2. Consider the network shown below. Suppose AS3 and AS2 are running OSPF for their intra-AS routing protocol. Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.



1. Router 3c learns about prefix x from which routing protocol: OSPF, RIP, eBGP, or iBGP?

   eBGP

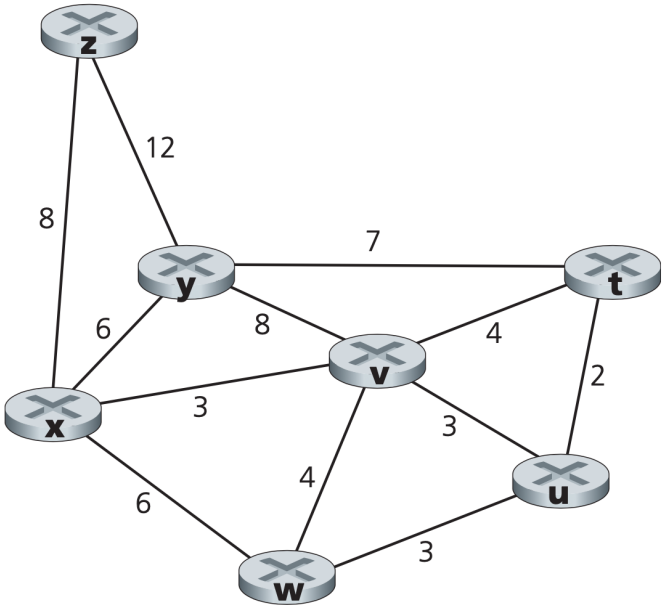
2. Referring to the above problem, once router 1d learns about x it will put an entry (x, I) in its forwarding table. Will I be equal to I1 or I2 for this entry? Explain why in one sentence.

   I1, because this interface begins the least cost path from 1d towards the gateway router 1c.

3. Now suppose that there is a physical link between AS2 and AS4, shown by the dotted line. Suppose router 1d learns that x is accessible via AS2 as well as via AS3. Will I be set to I1 or I2? Explain why in one sentence.

   I2. Both routes have equal AS-PATH length but I2 begins the path that has the closest NEXT-HOP router.

Qn3. In the graph below



1. Using x as the source and assuming the link-state routing algorithm is used, at steady state, illustrate the Dijkstra's algorithm (show all steps)

   Please check the slides for detail Dijkstra's algorithm.

2. Illustrate the routing table at x.

Qn4. Consider a router that interconnects three subnets: Subnet 1, Subnet 2, and Subnet 3. Suppose all of the interfaces in each of these three subnets are required to have the prefix 223.1.17/24. Also suppose that Subnet 1 is required to support at least 60 interfaces, Subnet 2 is to support at least 90 interfaces, and Subnet 3 is to support at least 12 interfaces. Provide three network addresses (of the form a.b.c.d/x) that satisfy these constraints.

223.1.17/24 = 11011111 00000001 00010001 ????????

Subnet 1: 223.1.17.0/26

Subnet 2: 223.1.17.128/25

Subnet 3: 223.1.17.64/28

The answers could be different as long as they fit the requirements.

Qn5. Of the several MAC algorithms you have studied, which MAC algorithm do you think is suitable for each of the following situations and Briefly mention Why?

1. The number of hosts in the network is 100 and they are always transmitting.

   channel partitioning MAC protocols (TDMA, FDMA)

2. There are 1000 users in the network, all talk to each other through a central node, which can manage the whole network.

   taking turns MAC protocols (polling, token passing)

Qn6. Assume there is a Certificate Authority (CA) with a well-known public key. Further assume every user is issued a certificate for his/her public key. For convenience, we use PKu and SKu to represent user u's public key and private key, respectively. Please answer the following questions (you can draw figures to better illustrate your answer).

1. Suppose Alice wants to send a large secret message M to Bob. Describe how Alice should send M in an authenticated way.

   Alice send the concatenation of her certificate, session key encrypted by her private key, and the message encrypted by the secret key.

   The message is $[C_A, SK_A(S_k), S_k(M)]$**.**

   It's similar to the email encryption.

2. Assume Bob receives the message sent by Alice. Describe how Bob should process the message.

   Bob first verify the certificate, then use the public key PK_A **to extract the secret key** S_k**, and decrypt the message** M **using** S_k**.**

3. Suppose Alice needs to send a number of large secret messages to Bob. Alice would like to avoid signing digital signatures for all these messages. Develop a protocol for Alice and Bob so that all the messages can be sent in a confidential and authenticated way. Briefly describe the intuition of your protocol first and then draw a diagram.

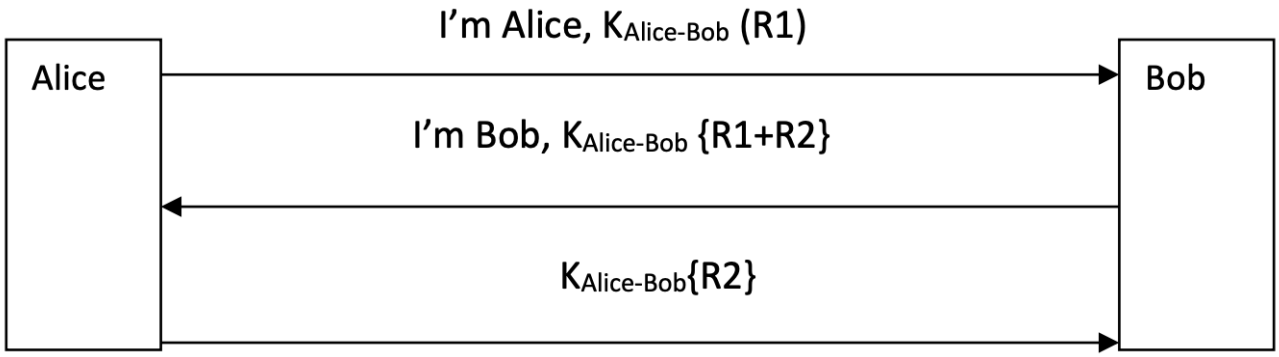
   The process is similar to TLS. Please check TLS in slides for details.

Qn7. Assume the internal network is 222.22/16. Please draw a filter table and a connection table for a stateful firewall that accomplishes the following:

1. allow internal users to surf the Web except Web server 208.65.153.238 (YouTube)
2. allow DNS packets to enter and leave the internal network
3. otherwise blocks all inbound and outbound traffic

action	source address	dest address	proto	source port	dest port	flag bit	check connection
allow	222.22/16	outside of 222.22/16 (except 208.65.153.238)	TCP	> 1023	80	any	
allow	outside of 222.22/16 (except 208.65.153.238)	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Qn8. In a three-message authentication protocol, Alice initiates contact with Bob. Assume that Alice and Bob share a key KAlice-Bob. The protocol works as follows, where R1 and R2 are random numbers generated by Alice and Bob, respectively.



1. Does this protocol provide mutual authentication? If yes, why? If no, who cannot authenticate whom and why? Please first answer Yes or No and then give your answer.

   No, Alice cannot authenticate Bob. Bob can send any arbitrary encrypted message to bypass the authentication.

2. Could a third person, Trudy, impersonate Alice? Describe a possible attack scenario. If it is not possible, clearly state so and give reasons. Please first answer Yes or No and then give your answer.

   No, Trudy cannot derive R2.