1.

THE NETWORK LAYER - WHERE IS IT?

Check all of the statements below about where (in the network) the network layer is implemented that are true.

- [ ] The network layer is implemented in wired Internet-connected devices but not wireless Internet-connected devices.
- [x] The network layer is implemented in hosts at the network's edge.
- [ ] The network layer is implemented in Ethernet switches in a local area network.
- [x] The network layer is implemented in routers in the network core.

That's Correct!

CHECK →

1/5

FORWARDING VERSUS ROUTING.

Consider the travel analogy discussed in the textbook - some actions we take on a trip correspond to forwarding and other actions we take on a trip correspond to routing. Which of the following travel actions below correspond to *forwarding*? The other travel actions that you don't select below the correspond to routing.

- [ ] A traveler decides to fly to Sydney through Singapore rather that Dubai.
- [x] A car takes the 3rd exit from a roundabout.
- [x] A car waits at light and then turns left at the intersection.
- [ ] A car takes highway 80 between New York and Chicago, rather than highway 87 to Albany and from there take Interstate 90 to Chicago.
- [ ] A climber decides to take the South Col Route to the top of Mt Everest rather than the Northeast Ridge route.
- [x] A car stops at an intersection to “gas-up” and take a “bathroom break”

That's Correct!

← CHECK →

2/

THE CONTROL PLANE VERSUS THE DATA PLANE.

For each of the actions below, select those actions below that are primarily in the network-layer data plane. The other actions that you don't select below then correspond to control-plane actions.

- [ ] Computing the contents of the forwarding table.
- [x] Looking up address bits in an arriving datagram header in the forwarding table.
- [ ] Monitoring and managing the configuration and performance of an network device.
- [x] Dropping a datagram due to a congested (full) output buffer.
- [x] Moving an arriving datagram from a router's input port to output port

That's Correct!

← CHECK →

3/

WHAT TYPE OF CONTROL PLANE?

We've seen that there are two approaches towards implementing the network control plane - a per-router control-plane approach and a software-defined networking (SDN) control-plane approach. Which of the following actions occur in a per-router control-plane approach? The other actions that you don't select below then correspond to actions in an SDN control plane.

- [ ] All routers in the network send information about their incoming and outgoing links to a logically centralized controller.
- [x] Routers send information about their incoming and outgoing links to other routers in the network.
- [x] A router exchanges messages with another router, indicating the cost for it (the sending router) to reach a destination host.
- [ ] A control agent in router receives a complete forwarding table, which it installs and uses to locally control datagram forwarding.

That's Correct!

← CHECK →

4/

BEST EFFORT SERVICE.

Which of the following quality-of-service guarantees are part of the Internet's best-effort service model? Check all that apply.

- [ ] A guaranteed minimum bandwidth is provided to a source-to-destination flow of packets
- [x] *None* of the other services listed here are part of the best-effort service model. Evidently, best-effort service really means no *guarantees* at all!
- [ ] In-order datagram payload delivery to the transport layer of those datagrams arriving to the receiving host.
- [ ] Guaranteed delivery time from sending host to receiving host.
- [ ] Guaranteed delivery from sending host to receiving host.

That's Correct!

← CHECK

5/

3

WHAT IS THE INTERNET PROTOCOL?

What are the principal components of the IPv4 protocol (check all that apply)?

- [ ] SDN controller protocols.
- [x] IPv4 datagram format.
- [x] IPv4 addressing conventions.
- [x] Packet handling conventions at routers (e.g., segmentation/reassembly)
- [ ] Routing algorithms and protocols like OSPF and BGP.
- [ ] ICMP (Internet Control Message Protocol)

That's Correct!

CHECK →

Version field

=

Type-of-service field

E

Fragmentation offset field

D

Time-to-live field

A

Header checksum field

H

Upper layer field

B

Payload/data field

C

Datagram length field.

G

A. The value in this field is decremented at each router; when it reaches zero, the packet must be dropped.

B. This field contains the "protocol number" for the transport-layer protocol to which this datagram's payload will be demultiplexed - UDP or TCP, for example.

C. This field *contains* a UDP or TCP segment, for example.

D. This field is used for datagram fragmentation/reassembly.

E. This field contains ECN and differentiated service bits.

F. This field contains the IP protocol version number.

G. This field indicates the total number of bytes in datagram.

H. This field contains the Internet checksum of this datagram's header fields.

WHAT IS AN IP ADDRESS ACTUALLY ASSOCIATED WITH?

Which of the following statements is true regarding an IP address? (Zero, one or more of the following statements is true).

- [ ] It is not necessary for a device using the IP protocol to actually have an IP address associated with it.
- [x] If a host has more than one interface, then it has more that one IP address at which it can be reached.
- [x] An IP address is associated with an interface.
- [x] If a router has more than one interface, then it has more that one IP address at which it can be reached.

That's Correct!

← CHECK →

WHAT IS A SUBNET?

What is meant by an IP subnet? (Check zero, one or more of the following characteristics of an IP subnet).

- [ ] A set of devices all manufactured by the same equipment maker/vendor.
- [x] A set of device interfaces that can physically reach each other without passing through an intervening router.
- [ ] A set of devices that always have a common first 16 bits in their IP address.
- [x] A set of devices that have a common set of leading high order bits in their IP address.

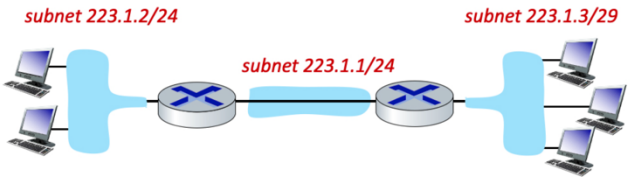
That's Correct!

← CHECK →

4/1

SUBNETTING(A).

Consider the three subnets in the diagram below.



What is the maximum # of interfaces in the 223.1.2/24 network?

- ○ 2**32
- ○ 128
- ◉ 256
- ○ Two hosts, as shown in the figure.
- ○ There's no a priori limit on the number of interfaces in this subnet.

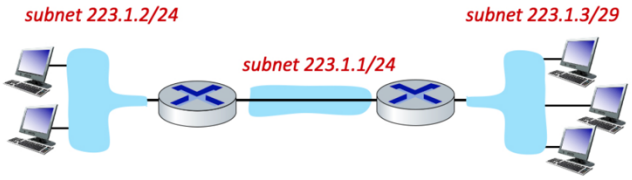
That's Correct!

← CHECK →

5/1

SUBNETTING(B).

Consider the three subnets in the diagram below.



What is the maximum # of interfaces in the 223.1.3/29 network?

- 128
- Three hosts, as shown in the figure.
- 8
- There's no a priori limit on the number of interfaces in this subnet.
- 2**32

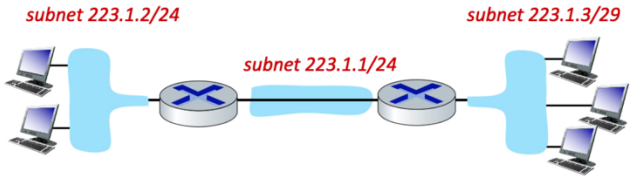
That's Correct!

← CHECK →

6/1

SUBNETTING(C).

Consider the three subnets in the diagram below.



Which of the following addresses can *not* be used by an interface in the 223.1.3/29 network? Check all that apply.

- [x] 223.1.2.6
- [ ] 223.1.3.6
- [x] 223.1.3.16
- [x] 223.1.3.28
- [ ] 223.1.3.2

That's Correct!

← CHECK →

7/1

PLUG-AND-PLAY.

What is meant by saying that DHCP is a "plug and play" protocol?

- ○ The host needs to "plug" (by wire or wirelessly) into the local network in order to access ("play" in) the Internet
- ◉ No manual configuration is needed for the host to join the network.
- ○ The network provides an Ethernet jack for a host's Ethernet adapter.

That's Correct!

← CHECK →

8/11

DHCP REQUEST MESSAGE.

Which of the following statements about a DHCP request message are true (check all that are true). Hint: check out Figure 4.24 in the 7th and 8th edition of our textbook.

- ☑ The transaction ID in a DHCP request message will be used to associate this message with future DHCP messages sent from, or to, this client.
- ☑ A DHCP request message *may* contain the IP address that the client will use.
- ☐ A DHCP request message is sent from a DHCP server to a DHCP client.
- ☐ A DHCP request message is optional in the DHCP protocol.
- ☑ A DHCP request message is sent broadcast, using the 255.255.255.255 IP destination address.
- ☐ The transaction ID in a DCHP request message is used to associate this message with previous messages sent by this client.

That's Correct!

← CHECK →

9/11

IPV4 VERSUS IPV6.

Which of the following fields occur *ONLY* in the IPv6 datagram header (i.e., appear in the IPv6 header but not in the IPv4 header)? Check all that apply.

- [ ] The upper layer protocol (or next header) field.
- [ ] The header length field.
- [ ] The options field.
- [x] 128-bit source and destination IP addresses.
- [ ] The IP version number field.
- [x] The flow label field.
- [ ] The header checksum field.
- [ ] The time-to-live (or hop limit) field.

That's Correct!

← CHECK →

10/11

PURPOSE OF DHCP.

What is the purpose of the Dynamic Host Configuration Protocol?

- ○ To get the 48-bit link-layer MAC address associated with a network-layer IP address.
- ◉ To obtain an IP address for a host attaching to an IP network.
- ○ To configure the set of available open ports (and hence well-known services) for a server.
- ○ To configure the interface speed to be used, for hardware like Ethernet, which can be used at different speeds.

That's Correct!

← CHECK

11/11

4. https://www.studocu.com/en-us/document/california-state-polytechnic-university-pomona/computer-networks/ch-4-6-knowledge-checks/47634006

DESTINATION-BASED MATCH+ACTION.

Destination-based forwarding, which we studied in section 4.2, is a specific instance of match+action and generalized forwarding. Select the phrase below which best completes the following sentence:

"In destination-based forwarding, ..."

- ... after *matching* on the port number in the segment's header, the *action* taken is to forward the datagram to the output port associated with that port number.
- ... after *matching* on the 48-bit link-layer destination MAC address, the *action* taken is to forward the datagram to the output port associated with that link-layer address.
- ... after *matching* on the source and destination IP address in the datagram header, the *action* taken is to forward the datagram to the output port associated with that source and destination IP address pair.
- ... after *matching* on the destination IP address in the datagram header, the *action* taken is to forward the datagram to the output port associated with that destination IP address.
- ... after *matching* on the port number in the segment's header, the *action* taken is to decide whether or not to drop the datagram containing that segment.
- ... after *matching* on the URL contained in an HTTP GET request in the TCP segment within the IP datagram, the *action* taken is to determine the IP address of the server associated with that URL, and to forward the datagram to the output port associated with that destination IP address.
- ... after *matching* on the destination IP address in the datagram header, the *action* taken is to decide whether or not to drop that datagram.

That's Correct!

CHECK →

1/7

GENERALIZED MATCH+ACTION.

Which of the following match+actions can be taken in the generalized OpenFlow 1.0 match+action paradigm that we studied in Section 4.4? Check all that apply.

- [ ] ... after *matching* on the URL contained in an HTTP GET request in the TCP segment within the IP datagram, the *action* taken is to determine the IP address of the server associated with that URL, and to forward the datagram to the output port associated with that destination IP address.
- [x] ... after *matching* on the destination IP address in the datagram header, the *action* taken is to forward the datagram to the output port associated with that destination IP address.
- [x] ... after *matching* on the source and destination IP address in the datagram header, the *action* taken is to forward the datagram to the output port associated with that source and destination IP address pair.
- [x] ... after *matching* on the 48-bit link-layer destination MAC address, the *action* taken is to forward the datagram to the output port associated with that link-layer address.
- [x] ... after *matching* on the destination IP address in the datagram header, the *action* taken is to decide whether or not to drop that datagram.
- [x] ... after *matching* on the port number in the segment's header, the *action* taken is to forward the datagram to the output port associated with that destination IP address.
- [x] ... after *matching* on the port number in the segment's header, the *action* taken is to decide whether or not to drop that datagram containing that segment.

That's Correct!

← CHECK →

2/7

WHAT FIELDS CAN BE MATCHED IN GENERALIZED MATCH+ACTION.

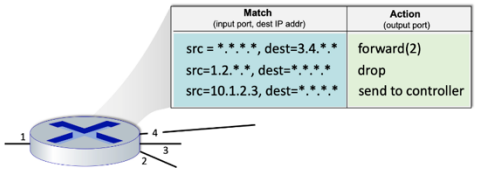
Which of the following fields in the frame/datagram/segment/application-layer message can be matched in OpenFlow 1.0? Check all that apply.

- [x] IP destination address
- [ ] Time-to-live field
- [x] Source and/or destination port number
- [ ] URL in HTTP message
- [ ] Number of bytes in the datagram
- [x] IP type-of-service field
- [x] IP source address
- [x] Upper layer protocol field

That's Correct!

← CHECK →

Consider the figure below that shows the generalized forwarding table in a router. Recall that a * represents a wildcard value. Now consider an arriving datagram with the IP source and destination address fields indicated below. For each source/destination IP address pair, indicate which rule is matched. Note: assume that a rule that is earlier in the table takes priority over a rule that is later in the table and that a datagram that matches none of the table entries is dropped.



QUESTION LIST:

Source: 1.2.56.32 Destination:128.116.40.186

C

Source: 65.92.15.27 Destination: 3.4.65.76

3

Source: 10.1.2.3 Destination: 7.8.9.2

D

Source: 10.1.34.56 Destination: 54.72.29.90

A

ANSWER LIST:

A. No match to any rule.

B. Rule 1, with action *forward(2)*

C. Rule 2, with action *drop*

D. Rule 3, with action *send to controller*

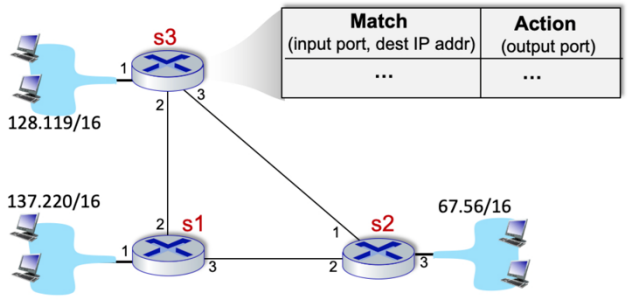
That's Correct!

← CHECK →

Consider the network below. We want to specify the match+action rules at s3 so that only the following network-wide behavior is allowed:

1. traffic from 128.119/16 and destined to 137.220/16 is forwarded on the direct link from s3 to s1;
2. traffic from 128.119/16 and destined to 67.56/16 is forwarded on the direct link from s3 to s2;
3. incoming traffic via port 2 or 3, and destined to 128.119/16 is forwarded to 128.119/16 via local port 1.
4. No other forwarding should be allowed. In particular s3 should not forward traffic arriving from 137.220/16 and destined for 67.56/16 and vice versa.

From the list of match+action rules below, select the rules to include in s3's flow table to implement this forwarding behavior. Assume that if a packet arrives and finds no matching rule, it is dropped.



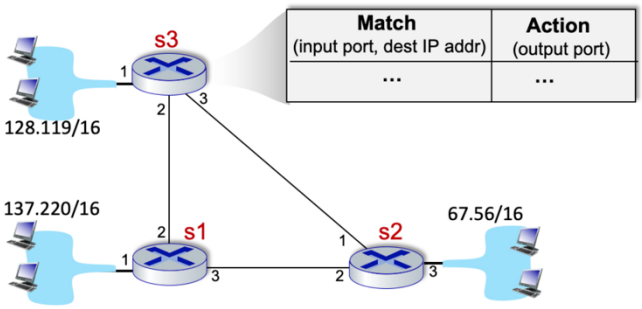
- [ ] Input port:1 ; Dest: 137.220/16 Action: forward(3)
- [x] Input port: 3; Dest: 128.119/16 Action: forward(1)
- [ ] Input port: 2; Dest: 67.56/16 Action: forward(3)
- [x] Input port: 2; Dest: 128.119/16 Action: forward(1)
- [ ] Input port: 1; Dest: 67.56/16 Action: forward(2)
- [ ] Input port: 3; Dest: 137.220/16 Action: forward(2)
- [x] Input port:1 ; Dest: 137.220/16 Action: forward(2)
- [x] Input port: 1; Dest: 67.56/16 Action: forward(3)

That's Correct!

← CHECK →

Consider the network below. We want to specify the match+action rules *at s3* so that s3 *acts only as a relay* for traffic between 137.220/16 and 67.56/16. In particular s3 should not accept/forward and traffic to/from 128.119/16.

From the list of match+action rules below, select the rules to include in s3's flow table to implement this forwarding behavior. Assume that if a packet arrives and finds no matching rule, it is dropped.



- [ ] Input port: 1; Dest: 67.56/16 Action: forward(3)
- [x] Input port: 2; Dest: 67.56/16 Action: forward(3)
- [ ] Input port:1 ; Dest: 137.220/16 Action: forward(3)
- [ ] Input port:1 ; Dest: 137.220/16 Action: forward(2)
- [ ] Input port: 1; Dest: 67.56/16 Action: forward(2)
- [x] Input port: 3; Dest: 137.220/16 Action: forward(2)
- [ ] Input port: 3; Dest: 128.119/16 Action: forward(1)
- [ ] Input port: 2; Dest: 128.119/16 Action: forward(1)

That's Correct!

← CHECK →

6/

GENERALIZED FORWARDING.

What is meant by generalized forwarding (as opposed to destination-based forwarding) in a router or switch?

- (•) Any of several actions (including drop (block), forward to a given interface, or duplicate-and-forward) can be made based on the contents of one or more packet header fields.
- ( ) In addition to performing forwarding, the device can generalize its services, also performing hop-by-hop reliable data transfer and per-hop congestion control.
- ( ) None of the other answers is a correct definition of generalized forwarding.
- ( ) The decision about which output port to forward a packet to can be made based on the link-type of the outgoing port (e.g., Ethernet versus WiFi).

That's Correct!

← CHECK

7/7