WHAT IS THE INTERNET? – CHAPTER 1

Which of the following descriptions below correspond to a *"nuts-and-bolts"* view of the Internet? Select one or more of the answers below that are correct. [Hint: more than one of answers below are correct].

- [x] A collection of hardware and software components executing protocols that define the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.
- [ ] A place I go for information, entertainment, and to communicate with people.
- [ ] A platform for building network applications.
- [x] A "network of networks".
- [x] A collection of billions of computing devices, and packet switches interconnected by links.

Which of the following descriptions below correspond to a *"services"* view of the Internet? Select one or more of the answers below below that are correct below that are correct. [Hint: more than one of answers below are correct].

- [ ] A collection of hardware and software components executing protocols that define the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.
- [x] A place I go for information, entertainment, and to communicate with people.
- [ ] A "network of networks".
- [ ] A collection of billions of computing devices, and packet switches interconnected by links.
- [x] A platform for building network applications.

Which of the following human scenarios involve a protocol (recall: "Protocols define the format, order of messages sent and received among network entities, and actions taken on message transmission, receipt")? Select one or more answers below that are correct. Hint: more than one of answers below are correct.

- [x] One person asking, and getting, the time to/from another person.
- [ ] A person reading a book.
- [ ] A person sleeping.
- [x] Two people introducing themselves to each other.
- [x] A student raising her/his hand to ask a really insightful question, followed by the teaching acknowledging the student, listening carefully to the question, and responding with a clear, insightful answer. And then thanking the student for the question, since teachers *love* to get questions.

---

2. The Network Edge

ACCESS NETWORK PER-SUBSCRIBER SPEEDS.

Match the access network with the approximate speeds that a subscriber might experience. (Note: if you look these up, do so in the 8E textbook, slides,or video -- not in the 7E or earlier versions, since link access speeds are always increasing over the years).

QUESTION LIST:

Ethernet

D

802.11 WiFi

B

Cable access network

G

Digital Subscriber Line

A

4G cellular LTE

C

ANSWER LIST:

A. Wired. Up to 10’s of Mbps downstream per user.
B. Wireless. 10’s to 100’s of Mbps per device.
C. Wireless. Up to 10’s Mbps per device.
D. Wired. Up to 100's Gbps per link.
E. Wired. Up to 1 Tbps per link.
F. Wireless, up to 10's Kbps per device.
G. Wired. Up to 10’s to 100’s of Mbps downstream per user.

LINK TRANSMISSION CHARACTERISTICS.

Which of the following physical layer technologies has the highest transmission rate *and* lowest bit error rate in practice?

- ○ 4G/5G cellular
- ○ wisted pair (e.g., CAT5, CAT6)
- ◉ Fiber optic cable
- ○ Coaxial cable
- ○ Satellite channel
- ○ 802.11 WiFi Channel

---

3. The Network Core

ROUTING VERSUS FORWARDING.

ĐỊNH TUYẾN SO VỚI CHUYỂN TIẾP

Choose one the following two definitions that makes the correct distinction between routing versus forwarding.(phân biệt chính xác giữa định tuyến và chuyển tiếp)

- ○ **Routing** is the local action of moving arriving packets from router's input link to appropriate router output link, while **forwarding** is the global action of determining the source-destination paths taken by packets.
- ◉ **Forwarding** is the local action of moving arriving packets from router's input link to appropriate router output link, while **routing** is the global action of determining the source-destination paths taken by packets.

PACKET SWITCHING VERSUS CIRCUIT SWITCHING (1).

Which of the characteristics below are associated with the technique of *packet switching*? Select all correct answers. [Hint: more than one of the answers is correct].

- ☐ Reserves resources needed for a call from source to destination.
- ☑ Data may be queued before being transmitted due to other user's data that's also queueing for transmission.
- ☐ Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) are two approaches for implementing this technique.
- ☐ This technique was the basis for the telephone call switching during the 20th century and into the beginning of this current century.
- ☑ Resources are used on demand, not reserved in advance.
- ☑ Congestion loss and variable end-end delays are possible with this technique.
- ☑ This technique is used in the Internet.

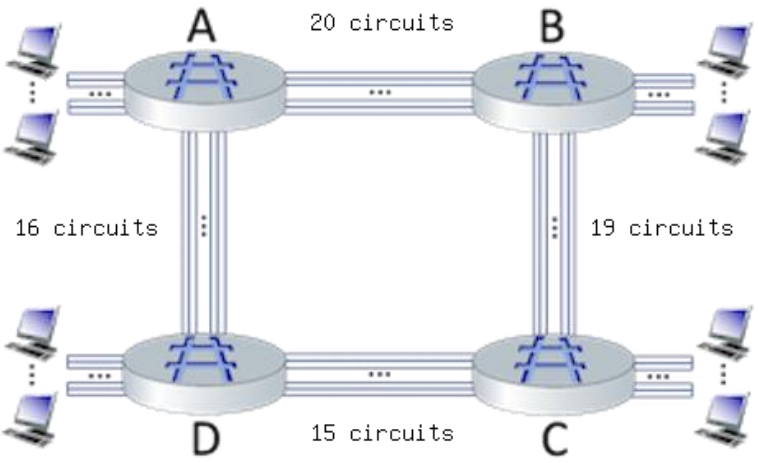
PACKET SWITCHING VERSUS CIRCUIT SWITCHING (2).

Which of the characteristics below are associated with the technique of *circuit switching*? Select all correct answers. [Hint: more than one of the answers is correct].

- [ ] Data may be queued before being transmitted due to other user's data that's also queueing for transmission.
- [ ] Resources are used on demand, not reserved in advance.
- [x] Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) are two approaches for implementing this technique.
- [ ] This technique is used in the Internet.
- [ ] Congestion loss and variable end-end delays are possible with this technique.
- [x] This technique was the basis for the telephone call switching during the 20th century and into the beginning of this current century.
- [x] Reserves resources needed for a call from source to destination.

HOW MANY CALLS CAN BE CARRIED?

Consider the circuit-switched network shown in the figure below, with four circuit switches A, B, C, and D. Suppose there are 20 circuits between A and B, 19 circuits between B and C, 15 circuits between C and D, and 16 circuits between D and A.



What is the maximum number of connections that can be ongoing in the network at any one time?

[Note: you can find more questions like this one here.

- ○ 20
- ○ 31

- (●) 70 (cộng lại hết là ra)
- ( ) 39
- ( ) 16

TRYING OUT TRACEROUTE.

Perform a traceroute from your computer (on whatever network you happen to be on) to gaia.cs.umass.edu. Use traceroute (on Mac terminal) or tracert (on Windows command line) or tracepath (on a Linux command line). Enter the missing part of the name of the router just before the host gaia.cs.umass.edu is reached:
??.cs.umass.edu

Note: Routing may change, so the answer here may not be correct anymore. Also, if you are a Verizon user, there are known problems using traceroute with Verizon - if traceroute shows you two hops only to gaia.cs.umass.edu or any destination, skip this question.

nscs1bbs1

WHAT IS A NETWORK OF NETWORKS?

When we say that the Internet is a “network of networks,” we mean? Check all that apply (hint: check two or more).

- [ ] The Internet is the *largest* network ever built.
- [ ] The Internet is the *fastest* network ever built.
- [x] The Internet is made up of access networks at the edge, tier-1 networks at the core, and interconnected regional and content provider networks as well.
- [x] The Internet is made up of a lot of different networks that are interconnected to each other.

PACKET SWITCHING OR CIRCUIT-SWITCHING?

Consider a scenario in which 5 users are being multiplexed over a channel of 10 Mbps. Under the various scenarios below, match the scenario to whether circuit switching or packet switching is better.

QUESTION LIST:

Each user generates traffic at an average rate of 2.1 Mbps, generating traffic at a rate of 15 Mbps when transmitting

A

Each user generates traffic at an average rate of 2 Mbps, generating traffic at a rate of 2 Mbps when transmitting

C

Each user generates traffic at an average rate of 0.21 Mbps, generating traffic at a rate of 15 Mbps when transmitting

B

ANSWER LIST:

A. Neither works well in this overload scenario (cả 2 đều không hoạt động tốt trong trường hợp bị quá tải)
B. Packet switching (chuyển mạch gói)

   https://vi.wikipedia.org/wiki/Chuy%E1%BB%83n_m%E1%BA%A1ch_g%C3%B3i

C. Circuit switching (chuyển mạch vòng)
   https://vi.wikipedia.org/wiki/Chuy%E1%BB%83n_m%E1%BA%A1ch_k%C3%AAnh

---

4. Performance: Delay, Loss and Throughput in Computer Networks

COMPONENTS OF PACKET DELAY.

Match the description of each component of packet delay to its name in the pull down list.

QUESTION LIST:

Time needed to perform an integrity check, lookup packet information in a local table and move the packet from an input link to an output link in a router.

A

Time spent waiting in packet buffers for link transmission.

C

Time spent transmitting packets bits into the link.

D

Time need for bits to physically propagate through the transmission medium from end one of a link to the other.

B

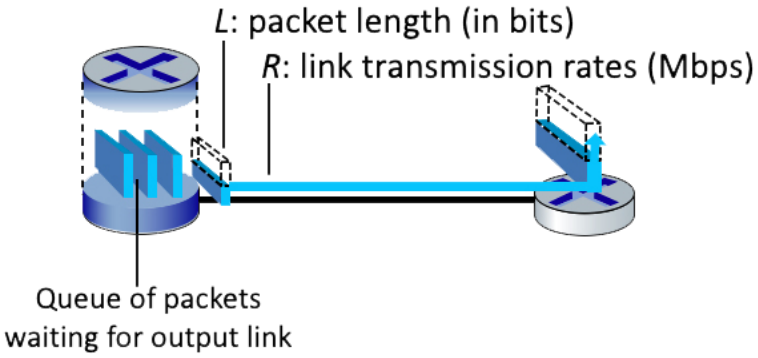
ANSWER LIST:

A. Processing delay

B. Propagation delay
C. Queueing delay
D. Transmission delay

COMPUTING PACKET TRANSMISSION DELAY(1).

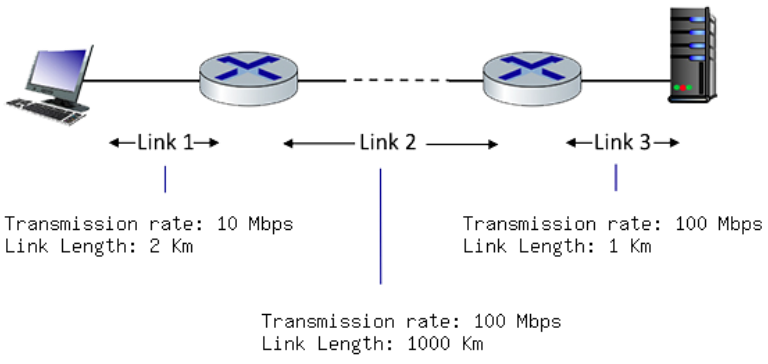
Suppose a packet is *L* = 1500 bytes long (one byte = 8 bits), and link transmits at R = 1 Gbps (i.e., a link can transmit bits 1,000,000,000 bits per second). What is the transmission delay for this packet? [Note: you can find more problems like this one here.]



- 666,666 secs
- .0000015 secs
- .000012 secs {(L*a)/R)
- .00012 secs
- .0015 secs

COMPUTING PACKET TRANSMISSION DELAY (3).

Consider the network shown in the figure below, with three links, each with the specified transmission rate and link length. Assume the length of a packet is 8000 bits.
Transmission delay is calculated by L / R
What is the transmission delay at **link 2?** [Note: you can find more problems like this one here.]



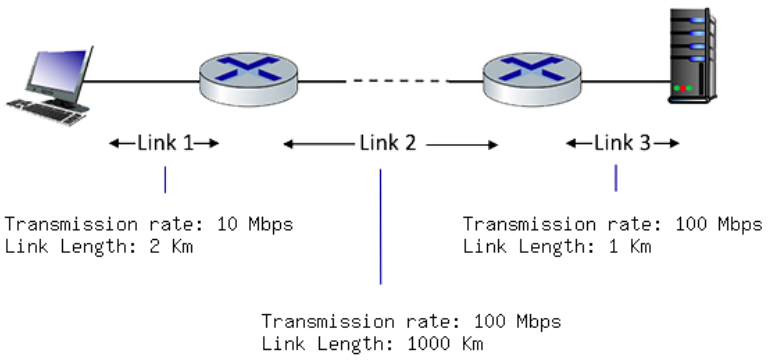
https://www.yumpu.com/en/document/read/22194701/computing-the-one-hop-transmission-delay-consider-the-figure- (tham khảo ở đây để biết làm) -> nhớ chuyển hết về 1 kiểu dữ liệu nhà như là bits/bits đừng để bits chia mbps nha

- 12.5 secs
- .00096 secs
- 12,500 secs
- 8 x 10^(-5) secs (nó hỏi là tại link 2 nha chứ k có hỏi là ở mọi điểm đâu)Ứ
- 100 secs

COMPUTING PROPAGATION DELAY.

Consider the network shown in the figure below, with three links, each with the specified transmission rate and link length. Assume the length of a packet is 8000 bits. The speed of light propagation delay on each link is 3x10^8 m/sec

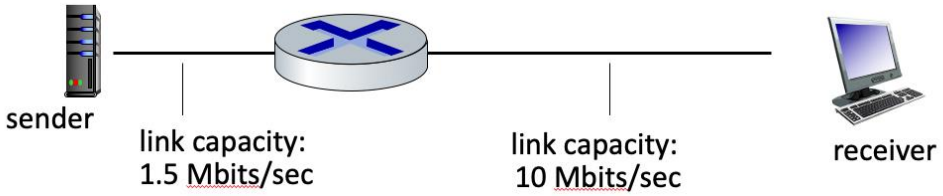
What is the propagation delay at (along) link 2?



- .33 secs
- 3 x 10^8 secs
- .0033 secs (d/s=quãng đg/thời gian)
- 3 secs

COMPUTING THROUGHPUT: A SIMPLE SCENARIO.

What is the maximum throughput achievable between sender and receiver in the scenario shown below?



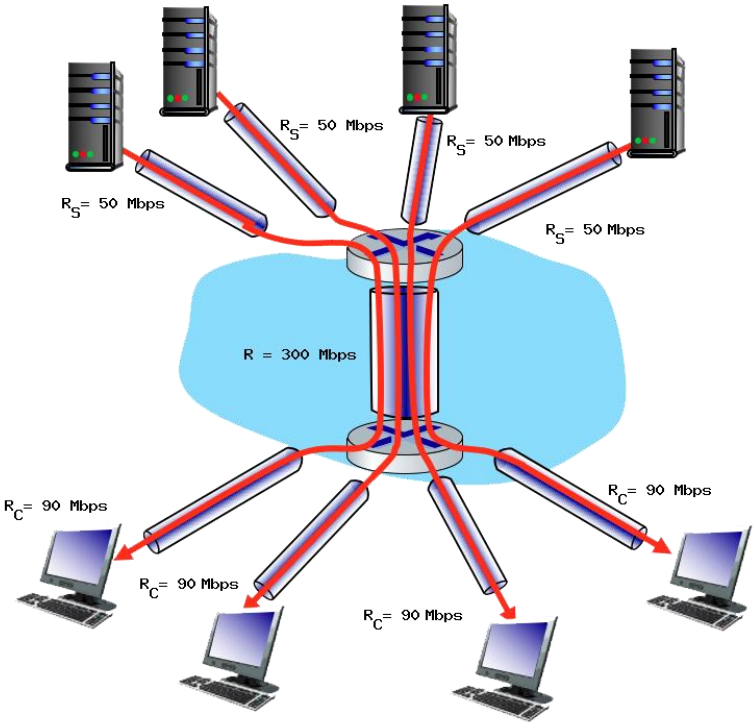
- 11.5 Mbps
- 1.5 Mbps
- 10 Mbps

COMPUTING THROUGHPUT.

https://itecnote.com/tecnote/end-to-end-throughput-and-bottleneck-links/

Consider the scenario shown below, with four different servers connected to four different clients over four three-hop paths. The four pairs share a common middle hop with a transmission capacity of R = 300 Mbps. The four links from the servers to the shared link have a transmission capacity of R_S = 50 Mbps. Each of the four links from the shared middle link to a client has a transmission capacity of R_C = 90 Mbps.
What is the maximum achievable end-end throughput (an integer value, in Mbps) for each of four client-to-server pairs, assuming that the middle link is fairly shared (divides its transmission rate equally) and all servers are trying to send at their maximum rate?
Your answer: [A] Mbps

the maximum achievable end-end throughput= min(Rs,Rc)



[Note: more questions like this one can be found here.]

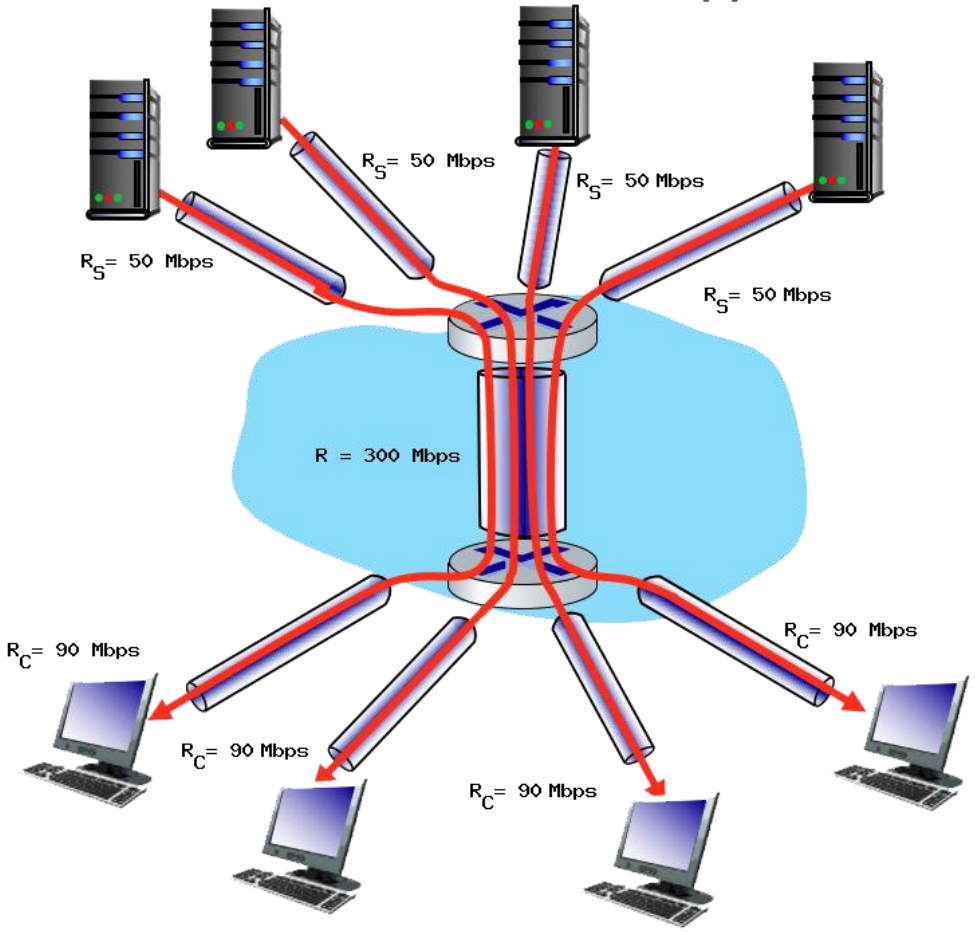
50

COMPUTING UTLILIZATION (1).

Consider the scenario shown below, with four different servers connected to four different clients over four three-hop paths. The four pairs share a common middle hop with a transmission capacity of R = 300 Mbps. The four links from the servers to the shared link have a transmission capacity of R_S = 50 Mbps. Each of the four links from the shared middle link to a client has a transmission capacity of R_C = 90 Mbps.

Assuming that the servers are all sending at their maximum rate possible, what are the link utilizations for the server links (**with transmission capacity R_S**)? Enter your answer in a decimal form of 1.00 (if the utilization is 1) or 0.xx (if the utilization is less than 1, rounded to the closest xx).

Your answer: The utilization of the server links is: [A]



[Note: more questions like this one can be found here.]

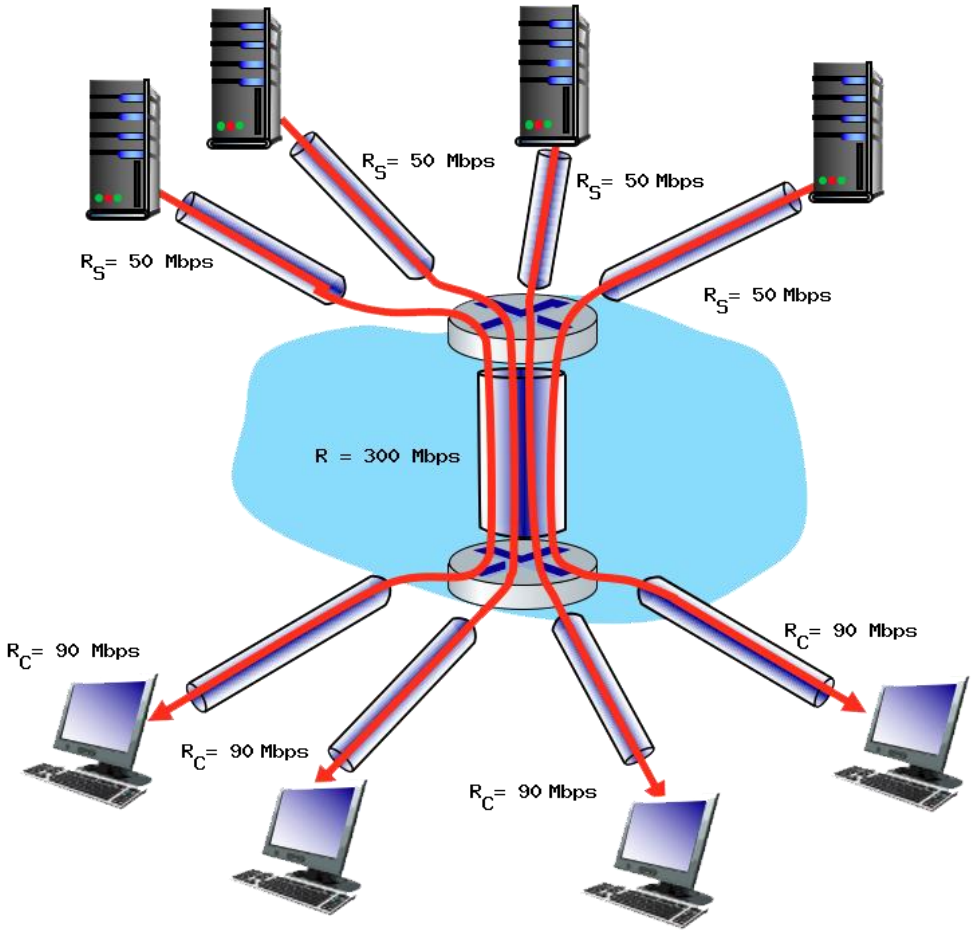
1.00 lấy maximum achievable end-end throughput chia cho Rs là ra

COMPUTING UTILIZATION (2).

Consider the scenario shown below, with four different servers connected to four different clients over four three-hop paths. The four pairs share a common middle hop with a transmission capacity of R = 300 Mbps. The four links from the servers to the shared link have a transmission capacity of R_S = 50 Mbps. Each of the four links from the shared middle link to a client has a transmission capacity of R_C = 90 Mbps.

Assuming that the servers are all sending at their maximum rate possible, what are the link utilizations of the shared link (**with transmission capacity R)?** Enter your answer in a decimal form of 1.00 (if the utilization is 1) or 0.xx (if the utilization is less than 1, rounded to the closest xx).

Your answer: The utilization of shared link is: [A]



[Note: more questions like this one can be found here.]

0.67 lấy maximum achievable end-end throughput chia cho R là ra

---

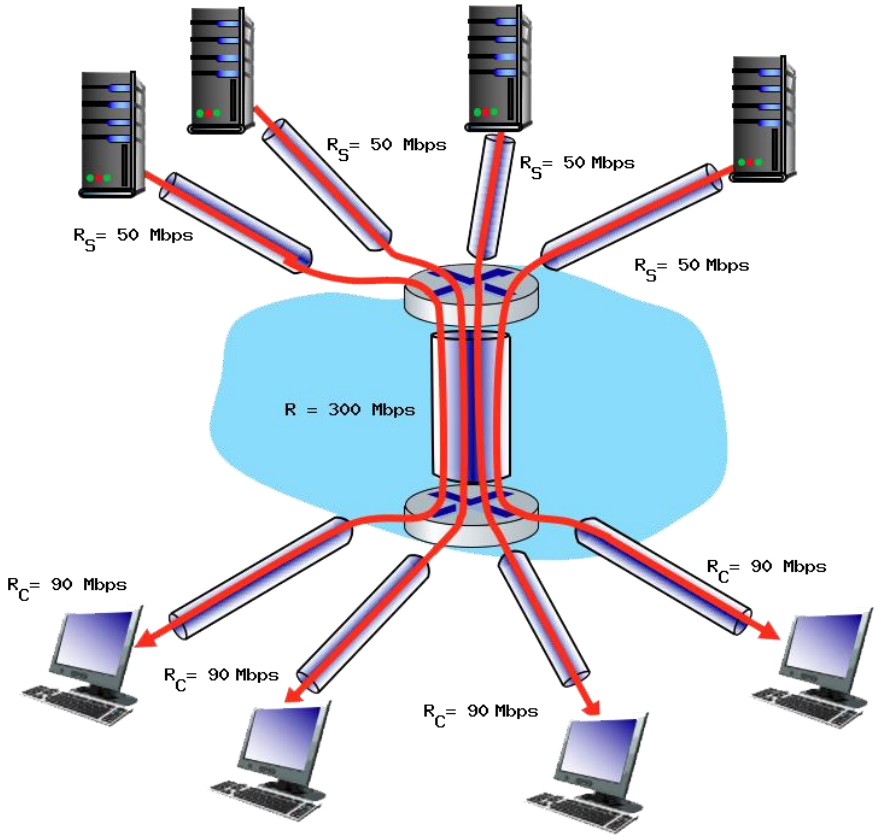
COMPUTING UTILIZATION (3).

Consider the scenario shown below, with four different servers connected to four different clients over four three-hop paths. The four pairs share a common middle hop with a transmission capacity of R = 300 Mbps. The four links from the servers to the shared link have a transmission capacity of

R_s = 50 Mbps. Each of the four links from the shared middle link to a client has a transmission capacity of R_c = 90 Mbps.

Assuming that the servers are all sending at their maximum rate possible, what are the link utilizations of the client links (with transmission capacity R_c)? Enter your answer in a decimal form of 1.00 (if the utilization is 1) or 0.xx (if the utilization is less than 1, rounded to the closest xx).

Your answer: The utilization of client link is: [A]



[Note: more questions like this one can be found here.]

0.56 lấy maximum achievable end-end throughput chia cho Rc là ra

---

5. Protocol layers and Their Service Models

LAYERS IN THE INTERNET PROTOCOL STACK.

Match the function of a layer in the Internet protocol stack to its its name in the pulldown menu.

QUESTION LIST:

Protocols that are part of a distributed network application.

B

Transfer of data between one process and another process (typically on different hosts).

A

Delivery of datagrams from a source host to a destination host (typically).

E

Transfer of data between neighboring network devices.

C

Transfer of a bit into and out of a transmission media.

D

ANSWER LIST:

A. Transport layer
B. Application Layer
C. Link layer
D. Physical layer
E. Network layer

WHAT'S A "PACKET" REALLY CALLED?

Match the name of an Internet layer with unit of data that is exchanged among protocol entities at that layer, using the pulldown menu.

QUESTION LIST:

Application layer

C

Transport layer

E

Network layer

A

Link layer

B

Physical layer

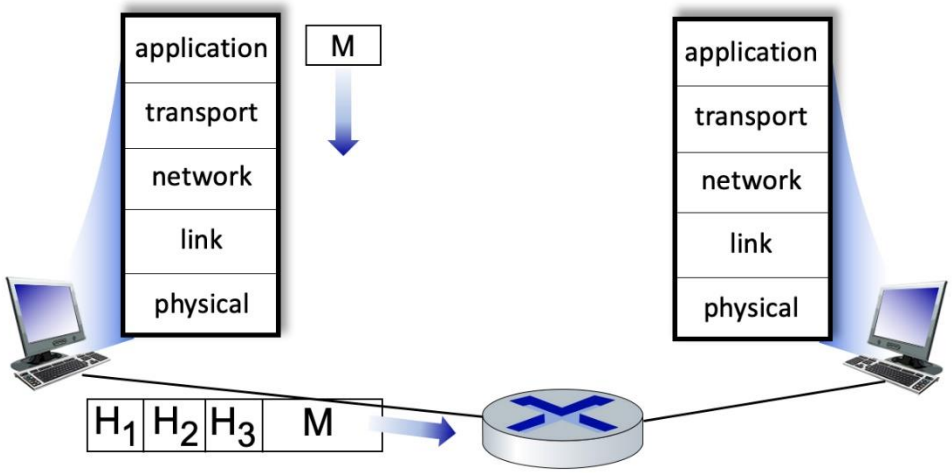
D

ANSWER LIST:

A. Datagram
B. Frame
C. Message
D. Bit
E. Segment

PROTOCOL HEADERS.

Consider the figure below, showing a link-layer frame heading from a host to a router. There are three header fields shown. Match the name of a header with a header label shown in the figure.



QUESTION LIST: SLIDE CHƯƠNG 1 TRANG 72

Header H_1

C

Header H_2

Choose Answer

Header H_3

D

ANSWER LIST:

A. Network Layer
B. Physical layer
C. Link layer
D. Transport layer
E. Application layer

WHAT IS "ENCAPSULATION"?

Which of the definitions below describe what is meant by the term "encapsulation"?

- (●) Taking data from the layer above, adding header fields appropriate for this layer, and then placing the data in the payload field of the “packet” for that layer.
- ( ) Starting a transport layer timer for a transmitted segment, and then if an ACK segment isn’t received before the timeout, placing that segment in a retransmission queue.
- ( ) Computing the sum of all of the bytes within a packet and placing that value in the packet header field.
- ( ) Receiving a “packet” from the layer below, extracting the payload field, and after some internal actions possibly delivering that payload to an upper layer protocol.
- ( ) Determining the name of the destination host, translating that name to an IP address and then placing that value in a packet header field.

---

6. Networks under attack

SECURITY DEFENSES.

Match the description of a security defense with its name.

QUESTION LIST: SLIDE CHƯƠNG 1 TRANG65

Specialized “middleboxes” filtering or blocking traffic, inspecting packet contents inspections

D

Provides confidentiality by encoding contents

A

Used to detect tampering/changing of message contents, and to identify the originator of a message.

B

Limiting use of resources or capabilities to given users.

E

Proving you are who you say you are.

C

ANSWER LIST:

A. Encryption

B. Digital signatures
C. Authentication
D. Firewall
E. Access control

---

7. History of Computer Networking; Chapter 1 Summary

NETWORKING HISTORY - WHEN DID IT HAPPEN?

Match the networking event with the time frame when the event occurred.

QUESTION LIST:SILDE CHƯƠNG 1 TRANG 79

Early studies of packet switching by Baran, Davies, Kleinrock.

C

First ARPAnet node operational.

F

Internetting: DARPA researchers connect three networks together.

A

The Internet Protocol (IP) is standardized in RFC 791.

G

Congestion control is added to the TCP protocol.

H

The WWW starts up (note: the WWW design started at the end of previous decade).

B

Software-defined networking begins.

E

The number wireless Internet-connected devices surpasses the number of connected wired devices.

D

ANSWER LIST:

A. 1970's
B. 1990's
C. Early 1960's
D. 2010 - 2020
E. 2000-2010
F. Late 1960's
G. Early 1980's
H. Late 1980's

8.The Internet Today

"WHO CONTROLS THE INTERNET?"

Match an organization name below with the role of the organization in Internet governance. To answer this question you'll need to watch the Chapter 1 supplemental video on "Who Controls the Internet?".

QUESTION LIST:

Internet Governance Forum (IGF)

A

Internet Engineering Task Force (IETF)

C

3rd Generation Partnership Project (3GPP).

B

Internet Corporation for Assigned Names and Numbers (ICANN)

D

Institute for Electrical and Electronics Engineers

E

ANSWER LIST:

A. A multistakeholder deliberation body, convened by the United Nations, that does not *make* decisions but informs and inspires those who do.
B. Sets the technical standards for 3G, 4G, and 5G mobile cellular system.
C. Sets the technical standards for Internet infrastructure -- particularly protocols, device requirements, and data formats -- in more than 9000 Request for Comments (RFCs).
D. Handles (assigns, adjudicates) Internet names, and manages the root level of the DNS.
E. Sets the technical standard for Ethernet and WiFi link-layer standards.

WHAT DOES IT MEAN TO "USE" THE INTERNET?

In 2021, the International Telecommunications Union (ITU) reported that 61.6% of the worlds's population are "Internet users". What does it mean to be an "Internet user" according to the ITU? To answer this question you'll need to watch the chapter 1 supplemental video on "Who Uses the Internet?"

- That someone uses the Internet at least once a day, on average.
- That someone has used the Internet at least once in the last three months.
- That someone has used the Internet at least once in the last one month
- That someone uses the Internet at least once a week, on average.

THE DIGITAL DIVIDE.

Between 2010 and 2018, which of the following digital divides has changed the least in the US? To answer this question you'll need to watch the chapter 1 supplemental video on "Who Uses the Internet?" To answer this question you'll need to watch the chapter 1 supplemental video on "Who Uses the Internet?"

- The gap in Internet use between Black and Hispanic populations versus White populations in the US.
- The gap in Internet use between rural populations versus urban populations in the US.

CHAPTER 2: APPLICATION LAYER

1.Principles of Network Applications

THE CLIENT-SERVER PARADIGM.

Which of the characteristics below are associated with a client-server approach to structuring network applications (as opposed to a P2P approach)?

- [ ] A process requests service from those it contacts and will provide service to processes that contact it.

- [x] There is a server that is always on.
- [x] HTTP uses this application structure.
- [x] There is a server with a well known server IP address.
- [ ] There is *not* a server that is always on.

SILDE CHƯƠNG 2 TRANG 6

THE PEER-TO-PEER (P2P) PARADIGM.

Which of the characteristics below are associated with a **P2P** approach to structuring network applications (as opposed to a client-server approach)?

- [ ] There is a server that is always on.
- [x] A process requests service from those it contacts and will provide service to processes that contact it.
- [x] There is *not* a server that is always on.
- [ ] HTTP uses this application structure.
- [ ] There is a server with a well known server IP address.

SILDE CHƯƠNG 2 TRANG 7

UDP SERVICE.

When an application uses a UDP socket, what transport services are provided to the application by UDP? Check all that apply.

- [ ] *Real-time delivery.* The service will guarantee that data will be delivered to the receiver within a specified time bound.
- [ ] *Flow Control.* The provided service will ensure that the sender does not send so fast as to overflow receiver buffers.
- [ ] *Throughput guarantee*. The socket can be configured to provide a minimum throughput guarantee between sender and receiver.
- [ ] *Loss-free data transfer.* The service will reliably transfer all data to the receiver, recovering from packets dropped in the network due to router buffer overflow.
- [x] *Best effort service.* The service will make a best effort to deliver data to the destination but makes no guarantees(đảm bảo) that any particular segment of data will actually get there.
- [ ] *Congestion control.* The service will control senders so that the senders do not collectively send more data than links in the network can handle.

TCP SERVICE.

When an application uses a TCP socket, what transport services are provided to the application by TCP? Check all that apply.

- [x] *Loss-free data transfer.* The service will reliably transfer all data to the receiver, recovering from packets dropped in the network due to router buffer overflow.
- [ ] *Throughput guarantee.* The socket can be configured to provide a minimum throughput guarantee between sender and receiver.
- [x] *Flow Control.* The provided service will ensure that the sender does not send so fast as to overflow receiver buffers.
- [ ] *Real-time delivery.* The service will guarantee that data will be delivered to the receiver within a specified time bound.
- [ ] *Best effort service.* The service will make a best effort to deliver data to the destination but makes no guarantees that any particular segment of data will actually get there.

☑ *Congestion control.* The service will control senders so that the senders do not collectively send more data than links in the network can handle.

2.The Web and HTTP

“HTTP IS STATELESS.”

What do we mean when we say “HTTP is stateless”? In answering this question, assume that cookies are not used. Check all answers that apply.

☐ We say this when an HTTP server is not operational.
☐ An HTTP client does not remember the identities of the servers with which it has interacted.
☐ The HTTP protocol is not licensed in any country.
☐ An HTTP *client* does not remember anything about what happened during earlier steps in interacting with any HTTP server.
☑ An HTTP *server* does not remember anything about what happened during earlier steps in interacting with this HTTP client.
SILDE CHƯƠNG 2 TRANG 20

HTTP COOKIES.

What is an HTTP cookie used for?

○ A cookies is a code used by a server, carried on a client’s HTTP request, to access information the server had earlier stored about an earlier interaction with this *person.* [Think about the distinction between a *browser* and a *person*.]
○ A cookie is a code used by a client to authenticate a person’s identity to an HTTP server.
○ Like dessert, cookies are used at the end of a transaction, to indicate the end of the transaction.
○ A cookie is used to spoof client identity to an HTTP server.
○ A cookie is a code used by a server, carried on a client’s HTTP request, to access information the server had earlier stored about an earlier interaction with this Web *browser*. [Think about the distinction between a *browser* and a *person*.]

THE HTTP GET.

What is the purpose of the HTTP GET message?

○ The HTTP GET request message is sent by a web server to a web client to get the identity of the web client.
○ The HTTP GET request message is used by a web client to request a web server to send the requested object from the server to the client.
○ The HTTP GET request message is used by a web client to post an object on a web server.
○ The HTTP GET request message is sent by a web server to a web client to get the next request from the web client.

A DETAILED LOOK AT AN HTTP GET (1).

Suppose a client is sending an HTTP GET request message to a web server, gaia.cs.umass.edu. Suppose the client-to-server HTTP GET message is the following:

GET /kurose_ross_sandbox/interactive/quotation2.htm HTTP/1.1
Host: gaia.cs.umass.edu
Accept: text/plain, text/html, text/xml, image/jpeg, image/gif, audio/mpeg, audio/mp4, video/wmv, video/mp4,
Accept-Language: en-us, en-gb;q=0.1, en;q=0.7, fr, fr-ch, da, de, fi
If-Modified-Since: Wed, 09 Sep 2020 16:06:01 -0700
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.56 Safari/535.11

What version of HTTP is the client using?

[Note: you can find additional questions similar to this here.]

- 2
- 2.1
- 1
- 1.1 (nhìn vào GET rồi nhìn xuống cuối dòng get thấy HTTP/1.1 -> 1.1 là version)

DETAILED LOOK AT AN HTTP GET (2).

Again, suppose a client is sending an HTTP GET request message to a web server, gaia.cs.umass.edu. The client-to-server HTTP GET message is the following (same as in previous problem):

GET /kurose_ross_sandbox/interactive/quotation2.htm HTTP/1.1
Host: gaia.cs.umass.edu
Accept: text/plain, text/html, text/xml, image/jpeg, image/gif, audio/mpeg, audio/mp4, video/wmv, video/mp4,
Accept-Language: en-us, en-gb;q=0.1, en;q=0.7, fr, fr-ch, da, de, fi
If-Modified-Since: Wed, 09 Sep 2020 16:06:01 -0700
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.56 Safari/535.11

What is the language in which the client would least prefer to get a response? [You may have to search around the Web a bit to answer this.]

[Note: you can find additional questions similar to this here.]

- US English
- Spanish
- Hindi

- United Kingdom English
- French
- Mandarin
- Finnish
- Farsi

A DETAILED LOOK AT AN HTTP GET (3).

Again, suppose a client is sending an HTTP GET request message to a web server, gaia.cs.umass.edu. Suppose the client-to-server HTTP GET message is the following (same as in previous problem):

GET /kurose_ross_sandbox/interactive/quotation2.htm HTTP/1.1
Host: gaia.cs.umass.edu
Accept: text/plain, text/html, text/xml, image/jpeg, image/gif, audio/mpeg, audio/mp4, video/wmv, video/mp4,
Accept-Language: en-us, en-gb;q=0.1, en;q=0.7, fr, fr-ch, da, de, fi
If-Modified-Since: Wed, 09 Sep 2020 16:06:01 -0700
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.56 Safari/535.11

Does the client have a cached copy of the object being requested?

[Note: you can find additional questions similar to this here.]

- Yes, because HTTP 1.1 is being used.
- There's not enough information in the header to answer this question.
- No, because a client would not request an object if it had that object in its cache.
- Yes, because this is a conditional GET, as evidenced by the If-Modified-Since field.

A DETAILED LOOK AT AN HTTP REPLY.

Suppose now the server sends the following HTTP response message the client:

HTTP/1.0 200 OK
Date: Wed, 09 Sep 2020 23:46:21 +0000
Server: Apache/2.2.3 (CentOS)
Last-Modified: Wed, 09 Sep 2020 23:51:41 +0000
ETag:17dc6-a5c-bf716880.
Content-Length: 418
Connection: Close
Content-type: image/html

Will the web server close the TCP connection after sending this message?

[Note: you can find more questions like this one here.]

○ Yes, because the HTTP response indicated that only one object was requested in the HTTP GET request.

○ There's not enough information in the response message to answer this question.

○ No, the server will leave the connection open as a persistent HTTP connection.

○ Yes, the server will close this connection because version 1.0 of HTTP is being used, and TCP connections do not stay open persistently.

WHY WEB CACHING?

Which of the following are advantages of using a web cache? Sselect one or more answers.

☑ Caching generally provides for a faster page load time at the client, if the web cache is in the client's institutional network, because the page is loaded from the nearby cache rather than from the distant server.
☑ Caching uses less bandwidth coming into an institutional network where the client is located, if the cache is also located in that institutional network.
☐ Caching allows an origin server to more carefully track which clients are requesting and receiving which web objects.
☐ Overall, caching requires fewer devices/hosts to satisfy a web request, thus saving on server/cache costs

---

HTTP/2 VERSUS HTTP/1.1.

Which of the following are changes between HTTP 1.1 and HTTP/2? Note: select one or more answers.

☑ HTTP/2 allows a large object to be broken down into smaller pieces, and the transmission of those pieces to be interleaved with transmission other smaller objects, thus preventing a large object from forcing many smaller objects to wait their turn for transmission.
☑ HTTP/2 allows objects in a persistent connection to be sent in a client-specified priority order.
☐ HTTP/2 has many new HTTP methods and status codes.
☐ HTTP/2 provides enhanced security by using transport layer security (TLS).

WHAT'S IN AN HTTP REPLY?

Which of the following pieces of information will appear in a server's application-level HTTP reply message? (Check all that apply.)

☑ A response phrase associated with a response code
☑ A response code
☐ A sequence number
☐ The server's IP address
☐ A checksum
☐ The name of the Web server (e.g., gaia.cs.umass.edu)

IF-MODIFIED-SINCE.

What is the purpose of the *If-Modified-Since* field in a HTTP GET request message

- To inform the HTTP cache that it (the cache) should retrieve the full object from the server, and then cache it until the specified time.
- (selected) To indicate to the server that the client has cached this object from a previous GET, and the time it was cached.
- To allow the server to indicate to the client that it (the client) should cache this object.
- To indicate to the server that the client wishes to receive this object, and the time until which it will cache the returned object in the browser's cache.
- To indicate to the server that the server should replace this named object with the new version of the object attached to the GET, if the object has not been modified since the specified time

---

COOKIES.

What is the purpose of a cookie value in the HTTP GET request?

- The cookie value indicates whether the user wants to use HTTP/1, HTTP/1.1, or HTTP/2 for this GET request.
- The cookie value encodes a default set of preferences that the user has previously specified for this web site.
- The cookie value is an encoding of a user email address associated with the GET request.
- (selected) The cookie value itself doesn't mean anything. It is just a value that was returned by a web server to this client during an earlier interaction.
- The cookie value encodes the format of the reply preferred by the client in the response to this GET reques

---

HTTP GET (EVEN MORE).

Suppose a client is sending an HTTP GET message to a web server, gaia.cs.umass.edu. Suppose the client-to-server HTTP GET message is the following:

GET /kurose_ross_sandbox/interactive/quotation2.htm HTTP/1.1
Host: gaia.cs.umass.edu
Accept: text/plain, text/html, text/xml, image/jpeg, image/gif, audio/mpeg, audio/mp4, video/wmv, video/mp4,
Accept-Language: en-us, en-gb;q=0.1, en;q=0.7, fr, fr-ch, da, de, fi
If-Modified-Since: Wed, 09 Sep 2020 16:06:01 -0700
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.56 Safari/535.11

Does the client have a cached copy of the object being requested?

- No, because the client would not request an object if it were cached.
- (selected) Yes, because this is a conditional GET.
- There’s not enough information to answer this question.

WHAT HAPPENS AFTER AN HTTP REPLY?

Suppose an HTTP server sends the following HTTP response message a client:

HTTP/1.0 200 OK
Date: Wed, 09 Sep 2020 23:46:21 +0000
Server: Apache/2.2.3 (CentOS)
Last-Modified: Wed, 09 Sep 2020 23:51:41 +0000
ETag:17dc6-a5c-bf716880.
Content-Length: 418
Connection: Close
Content-type: image/html

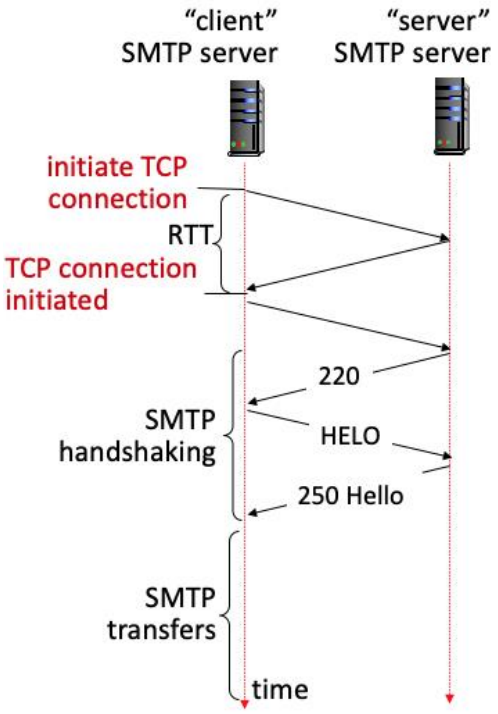
Will the web server close the TCP connection after sending this message?

- There's not enough information to answer this question.
- Yes, because this is HTTP 1.0
- No, this is a persistent connection, and so the server will keep the TCP connection open.

3.Email

E-MAIL DELAYS.

How many RTTs are there from when a client first contacts an email server (by initiating a TCP session) to when the client can begin sending the email message itself – that is following all initial TCP or SMTP handshaking required?
Recall the figure below from our class notes:



- 2.5
- 2
- 0
- 1
- 3 3 is answer

SLIDE chương 2 trang 57

COMPARING AND CONTRASTING HTTP AND SMTP.

Which of the following characteristics apply to HTTP only (and do *not* apply to SMTP)? Note: check one or more of the characteristics below.

- [x] Uses server port 80.
- [ ] Uses server port 25.
- [ ] Operates mostly as a “client push” protocol.
- [ ] Has ASCII command/response interaction, status codes.
- [ ] Is able to use a persistent TCP connection to transfer multiple objects.
- [ ] Uses CRLF.CRLF to indicate end of message.
- [x] Operates mostly as a “client pull” protocol.
- [x] Uses a blank line (CRLF) to indicate end of request header.

COMPARING AND CONTRASTING HTTP AND SMTP (2).

Which of the following characteristics apply to SMTP only (and do *not* apply to HTTP)? Note: check one or more of the characteristics below.

- [x] Uses server port 25.
- [x] Uses CRLF.CRLF to indicate end of message.
- [x] Operates mostly as a “client push” protocol.
- [ ] Operates mostly as a “client pull” protocol.
- [ ] Uses a blank line (CRLF) to indicate end of request header.
- [ ] Has ASCII command/response interaction, status codes.
- [ ] Is able to use a persistent TCP connection to transfer multiple objects.
- [ ] Uses server port 80.

COMPARING AND CONTRASTING HTTP AND SMTP (3).

Which of the following characteristics apply to both HTTP and SMTP? Note: check one or more of the characteristics below.

- [ ] Uses a blank line (CRLF) to indicate end of request header.
- [ ] Operates mostly as a “client pull” protocol.
- [x] Is able to use a persistent TCP connection to transfer multiple objects.
- [ ] Uses CRLF.CRLF to indicate end of message.
- [ ] Operates mostly as a “client push” protocol.
- [x] Has ASCII command/response interaction, status codes.

WHICH E-MAIL PROTOCOL?

Match the functionality of a protocol with the name of a the email protocol (if any) that implements that functionality.

QUESTION LIST:

Pushes email from a mail client to a mail server.

C

Pulls mail from one mail server to another mail server.

A

Pulls email to a mail client from a mail server.

B

ANSWER LIST:

A. Neither SMTP nor IMAP does this.
B. IMAP
C. SMTP

4.The Domain Name Service: DNS

DNS FUNCTIONS.

Match the function of a server to a given type of DNS server in the DNS server hierarchy.

QUESTION LIST:

Provides authoritative hostname to IP mappings for organization's named hosts.

D

Replies to DNS query by local host, by contacting other DNS servers to answer the query.

A

Responsible for a domain (e.g., *.com, *.edu); knows how to contact authoritative name servers.

C

Highest level of the DNS hierarchy, knows how to reach servers responsible for a given domain (e.g., *.com, *.edu).

B

ANSWER LIST:

A. Local DNS server
B. DNS root servers
C. Top Level Domain (TLD) servers
D. Authoritative DNS server

WHY DOES THE DNS PERFORM CACHING?

What is the value of caching in the local DNS name server? Check all that apply.

- [ ] DNS caching provides prioritized access to the root servers, since the DNS request is from a local DNS cache.
- [x] DNS caching provides for faster replies, if the reply to the query is found in the cache.
- [ ] DNS caching provides the ability to serve as authoritative name server for multiple organizations.
- [x] DNS caching results in less load elsewhere in DNS, when the reply to a query is found in the local cache.

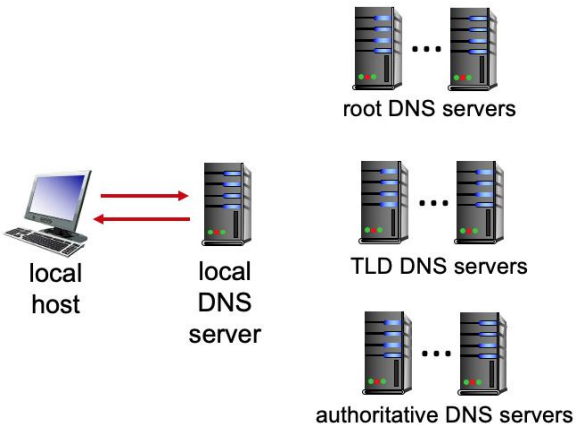
WHAT'S IN THE DNS TYPE A RESOURCE RECORD?

What information does the type “A” resource record hold in the DNS database? Check all that apply.

- [ ] A domain name and the name of the authoritative name server for that domain.
- [ ] An alias name and a true name for a server.
- [x] A hostname and an IP address.
- [ ] A name and the name of the SMTP server associated with that name.

DNS IN ACTION (1).

Suppose that the local DNS server caches all information coming in from all root, TLD, and authoritative DNS servers for 20 time units. (Thus, for example, when a root server returns the name and address of a TLD server for .com, the cache remembers that this is the TLD server to use to resolve a .com name). Assume also that the local cache is initially empty, that iterative DNS queries are always used, that DNS requests are just for name-to-IP-address translation, that 1 time unit is needed for each server-to-server or host-to-server (one way) request or response, and that there is only one authoritative name server (each) for any .edu or .com domain.



Consider the following DNS requests, made by the local host at the given times:

- *t=0,* the local host requests that the name gaia.cs.umass.edu be resolved to an IP address.
- *t=1,* the local host requests that the name icann.org be resolved to an IP address.

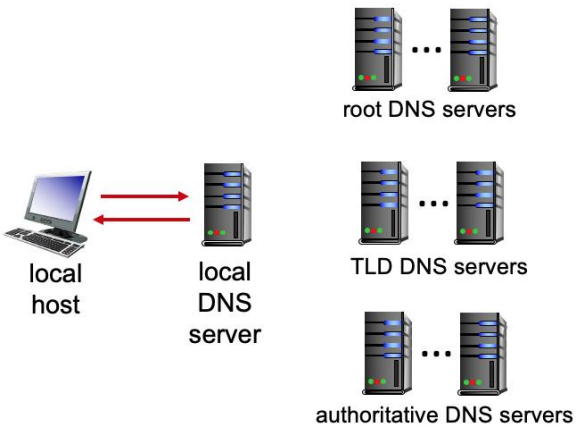
- *t=5,* the local host requests that the name cs.umd.edu be resolved to an IP address. (Hint: be careful!)
- *t=10,* the local host *again* requests that the name gaia.cs.umass.edu be resolved to an IP address.
- *t=12*, the local host requests that the name cs.mit.edu be resolved to an IP address.
- *t=30,* the local host *again* requests that the name gaia.cs.umass.edu be resolved to an IP address. (Hint: be careful!)

Which of the requests require 8 time units to be resolved?

- [ ] The request at *t=10*.
- [x] The request at *t=1*.
- [x] The request at *t=30*.
- [ ] The request at *t=5*.
- [x] The request at *t=0*.
- [ ] The request at *t=12*.

DNS IN ACTION (2).

[This question is the same as an earlier question, except for the question statement at the very end.] Suppose that the local DNS server caches all information coming in from all root, TLD, and authoritative DNS servers for 20 time units. (Thus, for example, when a root server returns the name and address of a TLD server for .com, the cache remembers that this is the TLD server to use to resolve a .com name). Assume also that the local cache is initially empty, that iterative DNS queries are always used, that DNS requests are just for name-to-IP-address translation, that 1 time unit is needed for each server-to-server or host-to-server (one way) request or response, and that there is only one authoritative name server (each) for any .edu or .com domain.



Consider the following DNS requests, made by the local host at the given times:

- *t=0,* the local host requests that the name gaia.cs.umass.edu be resolved to an IP address.
- *t=1,* the local host requests that the name icann.org be resolved to an IP address.
- *t=5,* the local host requests that the name cs.umd.edu be resolved to an IP address. (Hint: be careful!)
- *t=10,* the local host *again* requests that the name gaia.cs.umass.edu be resolved to an IP address.
- *t=12*, the local host requests that the name cs.mit.edu be resolved to an IP address.
- *t=30,* the local host *again* requests that the name gaia.cs.umass.edu be resolved to an IP address. (Hint: be careful!)

Which of the requests require 6 time units to be resolved?

- [x] The request at *t=5*.
- [x] The request at *t=12*.
- [ ] The request at *t=30*.
- [ ] The request at *t=0*.
- [ ] The request at *t=10*.
- [ ] The request at *t=1*.

THE LOCAL DNS SERVER.

Check all of the phrases below that state a true property of a *local* DNS server.

- [x] The local DNS server can decrease the name-to-IP-address resolution time experienced by a querying local host over the case when a DNS is resolved via querying into the DNS hierarchy.
- [ ] The local DNS server holds hostname-to-IP translation records, but not other DNS records such as MX records.
- [x] The local DNS server record for a remote host is sometimes different from that of the authoritative server for that host.
- [ ] The local DNS server is only contacted by a local host if that local host is unable to resolve a name via iterative or recursive queries into the DNS hierarchy.

THE DNS AUTHORITATIVE NAME SERVER.

What is the role of an authoritative name server in the DNS? (Check all that apply)

- [ ] It is a local (to the querying host) server that caches name-to-IP address translation pairs, so it can answer authoritatively and can do so quickly.
- [x] It provides the definitive answer to the query with respect to a name in the authoritative name server's domain.
- [ ] It provides the IP address of the DNS server that can provide the definitive answer to the query.
- [ ] It provides a list of TLD servers that can be queried to find the IP address of the DNS server that can provide the definitive answer to this query.

DNS AND HTTP CACHING.

We learned that in HTTP web browser caching, HTTP local web server caching, and in local DNS caching, that a user benefits (e.g., shorter delays over the case of no caching) from finding a local/nearby copy of a requested item. In which of the following forms of caching does a user benefit from its not only from its own recent requests (and cached replies) *but also from recent requests made from other users*?

- [x] HTTP local web caching
- [ ] HTTP browser caching
- [x] Local DNS server caching

6.Video Streaming and Content Distribution Networks

.6-4

Manifest file. What is the purpose of a *manifest file* in a streaming multimedia setting?

- To let a OTT (Over-the-top) video server know the video that the client wants to view.
- To allow a client to reserve bandwidth along a path from a server to that client, so the client can view a stream video without impairment.
- Allows a video service to log the video and the server from which a client streams a video.
- To let a client know where it can retrieve different video segments, encoded at different rates

---

CDNS.

What approach is taken by a CDN to stream content to hundreds of thousands of simultaneous users?

- Proactively push videos to a client device before they're requested, using machine learning to predict requested videos.
- Store/serve multiple copies of videos at multiple geographically distributed sites.
- Serve video from a single central "mega-server" with ultra-high-speed network connectivity, and high-speed storage.
- Allow client devices to send requested content to each other, in order to offload the CDN infrastructure.

SILDE CHƯƠNG 2 TRANG 101

STREAMING VIDEO DEFINITIONS.

Match the definition/function of an element or approach in a networked streaming video system, with its name.

QUESTION LIST:

A unit of video, each of which may be encoded at multiple different rates, stored in different files.

A

A file containing the location and encoding rate of files corresponding to video segments in a video.

C

An approach that allows a client to adapt the encoding rate of retrieved video to network congestion conditions.

F

A CDN approach that stores content in access networks, close to clients.

B

ANSWER LIST:

A. **Chunk**(là một đoạn thông tin được sử dụng nhiều ở định dạng tệp đa phương tiện, chẳng hạn như PNG,IFF,MP3, ... Mỗi đoạn chưa một tiêu đề cho biết một tahm số. Theo sau phần đầu là một vùng biến dữ liệu, được chương trình giải mã từ các tham số trong phần đầu https://en.wikipedia.org/wiki/Chunk_(information))
B. **Enter deep**
C. **Manifest (rõ ràng?)**
D. **Video frame**
E. **Over The Top (OTT)**
F. **DASH**

WHAT IS DASH?

In DASH (Dynamic, Adaptive Streaming over HTTP), a server divides a video file into chunks that ... (pick best completion from below)

○ ... are downloaded just before their playout time. Chunking is used primarily because a viewer may jump around (e.g., fast forward) in a video.
○ ... allow premium users to avoid watching chunks that contain commercials.
○ ... are stored, each encoded at multiple rates (video quality). The client receives multiple video chunks (encoded at different rates) and plays out the chunks that best fit the screen size.
○ ... are download smallest-chunk-first in order to maximize the number of chunks received.
○ ... are stored, each encoded at multiple rates (video quality). The client plays the video chunk-by-chunk, with each chunk requested at encoding rate that fits the available bandwidth at the time.

7.Socket Programming: Creating Network Applications

UDP SOCKETS.

Which of the following characteristics below are associated with a UDP socket? Check one or more that apply.

☑ provides unreliable transfer of a groups of bytes (“a datagram”), from client to server
☑ the application must explicitly specify the IP destination address and port number for each group of bytes written into a socket

- [ ] provides reliable, in-order byte-stream transfer (a “pipe”), from client to server
- [x] data from different clients can be received on the same socket
- [ ] when contacted, the server will create a new server-side socket to communicate with that client
- [ ] socket(AF_INET, SOCK_STREAM) creates this type of socket
- [x] socket(AF_INET, SOCK_DGRAM) creates this type of socket
- [ ] a server can perform an accept() on this type of socket.

TCP SOCKETS.

Which of the following characteristics below are associated with a TCP socket? Check one or more that apply.

- [ ] data from different clients can be received on the same socket
- [x] socket(AF_INET, SOCK_STREAM) creates this type of socket
- [x] when contacted, the server will create a new server-side socket to communicate with that client
- [ ] socket(AF_INET, SOCK_DGRAM) creates this type of socket
- [ ] provides unreliable transfer of a group of bytes (a “datagram”), from client to server
- [x] provides reliable, in-order byte-stream transfer (a “pipe”), from client to server
- [ ] the application must explicitly specify the IP destination address and port number for each group of bytes written into a socket
- [x] a server can perform an accept() on this type of socket

---

SERVER REPLY (UDP).

How does the networked application running on a server know the client IP address and the port number to reply to in response to a received datagram?

- ○ The server will query the DNS to learn the IP address of the client.
- ○ As the result of performing the accept() statement, the server has created a new socket that is bound to that specific client, and so sending into this new socket (without explicitly specifying the client IP address and port number) is sufficient to ensure that the sent data will be addressed to the correct client.
- ○ The application code at the server determines client IP address and port # from the initial segment sent by client, and must explicitly specify these values when sending into a socket back to that client.
- ○ The server will know the port number being used by the client since all services have a well-known port number.

BOUNS CHAPTER 2

Manifest file. What is the purpose of a *manifest file* in a streaming multimedia setting?
AS: To let a client know where it can retrieve different video segments, encoded at different rates

CHAPTER 3: TRANSPORT LAYER

1. **Introduction and Transport-layer Services**

LOCATION OF TRANSPORT-LAYER FUNCTIONALITY.

Where is transport-layer functionality primarily implemented?

- Transport layer functions are implemented primarily at the hosts at the “edge” of the network.
- Transport layer functions are implemented primarily at the routers and switches in the network.
- Transport layer functions are implemented primarily at each end of a physical link connecting one host/router/switch to another one host/router/switch.

TRANSPORT-LAYER FUNCTIONALITY.

True or False: The transport layer provides for host-to-host delivery service?

- True.
- False

TRANSPORT LAYER SERVICES USING TCP.

Check all of the services below that are provided by the TCP protocol.

- [ ] A guarantee on the maximum amount of time needed to deliver data from sender to receiver.
- [x] In-order data delivery
- [x] A congestion control service to ensure that multiple senders do not overload network links.
- [x] A byte stream abstraction, that does not preserve boundaries between message data sent in different socket send calls at the sender.
- [ ] A message abstraction, that preserves boundaries between message data sent in different socket send calls at the sender.
- [x] A flow-control service that ensures that a sender will not send at such a high rate so as to overflow receiving host buffers.
- [ ] A guarantee on the *minimum* amount of throughput that will be provided between sender and receiver.
- [x] Reliable data delivery.

TRANSPORT-LAYER SERVICES USING UDP.

Check all of the services below that are provided by the UDP protocol.

- [ ] In-order data delivery
- [x] A message abstraction, that preserves boundaries between message data sent in different socket send calls at the sender.
- [ ] A congestion control service to ensure that multiple senders do not overload network links.
- [ ] Reliable data delivery.
- [ ] A byte stream abstraction, that does not preserve boundaries between message data sent in different socket send calls at the sender.
- [ ] A guarantee on the maximum amount of time needed to deliver data from sender to receiver.
- [ ] A guarantee on the *minimum* amount of throughput that will be provided between sender and receiver.
- [ ] A flow-control service that ensures that a sender will not send at such a high rate so as to overflow receiving host buffers

NETWORK-LAYER FUNCTIONALITY.

The transport layer sits on top of the network layer, and provides its services using the services provided to it by the network layer. Thus it's important that we know what is meant by the network layer's "best effort" delivery service. True or False:

> *The network layer's best-effort delivery service means that IP makes its "best effort" to deliver segments between communicating hosts, but it makes no guarantees. In particular, it does not guarantee segment delivery, it does not guarantee orderly delivery of segments, and it does not guarantee the integrity of the data in the segments.*

- ○ Correct! The network layer's best effort service doesn't really provide much service at all, does it?
- ○ Nope. The network layer's best effort service doesn't really provide much service at all, does it?

2. **Multiplexing and Demultiplexing**

TRANSPORT-LAYER DEMULTIPLEXING.

What is meant by transport-layer demultiplexing?

- Taking data from multiple sockets, all associated with the same destination IP address, adding destination port numbers to each piece of data, and then concatenating these to form a transport-layer segment, and eventually passing this segment to the network layer.
- Receiving a transport-layer segment from the network layer, extracting the payload, determining the destination IP address for the data, and then passing the segment and the IP address back down to the network layer.
- Receiving a transport-layer segment from the network layer, extracting the payload (data) and delivering the data to the correct socket.
- Taking data from one socket (one of possibly many sockets), encapsulating a data chuck with header information – thereby creating a transport layer segment – and eventually passing this segment to the network layer.

TRANSPORT-LAYER MULTIPLEXING.

What is meant by transport-layer multiplexing?

- Taking data from multiple sockets, all associated with the same destination IP address, adding destination port numbers to each piece of data, and then concatenating these to form a transport-layer segment, and eventually passing this segment to the network layer.
- Taking data from one socket (one of possibly many sockets), encapsulating a data chuck with header information – thereby creating a transport layer segment – and eventually passing this segment to the network layer.
- Receiving a transport-layer segment from the network layer, extracting the payload, determining the destination IP address for the data, and then passing the segment and the IP address back down to the network layer.
- Receiving a transport-layer segment from the network layer, extracting the payload (data) and delivering the data to the correct socket.

MULTIPLEXING/DEMULTIPLEXING: UDP PORT NUMBERS.

True or False: When multiple UDP clients send UDP segments to the same destination port number at a receiving host, those segments (from different senders) will always be directed to the same socket at the receiving host.

- True
- False

MULTIPLEXING/DEMULTIPLEXING: TCP PORT NUMBERS.

True or False: When multiple TCP clients send TCP segments to the same destination port number at a receiving host, those segments (from different senders) will always be directed to the same socket at the receiving host.

- False
- True

MULTIPLEXING UDP WITH IDENTICAL PORT NUMBERS.

True or False: It is possible for two UDP segments to be sent from the same socket with source port 5723 at a server to two different clients.

- False
- True

MULTIPLEXING TCP WITH IDENTICAL PORT NUMBERS.

True or False: It is possible for two TCP segments with source port 80 to be sent by the sending host to different clients.

- True
- False

3. **Connectionless Transport: UDP**

DOES UDP PRESERVE APPLICATION-LAYER MESSAGE BOUNDARIES?

True or False: On the sending side, the UDP sender will take each application-layer chunk of data written into a UDP socket and send it in a distinct UDP datagram. And then on the receiving side, UDP will deliver a segment's payload into the appropriate socket, preserving the application-defined message boundary.

- ○ True
- ○ False

UDP HEADER FIELDS.

Which of the fields below are in a UDP segment header? *[Hint: note the use of the word "header" in this question statement.]*

- ☑ Source port number
- ☑ Destination port number
- ☐ Upper layer protocol
- ☐ Source IP address
- ☐ Sequence number
- ☑ Internet checksum
- ☑ Length (of UDP header plus payload)
- ☐ Data (payload)

UDP SEGMENT LENGTH FIELD.

Why is the UDP header length field needed?

- ○ To make the header and even number of bytes
- ○ Because the payload section can be of variable length, and this lets UDP know where the segment ends.
- ○ Because this field is needed in TCP as well.
- ○ (a) and (b) above

INTERNET CHECKSUM AND UDP.

Over what set of bytes is the checksum field in the UDP header computed over?

- ◉ The entire UDP segment, except the checksum field itself, and the IP sender and receive address fields
- ○ Just the UDP header but not the payload.
- ○ The entire UDP segment, except the checksum field itself.

WHAT IS A CHECKSUM?

Which of the following statements are true about a checksum? Hint: more than one statement is true.

- [x] The receiver of a packet with a checksum field will add up the received bytes, just as the sender did, and compare this locally-computed checksum with the checksum value in the packet header. If these two values are *different* then the receiver*knows* that one of the bits in the received packet has been changed during transmission from sender to receiver.
- [ ] The receiver of a packet with a checksum will add up the received bytes, just as the sender did, and compare this locally-computed checksum with the checksum value in the packet header. If these two values are the *same* then the receiver *knows*that all of the bits in the received packet are correct, i.e., that no bits have been changed during transmission from sender to receiver.
- [x] The sender-computed checksum value is often included in a checksum field within a packet header.
- [x] A checksum is computed at a sender by considering each byte within a packet as a number, and then adding these numbers (each number representing a bytes) together to compute a sum (which is known as a checksum).

COMPUTING THE INTERNET CHECKSUM (1).

Compute the Internet checksum value for these two 16-bit words: 11110101 11010011 and 10110011 01000100

[Note: you can find more problems like this one here.]

- ○ 01010110 11101000
- ○ 01101110 11010101
- ○ 01010110 11100111
- ○ 01011110 11000101

COMPUTING THE INTERNET CHECKSUM (2).

Compute the Internet checksum value for these two 16-bit words: 01000001 11000100 and 00100000 00101011

[Note: you can find more problems like this one here.]

- ○ 10011110 00001111
- ○ 10011110 00010000
- ○ 10011110 00010001
- ○ 01101110 11010101

UDP CHECKSUM: HOW GOOD IS IT?

True or False: When computing the Internet checksum for two numbers, a single flipped bit (i.e., in just one of the two numbers) will always result in a changed checksum.

- ○ False

- True

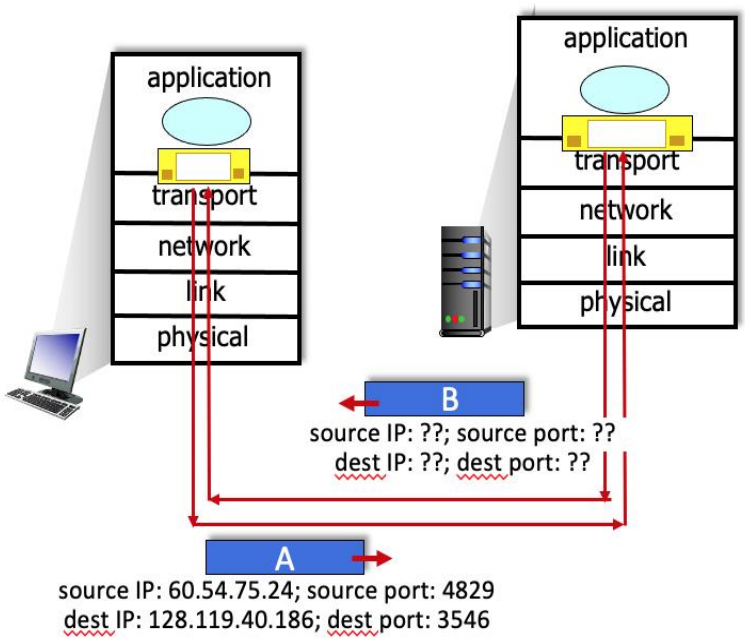
UDP CHECKSUM: HOW GOOD IS IT?

True or False: When computing the Internet checksum for two numbers, a single flipped bit in each of the two numbers will always result in a changed checksum.

- False
- True

IP ADDRESSES AND PORT NUMBERS IN A UDP SEGMENT SENT IN REPLY.

Suppose a UDP segment (A in the figure below) arrives at a host with an IP address of 128.119.40.186. The source port in the UDP segment is 4829 and the destination port is 3546. The IP address of the sending host is 60.54.75.24.



Now consider the UDP datagram (and the IP datagram that will encapsulate it) sent in reply by the application on host 128.119.40.186 to the original sender host, labeled B in the figure above. Complete the sentences below ...

What are the source and destination port numbers and IP addresses? (Enter the integer port number or the 4-part dotted decimal IP address, included the period)

The source port number of the UDP segment (B) sent in reply is:

The source IP address of the IP datagram containing the UDP segment (B) sent in reply is:

The destination port number of the UDP segment (B) sent in reply is:

The destination IP address of the IP datagram containing the UDP segment (B) sent in reply is:

[Note: you can find more problems like this one here.]

QUESTION LIST:

The source port number of the UDP segment (B) sent in reply is:

C

The source IP address of the IP datagram containing the UDP segment (B) sent in reply is:

G

The destination port number of the UDP segment (B) sent in reply is:

E

The destination IP address of the IP datagram containing the UDP segment (B) sent in reply is:

F

ANSWER LIST:

A. 10.0.0.1
B. 80
C. 3546
D. 24
E. 4829
F. 60.54.75.24
G. 128.119.40.186

4. **Principles of Reliable Data Transfer**

RELIABLE DATA TRANSFER PROTOCOL MECHANISMS.

Consider the purposes/goals/use of different reliable data transfer protocol mechanisms. For the given purpose/goal/use match it to the RDT mechanism that is used to implement the given purpose/goal/use.

QUESTION LIST:

Lets the sender know that a packet was NOT received correctly at the receiver.

A

Used by sender or receiver to detect bits flipped during a packet's transmission.

E

Allows for duplicate detection at receiver.

D

Lets the sender know that a packet was received correctly at the receiver.

C

Allows the receiver to eventually receive a packet that was corrupted or lost in an earlier transmission.

B

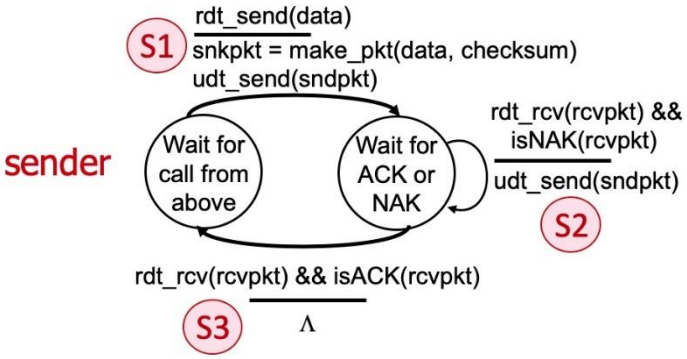
ANSWER LIST:

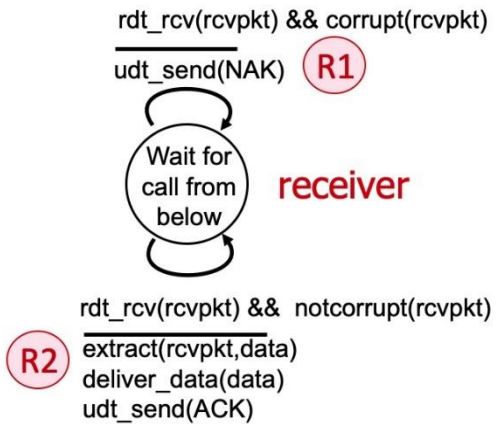
A. NAK
B. Retransmission
C. ACK
D. Sequence numbers
E. Checksum

THE RDT 2.0 PROTOCOL.

Consider the rdt 2.0 sender and receiver shown below, with FSM transitions at the sender labeled S1, S2, and S3; and receiver transitions labeled R1 and R2.

Which of the following sequences of transitions could possibly occur as a result of an initial rdt_send() call at the sender, and possible later message corruption and subsequent error recovery.

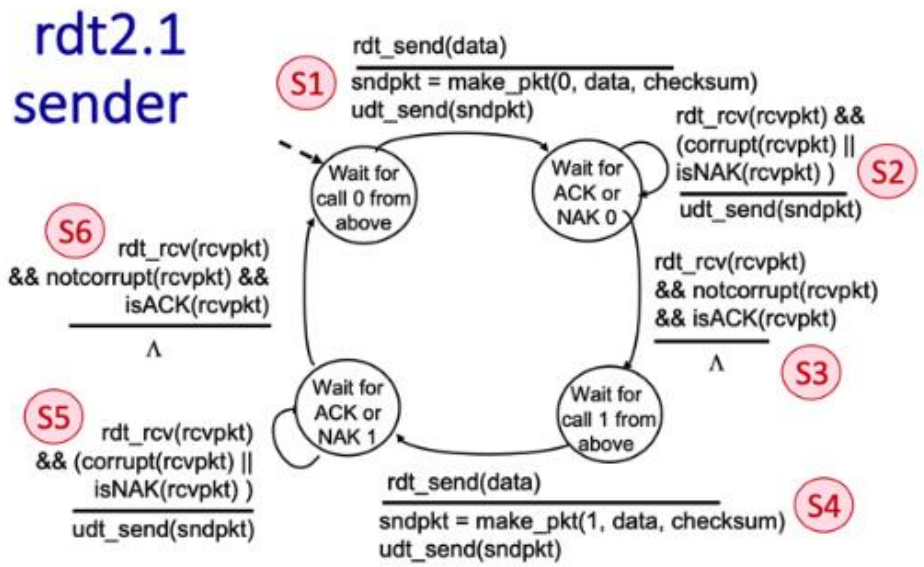


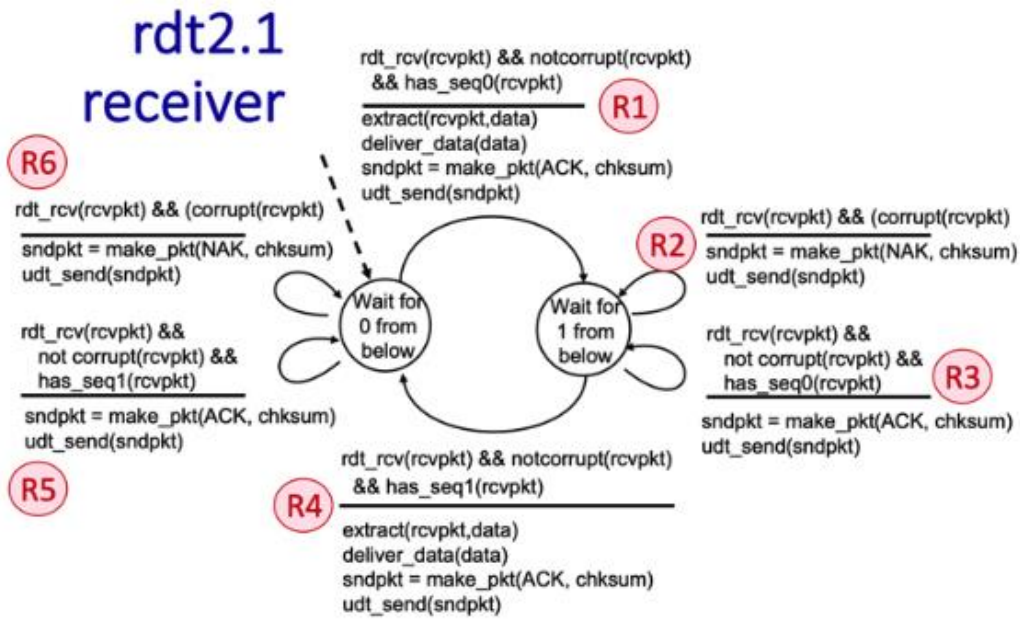


- [ ] S1, R1, S2, R1, S3
- [x] S1, R2, S3
- [ ] S1, R2, S2
- [x] S1, R1, S2, R2,S3
- [ ] S1, S2, S3
- [x] S1, R1, S2
- [ ] S1, R1, S3

THE RDT 2.1 PROTOCOL (A).

Consider the rdt2.1 sender and receiver FSMs shown below, with labeled transitions S1 through S6 at the sender, and transitions R1 through R6 at the receiver. The sender and receiver start in the “Wait for call 0 from above” and “Wait for 0 from below” states, respectively.





Suppose that no channel errors occur. A sequence of interleaved sender and receiver transitions is given below. Transitions S1 and S4 are already provided. Choose the sender or receiver transition for the unlabeled transitions x_1, x_2, x_3, and x_4 below to indicate the time-ordered sequence of transitions (interleaved sender and receiver transitions) that will result in two

messages being delivered at the receiver, with the sender and receiver returning to their initial states (again, given that no channel errors occur).

S1, x_1, x_2, S4, x_3, x_4

QUESTION LIST:

transition x_1

B

transition x_2

D

transition x_3

E

transition x_4

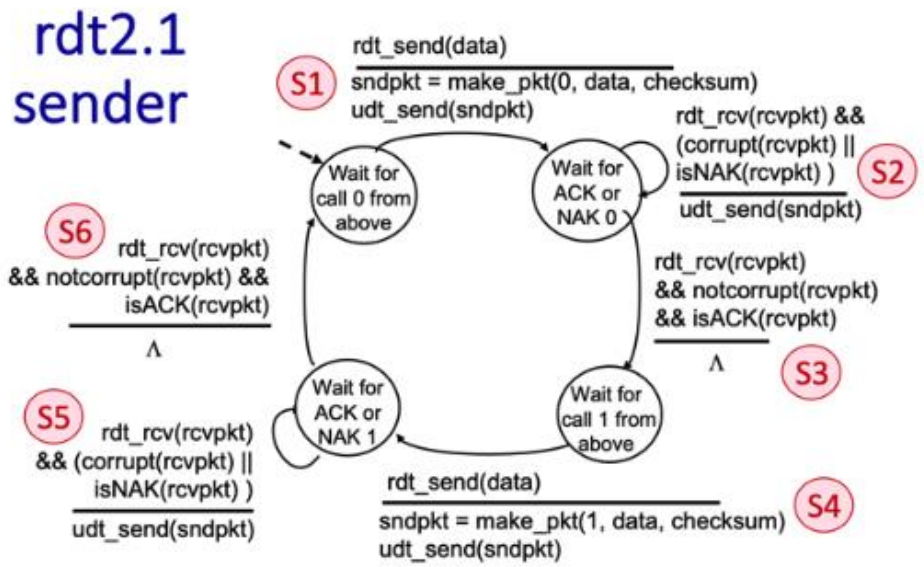
C

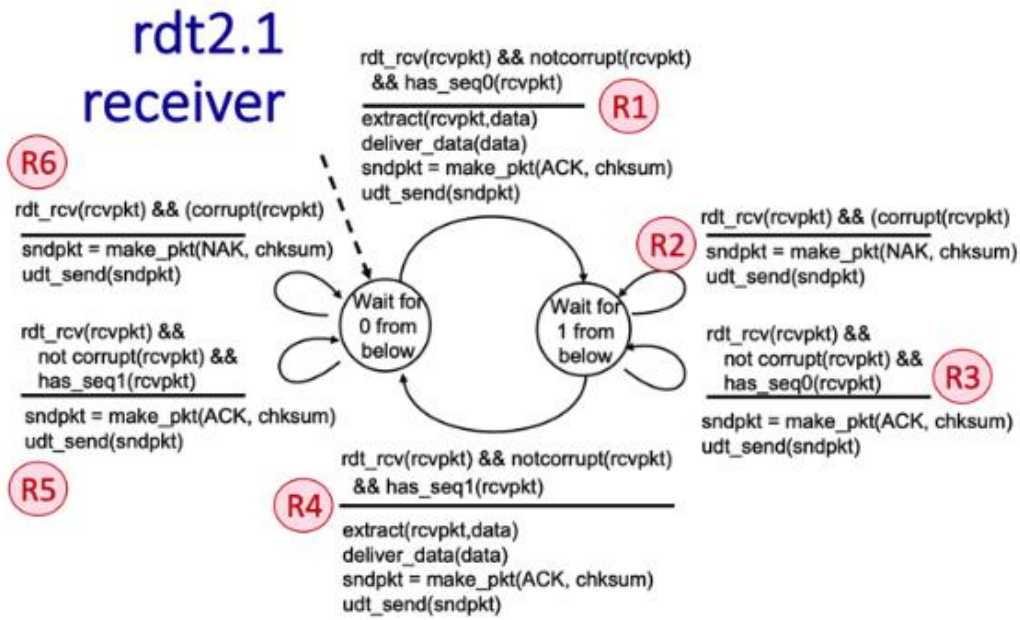
ANSWER LIST:

A. R3
B. R1
C. S6
D. S3
E. R4
F. S2

THE RDT 2.1 PROTOCOL (B).

Consider the rdt2.1 sender and receiver FSMs shown below, with labeled transitions S1 through S6 at the sender, and transitions R1 through R6 at the receiver. The sender and receiver start in the “Wait for call 0 from above” and “Wait for 0 from below” states, respectively.





Suppose that the initial message transmission by the sender is corrupted, but that no other message transmissions are corrupted. Match the unlabeled transitions x_1, x_2, x_3, x_4, x_5 in the time-ordered sequence of transitions below (interleaved sender and receiver transitions) that will occur following the initial S1 transition (which is corrupted), that will result in two messages being delivered at the receiver, with the sender and receiver returning to their initial states (again, given that the initial

message transmission by the sender is corrupted). Note that transitions S1, S4, and S6 are already provided below.

S1 (message corrupted), x_1, x_2, x_3, x_4, S4, x_5, S6.

QUESTION LIST:

transition x_1

B

transition x_2

F

transition x_3

C

transition x_4

A

transition x_5

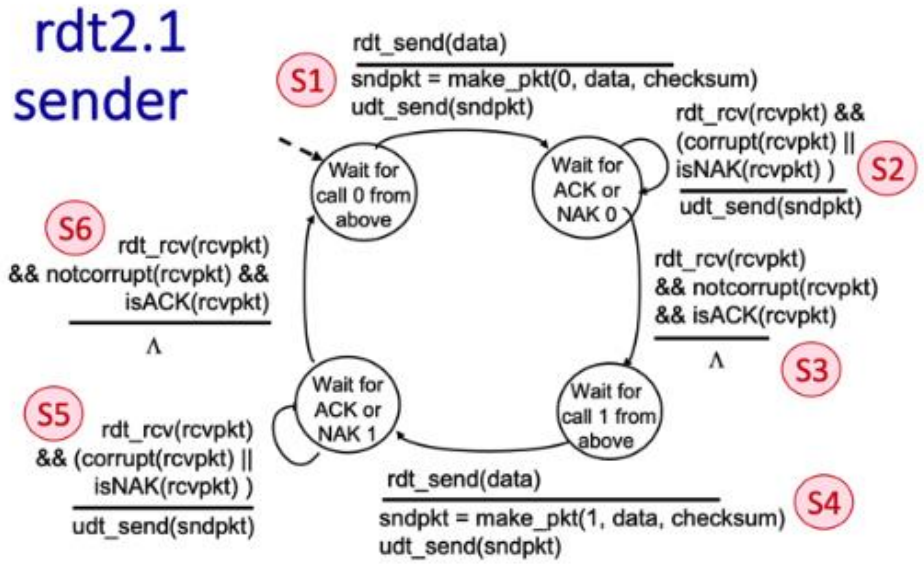
E

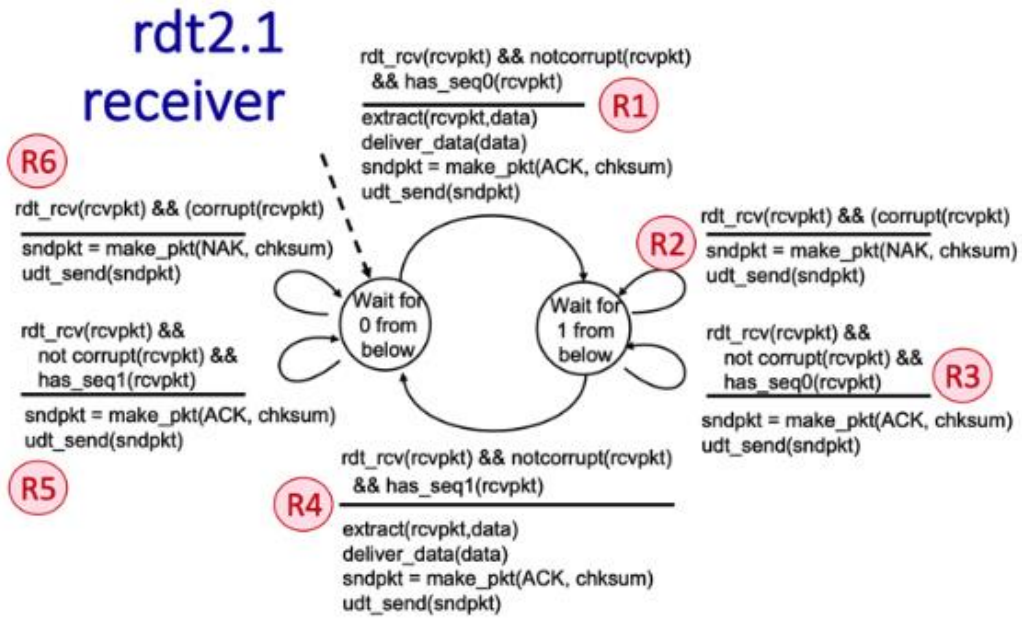
ANSWER LIST:

A. S3
B. R6
C. R1
D. S4
E. R4
F. S2
G. R3

THE RDT 2.1 PROTOCOL (C).

Consider the rdt2.1 sender and receiver FSMs shown below, with labeled transitions S1 through S6 at the sender, and transitions R1 through R6 at the receiver. The sender and receiver start in the “Wait for call 0 from above” and “Wait for 0 from below” states, respectively.





Suppose that the first packet from the sender is correctly received at the receiver but that ACK message sent from receiver-to-sender is corrupted; all other

messages (before or after that ACK) are transmitted error-free. Match the unlabeled transitions x_1, x_2, x_3, x_4, x_5 in the time-ordered sequence of transitions below (interleaved sender and receiver transitions) that will occur following the initial S1 transition, which is followed by a corrupted ACK transmission, that will result in a message being delivered at the receiver, with the sender and receiver returning to their initial states. Note that some transitions are already provided below.

S1, $x_{1\ (ACK\ corrupted)}$, x_2, x_3, x_4, S4, x_5, S6.

QUESTION LIST:

transition x_1

D

transition x_2

E

transition x_3

B

transition x_4

A

transition x_5

C

ANSWER LIST:

A. S3
B. R3
C. R4
D. R1
E. S2
F. R2

CUMULATIVE ACK.

What is meant by a cumulative acknowledgment, ACK*(n)*?

- A cumulative ACK*(n)* allows the receiver to let the sender know that it has not yet received an ACK for packet with sequence number *n*.
- A cumulative ACK*(n)* acks all packets with a sequence number up to and including *n* as being received.
- A cumulative ACK*(n)* allows the receiver to let the sender know that it has not received any packets with a new sequence number since the last cumulative ACK*(n)* was sent.

STOP-AND-WAIT: CHANNEL UTILIZATION.

Suppose a packet is 10K bits long, the channel transmission rate connecting a sender and receiver is 10 Mbps, and the round-trip propagation delay is 10 ms. What is the maximum channel utilization of a stop-and-wait protocol for this channel?

- .01
- .001
- 1.0
- 10.0
- .1

CHANNEL UTILIZATION WITH PIPELINING.

Suppose a packet is 10K bits long, the channel transmission rate connecting a sender and receiver is 10 Mbps, and the round-trip propagation delay is 10 ms. What is the channel utilization of a pipelined protocol with an arbitrarily high level of pipelining for this channel?

- 0.001
- 10.0
- 0.01
- 0.1
- 1.0

CHANNEL UTILIZATION WITH PIPELINING (MORE).

Suppose a packet is 10K bits long, the channel transmission rate connecting a sender and receiver is 10 Mbps, and the round-trip propagation delay is 10 ms. How many packets can the sender transmit before it starts receiving acknowledgments back?

- 100
- 1000
- 1
- 10,000
- 10

PIPELINING.

Which of the following statements about pipelining are true? One or more statements may be true.

- [x] With a pipelined sender, there may be transmitted packets “in flight” – propagating through the channel – packets that the sender has sent but that the receiver has not yet received.
- [ ] With pipelining, a packet is only retransmitted if that packet, or its ACK, has been lost.
- [ ] With pipelining, a receiver will have to send fewer acknowledgments as the degree of pipelining increases
- [x] A pipelined sender can have transmitted multiple packets for which the sender has yet to receive an ACK from the receiver.

PACKET BUFFERING IN GO-BACK-N.

What are some reasons for discarding received-but- out-of-sequence packets at the receiver in GBN? Indicate one or more of the following statements that are correct.

- [x] The implementation at the receiver is simpler.
- [x] The sender will resend that packet in any case.

- [ ] If some packets are in error, then its likely that other packets are in error as well.
- [ ] Discarding an out of sequence packet will really force the sender to retransmit.

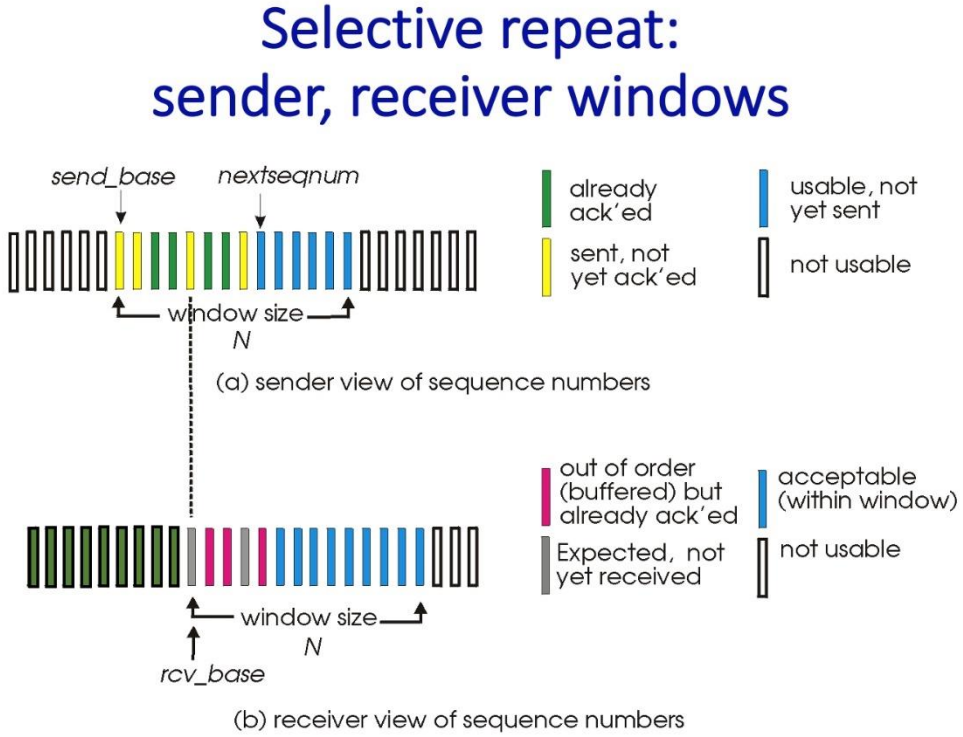
PACKET BUFFERING IN GO-BACK-N (MORE).

What are some reasons for ***not*** discarding received-but- out-of-sequence packets at the receiver in GBN? Indicate one or more of the following statements that are correct.

- [ ] By not discarding, the receiver can implicitly let the sender know that it (the sender) does not necessarily have to retransmit that packet.
- [ ] Complex protocols are always better.
- [x] Even though that packet will be retransmitted, its next retransmission could be corrupted, so don’t discard a perfectly well-received packet, silly!

RECEIVER OPERATION IN SELECTIVE REPEAT.

In the SR receiver window (see diagram below, taken from PPT slides and video), why haven't the red packets been delivered yet? Check the one or more reasons below that apply.



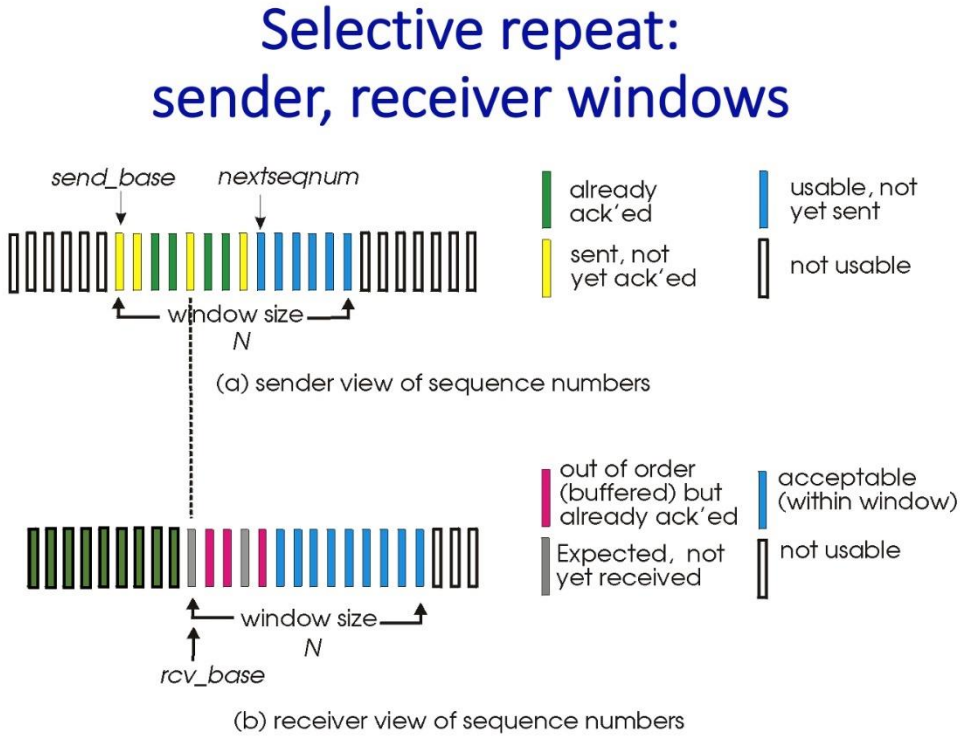
☑ There is a packet with a lower sequence number than any of the red packets that has yet to be received, so in-order delivery of data in the red packets up to the application layer is not possible.

☐ There is a packet with a higher sequence number than any of the red packets that has yet to be received, so in-order delivery of data in the red packets to the application layer is not yet possible.

☐ Red packets have a lower delivery priority up to the application.

RECEIVER OPERATION IN SELECTIVE REPEAT (MORE).

In SR, why does the receiver have to acknowledge packets with sequence numbers that are less than (and to the left of) those in its window, which starts at *rcv_base*.



☐ Actually, this ACK retransmission can be ignored and the protocol will still function correctly, but its performance won't be as good.

☑ Because the sender may not have received an ACK for that packet yet.

☐ Because, at the time of the data packet arrival at the receiver, the sender has definitely still not received an ACK for that packet.

5.Connection-oriented Transport: TCP

TCP RELIABILITY SEMANTICS.

True or False: On the sending side, the TCP sender will take each application-layer chunk of data written into a TCP socket and send it in a distinct TCP segment. And then on the receiving side, TCP will deliver a segment's payload into the appropriate socket, preserving the application-defined message boundary.

- ○ True.
- ◉ False.

TCP EGMENT FORMAT.

For the given function of a field in the TCP segment, select the name of that field from the pull-down list.

QUESTION LIST:

This field contains the port number associated with the sending socket for this TCP segment.

E

This field contains application data that was written into a socket by the sender of this TCP segment.

D

This field contains the index in the sender-to-receiver byte stream of the first byte of that data in the payload carried in this segment.

B

This field contains the index in the byte stream of the next in-order byte expected at the receiver

F

If set, this segment cumulatively ACKs all data bytes up to, but not including, the byte index in the ACK value field of this segment.

C

This field contains the number of available bytes in the TCP receiver's buffer.

H

This field contains the Internet checksum of the TCP segment and selected fields in the IP datagram header.

A

This field contains the number of bytes in the TCP header.

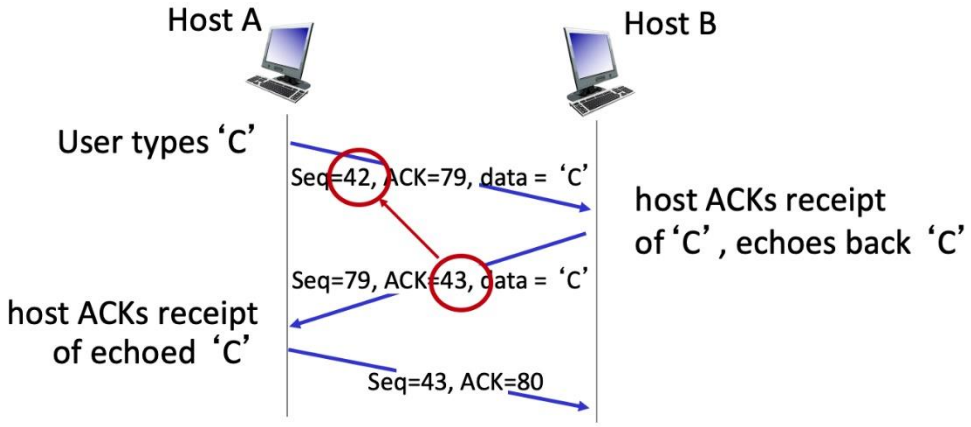
G

ANSWER LIST:

A. Checksum
B. Sequence number
C. ACK bit
D. Data (or payload).
E. Source port number
F. ACK number field
G. Header length field

TCP SEQUENCE NUMBERS AND ACKS (1).

Consider the TCP Telnet scenario below (from Fig. 3.31 in text). Why is it that the receiver sends an ACK that is one larger than the sequence number in the received datagram?



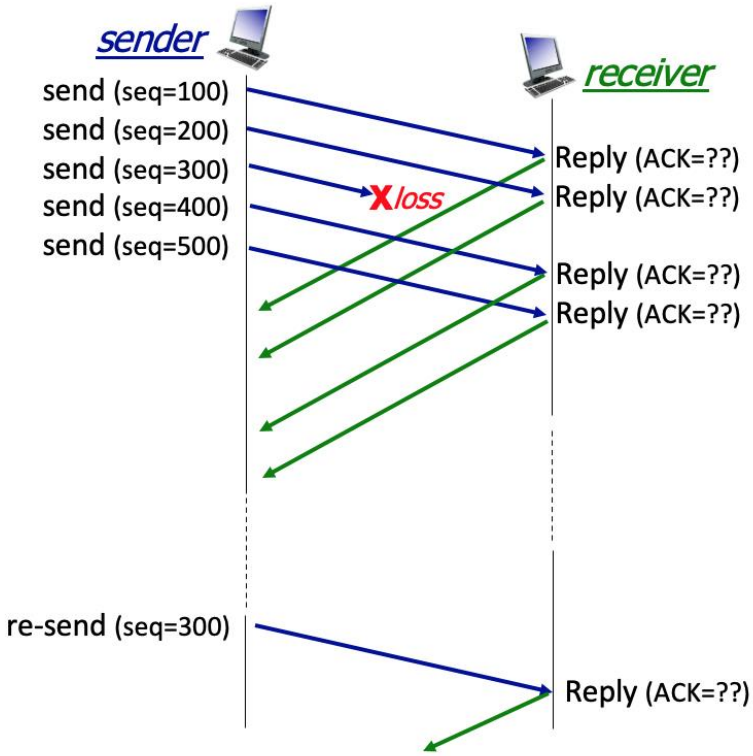
simple telnet scenario

○ Because TCP sequence numbers always increase by 1, with every new segment, and the TCP receiver always send the sequence number of the next expected segment

◉ Because the send-to receiver segment carries only one byte of data, and after that segment is received, the next expected byte of data is just the next byte (i.e., has an index that is one larger) in the data stream.

TCP SEQUENCE NUMBERS AND ACKS (2).

Suppose that as shown in the figure below, a TCP sender is sending segments with 100 bytes of payload. The TCP sender sends five segments with sequence numbers 100, 200, 300, 400, and 500. Suppose that the segment with sequence number 300 is lost. The TCP receiver will buffer correctly-received but not-yet-in-order segments for later delivery to the application layer (once missing segments are later received).



Complete the sentences below ....

QUESTION LIST:

After receiving segment 100, the receiver responds with an ACK with value:

D

After receiving segment 200, the receiver responds with an ACK with value:

A

After receiving segment 500, the receiver responds with an ACK with value:

C

After receiving the *retransmitted* segment 300, the receiver responds with an ACK with value:

B

The TCP receiver does *not* respond in the example, with an ACK with value:

E

ANSWER LIST:

A. 300
B. 600
C. 300, a duplicate ACK
D. 200

TCP RTT ESTIMATION: EWMA.

Consider TCP use of an exponentially weighted moving average (EWMA) to compute the nth value of the estimated RTT:

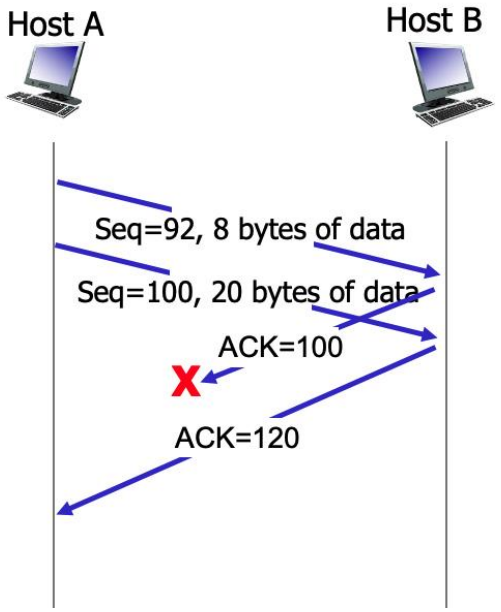
$EstimatedRTT_n = (1- a)*EstimatedRTT_{n-1} + a*SampleRTT_n$

True or False: with this EWMA algorithm the value of $EstimatedRTT_n$ has no dependence on the earlier sample, $SampleRTT_{n-1}$

- ○ True
- ◉ False

TCP TIMER MANAGEMENT.

Consider the TCP Telnet scenario below (from Fig. 3.36 in text). What timer-related action does the sender take on the receipt of ACK 120?



- ○ Leaves any currently-running timers running.
- ○ Restarts a timer for the segment with sequence number 92.
- ◉ cancels any running timers.

TCP FLOW CONTROL.

True or False: with TCP's flow control mechanism, where the receiver tells the sender how much free buffer space it has (and the sender always limits the amount of outstanding, unACKed, in-flight data to less than this amount), it is not possible for the sender to send more data than the receiver has room to buffer.

- (•) True
- ( ) False

TCP CONNECTION MANAGEMENT.

Match the description of a TCP connection management message with the name of the message used to accomplish that function.

QUESTION LIST:

A message from client to server initiating a connection request.

D

A message from server to client ACKing receipt of a SYN message and indicating the willingness of the server to establish a TCP connection with the client.

A

A message indicating that the sending side is initiating the protocol to terminate a connection.

E

A message sent in response to a request to terminate a connection, ACKing that the side receiving this message is also willing to terminate the connection

C

A general purpose error message used during connection set up or tear down to let the other side know that an error has occurred, and that the referenced connection should be shut down.

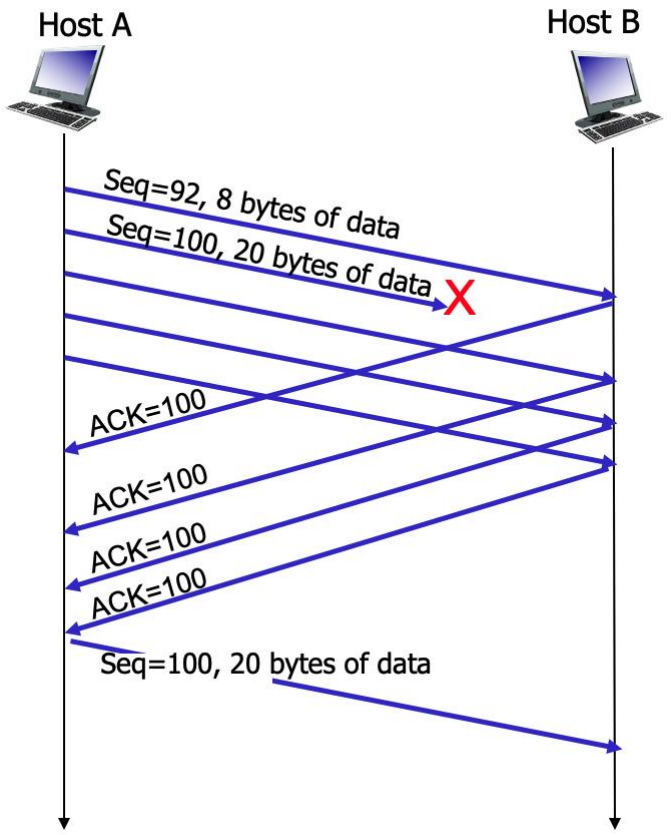
A

ANSWER LIST:

A. SYNACK message
B. RESET message
C. FINACK message
D. SYN mesage
E. FIN message

TCP FAST RETRANSMIT.

Consider TCP's Fast Retransmit optimization (see Figure 3.37 from the text, below). Of course, the sender doesn't know for sure that the segment with sequence # 100 is actually lost (it can't see into the channel). Can a sender get three duplicate ACKs for a segment that in fact has *not* been lost? Which of the following statements are true? Suppose a channel can lose, but will not corrupt, messages.



☑ If the channel can reorder messages, a triple duplicate ACK can occur even though a message is not lost; since it's possible that a message has just been reordered and has not yet arrived when the three duplicate ACKs were generated.

☑ If the channel cannot reorder messages, a triple duplicate ACK indicates to the sender that a segment loss has happened for sure. Actually (again assuming the channel cannot corrupt or reorder messages), even a *single* duplicate ACK would indicate that a segment loss has happed for sure.

6. Principles of Congestion Control

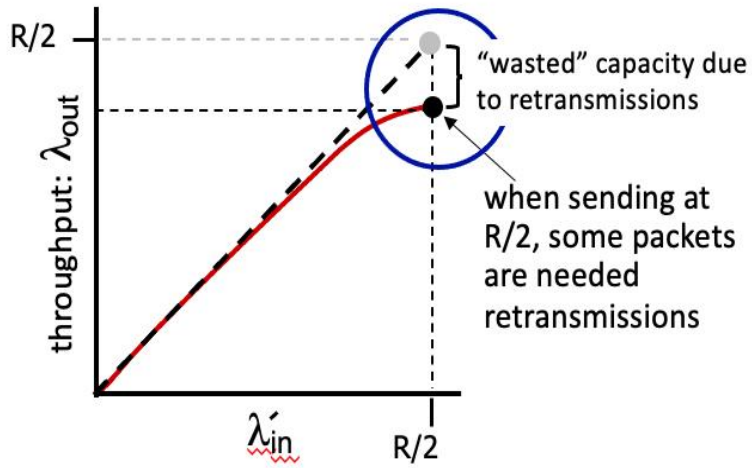
CONGESTION CONTROL VERSUS FLOW CONTROL.

Consider the five images below. Indicate which of these images suggest the need for *flow* control (the others would suggest the need for congestion control).

- [x] A glass overflowing
- [ ] Car traffic
- [x] A talking head
- [ ] A crowd of people
- [ ] A penguin crowd

TWO CONGESTED SENDERS.

Consider the figure below, which shows the application-to-application throughput achieved when two senders are competing at a shared bottleneck link. Suppose that when the overall arrival rate, $lambda_{in}$' (for each sender) is close to R/2, the throughput to the application layer (at each receiver), $lambda_{out}$, is equal to 0.8 * $lambda_{in}$'.



What fraction of the packets transmitted at the sender are retransmissions?

- (•) .20
- ( ) 0
- ( ) .80
- ( ) .50

NETWORK-ASSISTED OR END-END CONGESTION CONTROL?

Which of the following actions are used in network-assisted congestion control (say versus end-end congestion control) to signal congestion. Check all that apply.

- [ ] A router drops a packet at a congested router.
- [ ] The sender decreases its sending rate in response to a measured increase in the RTT.
- [ ] The transport-layer receiver informs sender of the size of its (transport-payer receiver) receive window.
- [x] A router sends an ICMP message to a host telling it to slow down its sending rate.
- [ ] A sender decreases its sending rate in response to packet loss detected via its transport-layer ACKing.
- [ ] A datagram experiences delay at a congested network router, which is then measured by the sender and used to decrease the sending rate.
- [x] A router marks a field in the datagram header at a congested router.

NETWORK-ASSISTED OR END-END CONGESTION CONTROL (2)?

Which of the following actions are associated with end-end congestion control (say versus network-assisted congestion control). Check all that apply.

- [x] The transport-layer sender decreases its sending rate in response to a measured increase in the RTT.
- [x] A router drops a packet at a congested router, which causes the transport-layer sender to infer that there is congestion due to the missing ACK for the lost packet.
- [ ] A router sends an ICMP message to a host telling it to slow down its sending rate.
- [x] A sender decreases its sending rate in response to packet loss detected via its transport-layer ACKing.
- [ ] A router marks a field in the datagram header at a congested router.
- [x] A datagram experiences delay at a congested network router, which is then measured by the sender and used to decrease the sending rate.
- [ ] The transport-layer receiver informs sender of the size of its (transport-payer receiver) receive window.

DIFFERENT APPROACHES TOWARDS CONGESTION CONTROL.

Use the pulldown menu to match a congestion control approach to how the sender detects congestion.

QUESTION LIST:

The sender infers segment loss from the absence of an ACK from the receiver.

B

Bits are set at a congested router in a sender-to-receiver datagram, and bits are in the returned to the sender in a receiver-to sender ACK, to indicate congestion to the sender.

B

The sender measures RTTs and uses the current RTT measurement to infer the level of congestion.

B

ANSWER LIST:

A. delay-based
B. network-assisted
C. end-end

7. **TCP Congestion Control**

TCP'S AIMD ALGORITHM.

Which of the following statements about TCP's Additive-increase-multiplicative-decrease (AIMD) algorithm are true? Check all that are true.

- [x] AIMD cuts the congestion window size, `cwnd`, in half whenever loss is detected by a triple duplicate ACK.
- [ ] AIMD uses observed packet loss to detect congestion.
- [ ] AIMD uses the measured RTT delay to detect congestion.
- [ ] AIMD *always* cuts the congestion window size, `cwnd`, in half whenever loss is detected.
- [x] AIMD is a end-end approach to congestion control.
- [ ] AIMD is a network-assisted approach to congestion control.
- [x] AIMD cuts the congestion window size,`cwnd, i` to 1 whenever a timeout occurs.

TCP'S AIMD ALGORITHM (2).

How is the sending rate typically regulated in a TCP implementation?

- ○ By using the retransmission timeout timer and counting the number of bytes sent since the last timeout to compute the sending rate since that last timeout, and then making sure its sending rate never exceed the rate set by AIMD.
- ○ By keeping a window of size cwnd over the sequence number space, and making sure that no more than `cwnd` bytes of data are outstanding (i.e, unACKnowledged). The size of `cwnd i`s regulated by AIMD.

TCP'S SLOWSTART ALGORITHM.

Which of the following best completes this sentence: "In the absence of loss, TCP slow start increases the sending rate ... "

- ◉ " ... faster than AIMD. In fact, slowstart increases the sending rate exponentially fast per RTT."
- ○ "... at the same rate as AIMD."
- ○ ... slower than AIMD, that's why it's called Slowstart."

UNCONTROLLED TRANSPORT-LAYER SENDERS.

Consider the transport-layer flows interacting at a congested link. In the face of such congestion, what happens at this link to a transport-layer flow that does not cut back on its sending rate?

- ○ The router will send a signal to the TCP sender that would force the TCP sender to cut its rate in half.
- ○ That sender's datagrams will be preferentially dropped at the congested link.
- ◉ Nothing different from the other flows crossing the congested link.

TCP CUBIC.

Assuming that the congestion window size, `cwnd`, has not yet reached W_{max}, TCP CUBIC will ... (check all that apply)

- ☐ ... have a sending rate that always increases faster than that of AIMD.
- ☑ ... increase its sending rate faster than AIMD when cwnd is far away from W_{max}, but increase slower than AIMD when cwnd is closer to W_{max}
- ☑ ... always have a window size, `cwnd`, and hence a sending rate, higher than that of AIMD (assuming a given window size, W_{max}, at which loss would occur).

DELAY-BASED CONGESTION CONTROL.

For delay-based congestion control, match the sender action to the relationship of the currently measured throughput to the value of $\texttt{cwnd/RTT}_{min}$

QUESTION LIST:

The currently measured throughput is greater than $\texttt{cwnd/RTT}_{min}$

B

The currently measured throughput is equal to or a bit less than than $\texttt{cwnd/RTT}_{min}$

A

The currently measured throughput is much less that than $\texttt{cwnd/RTT}_{min}$

C

ANSWER LIST:

A. increase the sending rate
B. This should never happen.
C. decrease the sending rat

8. **Evolution of Transport Layer Functionality**

QUIC STREAMS.

What are advantages of the *streams* concept in QUIC? Select all that apply.

☐ With *N* streams, the overall throughput can be increased by a factor of *N*, since each stream has its own separate congestion control.
☑ Streams allow concurrent retrieval of web objects, while avoiding Head of the Line (HOL) blocking.
☑ Since each stream has its own error control, if one stream experiences an error (e.g., lost or damaged segment), the other streams are unaffected.

QUIC: AN APPLICATION-LAYER PROTOCOL.

What are advantages of implementing transport-layer functionality in QUIC at the application layer? Select all that apply.

☑ QUIC can establish all connection parameters (security, reliability, flow and congestion control)in just one handshake rather than separately in two.
☐ QUIC's performance can be better optimized at the application-layer, so it will have better performance than if these functions were implremented in the operating system.
☐ QUIC performs both congestion control and error recovery different from TCP, leveraging all of the knowledge that has built up since TCP was first standardized, and therefore has better performance than TCP.
☑ As an application-layer protocol, QUIC can be updated/modified at "app frequency" rather than at the frequency of operating system updates.

CHAPTER 4: NETWORK LAYER: DATA PLANE

1. **Network Layer Overview**

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

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 then correspond to routing.

- ☐ A climber decides to take the South Col Route to the top of Mt Everest rather than the Northeast Ridge route.
- ☑ A car waits at light and then turns left at the intersection.
- ☑ A car takes the 3rd exit from a roundabout.
- ☐ A traveler decides to fly to Sydney through Singapore rather that Dubai.
- ☐ 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 car stops at an intersection to “gas-up” and take a “bathroom break”

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.

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

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.

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

BEST EFFORT SERVICE.

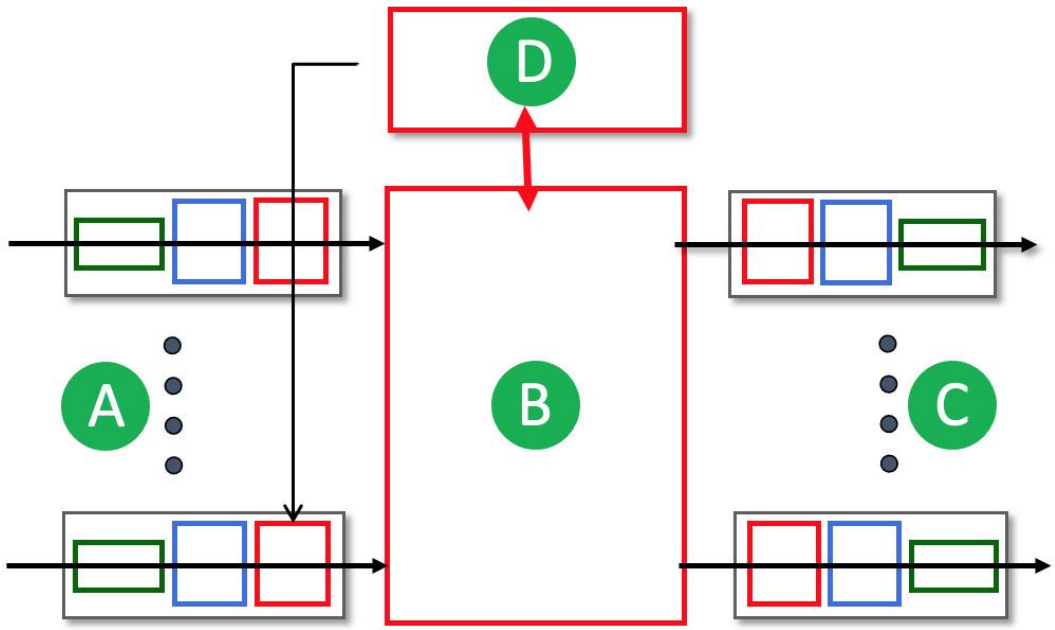
Which of the following quality-of-service guarantees are part of the Internet's best-effort service model? Check all that apply.

- [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!
- [ ] Guaranteed delivery time from sending host to receiving host.
- [ ] In-order datagram payload delivery to the transport layer of those datagrams arriving to the receiving host.
- [ ] Guaranteed delivery from sending host to receiving host.
- [ ] A guaranteed minimum bandwidth is provided to a source-to-destination flow of packets

2. **Whats Inside a Router?**

WHAT'S INSIDE A ROUTER?

Match the names of the principal router components (A,B,C,D below) with their function and whether they are in the network-layer data plane or control plane.



QUESTION LIST:

(A) are ...

C

(B) is ...

E

(C) are ...

D

(D) is ...

A

ANSWER LIST:

A. the routing processor, operating primarily in the control plane.
B. the switching fabric, operating primarily in the control plane.
C. input ports, operating primarily in the data plane.
D. output ports, operating primarily in the data plane.
E. the switching fabric, operating primarily in the data plane.
F. input ports, operating primarily in the control plane.
G. the routing processor, operating primarily in the data plane.
H. output ports, operating primarily in the control plane.

WHERE DOES DESTINATION ADDRESS LOOKUP HAPPEN?

Where in a router is the destination IP address looked up in a forwarding table to determine the appropriate output port to which the datagram should be directed?

- ○ At the output port leading to the next hop towards the destination.
- ○ Within the switching fabric.
- ○ Within the routing processor.
- ○ At the input port where a packet arrives.

WHERE DOES "MATCH+ACTION" HAPPEN?

Where in a router does "match plus action" happen to determine the appropriate output port to which the arriving datagram should be directed?

- ○ At the output port leading to the next hop towards the destination.
- ○ Within the switching fabric.
- ◉ At the input port where a packet arrives.
- ○ Within the routing processor.

LONGEST PREFIX MATCHING.

Consider the following forwarding table below. Indicate the output to link interface to which a datagram with the destination addresses below will be forwarded under longest prefix matching. (Note: The list of addresses is ordered below. If two addresses map to the same output link interface, map the first of these two addresses to the first instance of that link interface.) [Note: You can find more examples of problems similar to this here.]

Destination Address Range	Link interface
11001000 00010111 00010*** ********	0
11001000 00010111 00011000 ********	1
11001000 00010111 00011*** ********	2
otherwise	3

QUESTION LIST:

11001000 00010111 00010010 10101101

B

11001000 00010111 00011000 00001101

A

11001000 00010111 00011001 11001101

F

10001000 11100000 00011000 00001101

C

11001000 00010111 00011000 11001111

G

11001000 00010111 00010001 01010101

H

11001000 00010111 00011101 01101101

D

ANSWER LIST:

A. This is the first destination address in the list that maps to output port **1**.
B. This is the first destination address in the list that maps to output port **0**.
C. This is the first destination address in the list that maps to output port **3**.
D. This is the second destination address in the list that maps to output port **2**.
E. This is the second destination address in the list that maps to output port **3**.
F. This is the first destination address in the list that maps to output port **2**.
G. This is the second destination address in the list that maps to output port **1**.
H. This is the second destination address in the list that maps to output port **0**.

PACKET DROPPING.

Suppose a datagram is switched through the switching fabric and arrives to its appropriate output to find that there are no free buffers. In this case:

- The packet will be dropped (lost).
- The packet will be sent back to the input port.
- The packet will either be dropped or another packet will be removed (lost) from the buffer to make room for this packet, depending on policy. But the packet will definitely not be be sent back to the input port.
- Another packet will be removed (lost) from the buffer to make room for this packet.

HOL BLOCKING.

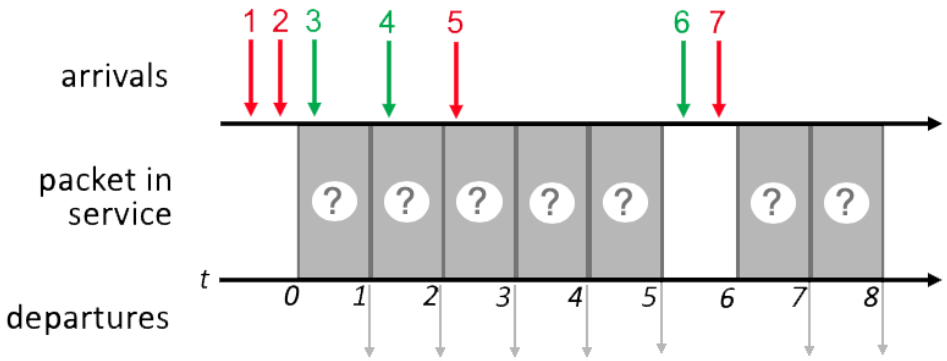
What is meant by Head of the Line (HOL) blocking?

- A queued datagram receiving service at the front of a queue prevents other datagrams in queue from receiving service.
- In a block error code, the first bytes of the code indicate the type of coding being used.
- A queued datagram waiting for service at the front of a queue prevents other datagrams in queue from moving forward in the queue.

PACKET SCHEDULING (SCENARIO 1, FCFS).

Consider the pattern of red and green packet arrivals to a router's output port queue, shown below. Suppose each packet takes one time slot to be transmitted, and can only begin transmission at the beginning of a time slot after its arrival. Indicate the sequence of departing packet numbers (at t = 1, 2, 3, 4, 5, 7, 8) under **FCFS** scheduling. Give your answer as 7 ordered digits (each corresponding to the packet number of a departing packet), with a single space between each digit, and no spaces before the first or after the last digit, e.g., in a form like 7 6 5 4 3 2 1).

[Note: You can find more examples of problems similar to this here.]



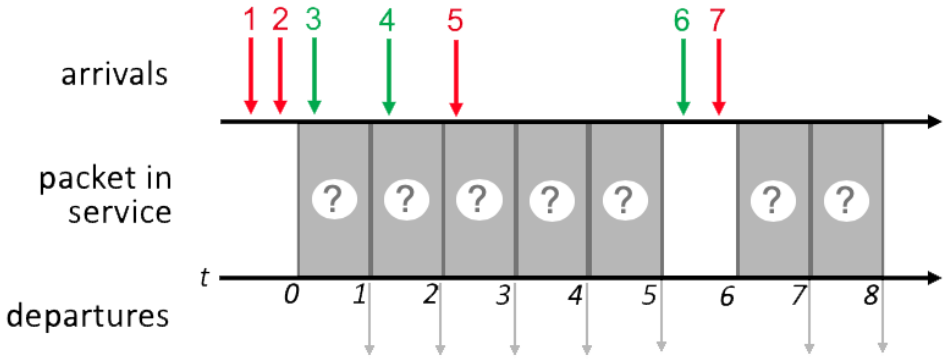
1234567

PACKET SCHEDULING (SCENARIO 1, PRIORITY).

Consider the pattern of red and green packet arrivals to a router's output port queue, shown below. Suppose each packet takes one time slot to be transmitted, and can only begin transmission at the beginning of a time slot after its arrival. Indicate the sequence of departing packet numbers (at t = 1, 2, 3, 4, 5, 7, 8) under **priority** scheduling, where red packets have higher priority.

Give your answer as 7 ordered digits (each corresponding to the packet number of a departing packet), with a single space between each digit, and no spaces before the first or after the last digit, e.g., in a form like 7 6 5 4 3 2 1).

[Note: You can find more examples of problems similar to this here.]



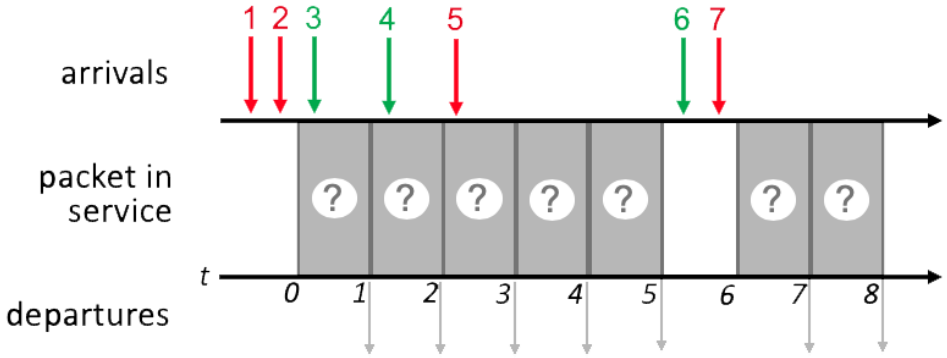
1235476

PACKET SCHEDULING (SCENARIO 1, RR).

Consider the pattern of red and green packet arrivals to a router's output port queue, shown below. Suppose each packet takes one time slot to be transmitted, and can only begin transmission at the beginning of a time slot after its arrival. Indicate the sequence of departing packet numbers (at t = 1, 2, 3, 4, 5, 7, 8) under **round robin scheduling**, where red starts a round if there are both red and green packets ready to transmit after an empty slot.

Give your answer as 7 ordered digits (each corresponding to the packet number of a departing packet), with a single space between each digit, and no spaces before the first or after the last digit, e.g., in a form like 7 6 5 4 3 2 1).

[Note: You can find more examples of problems similar to this here.]

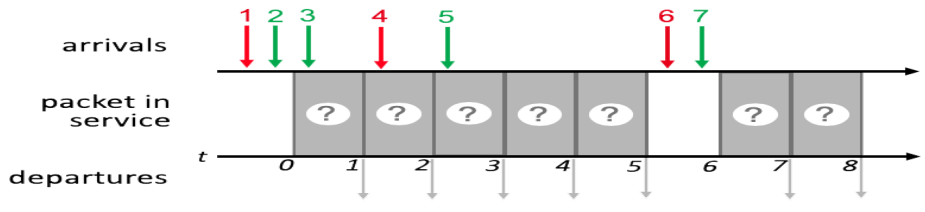


1324576

PACKET SCHEDULING (SCENARIO 2, FCFS).

Consider the pattern of red and green packet arrivals to a router's output port queue, shown below. Suppose each packet takes one time slot to be transmitted, and can only begin transmission at the beginning of a time slot after its arrival. Indicate the sequence of departing packet numbers (at t = 1, 2, 3, 4, 5, 7, 8) under **FCFS** scheduling. Give your answer as 7 ordered digits (each corresponding to the packet number of a departing packet), with a single space between each digit, and no spaces before the first or after the last digit, e.g., in a form like 7 6 5 4 3 2 1).

[Note: You can find more examples of problems similar to this here.]



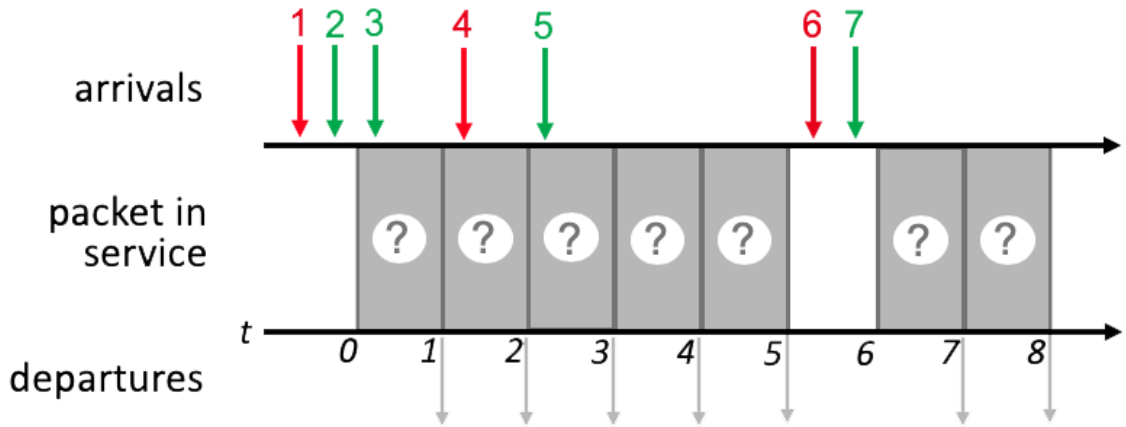
1234567

PACKET SCHEDULING (SCENARIO 2, PRIORITY).

Consider the pattern of red and green packet arrivals to a router's output port queue, shown below. Suppose each packet takes one time slot to be transmitted, and can only begin transmission at the beginning of a time slot after its arrival. Indicate the sequence of departing packet numbers (at t = 1, 2, 3, 4, 5, 7, 8) under **priority** scheduling, where red packets have higher priority.

Give your answer as 7 ordered digits (each corresponding to the packet number of a departing packet), with a single space between each digit, and no spaces before the first or after the last digit, e.g., in a form like 7 6 5 4 3 2 1).

[Note: You can find more examples of problems similar to this here



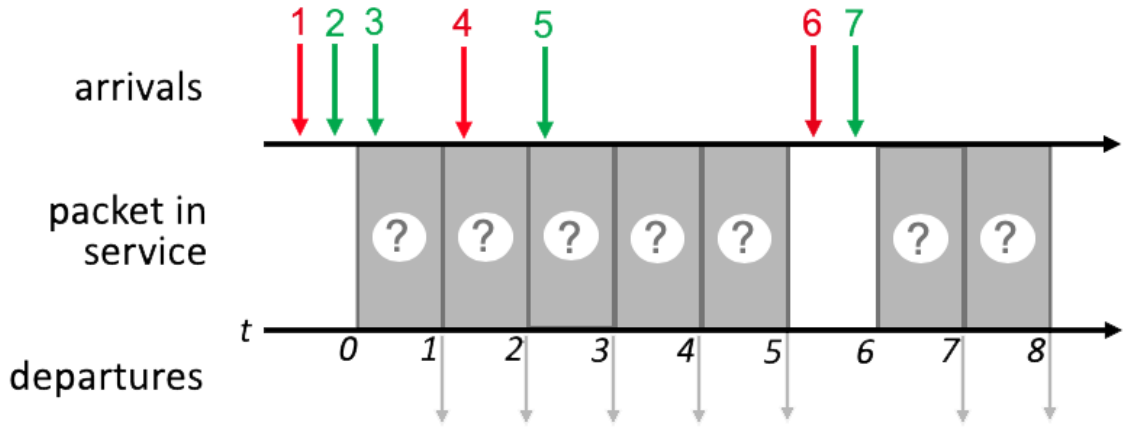
1243567

PACKET SCHEDULING (SCENARIO 2, RR).

Consider the pattern of red and green packet arrivals to a router's output port queue, shown below. Suppose each packet takes one time slot to be transmitted, and can only begin transmission at the beginning of a time slot after its arrival. Indicate the sequence of departing packet numbers (at t = 1, 2, 3, 4, 5, 7, 8) under **round robin scheduling**, where red starts a round if there are both red and green packets ready to transmit after an empty slot.

Give your answer as 7 ordered digits (each corresponding to the packet number of a departing packet), with a single space between each digit, and no spaces before the first or after the last digit, e.g., in a form like 7 6 5 4 3 2 1).

[Note: You can find more examples of problems similar to this here.]


1 2 3 4 5 6 7
arrivals
packet in service
departures
t
0 1 2 3 4 5 6 7 8

1243567

3. **The Internet Protocol**

WHAT IS THE INTERNET PROTOCOL?

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

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

THE IPV4 HEADER.

Match each of the following fields in the IP header with its description, function or use.

QUESTION LIST:

Version field

F

Type-of-service field

H

Fragmentation offset field

B

Time-to-live field

A

Header checksum field

E

Upper layer field

C

Payload/data field

D

Datagram length field.

G

ANSWER LIST:

A. The value in this field is decremented at each router; when it reaches zero, the packet must be dropped.
B. This field is used for datagram fragmentation/reassembly.
C. 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.
D. This field *contains* a UDP or TCP segment, for example.
E. This field contains the Internet checksum of this datagram's header fields.
F. This field contains the IP protocol version number.
G. This field indicates the total number of bytes in datagram.
H. This field contains ECN and differentiated service bits.

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).

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

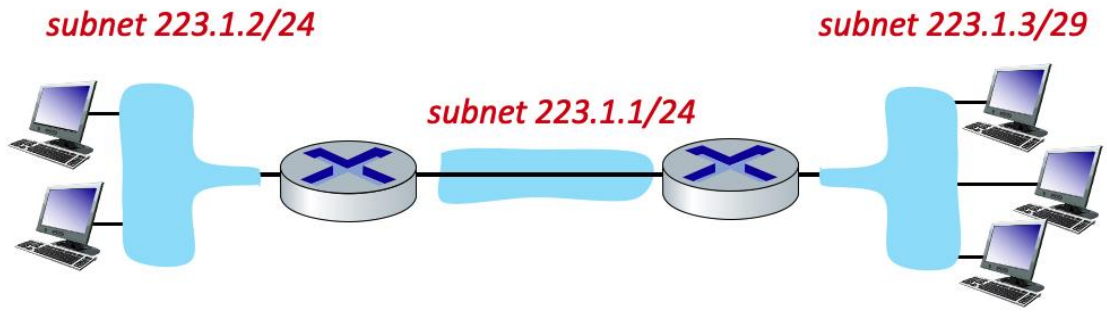
WHAT IS A SUBNET?

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

☑ A set of devices that have a common set of leading high order bits in their IP address.
☐ A set of devices all manufactured by the same equipment maker/vendor.
☑ 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.

SUBNETTING(A).

Consider the three subnets in the diagram below.

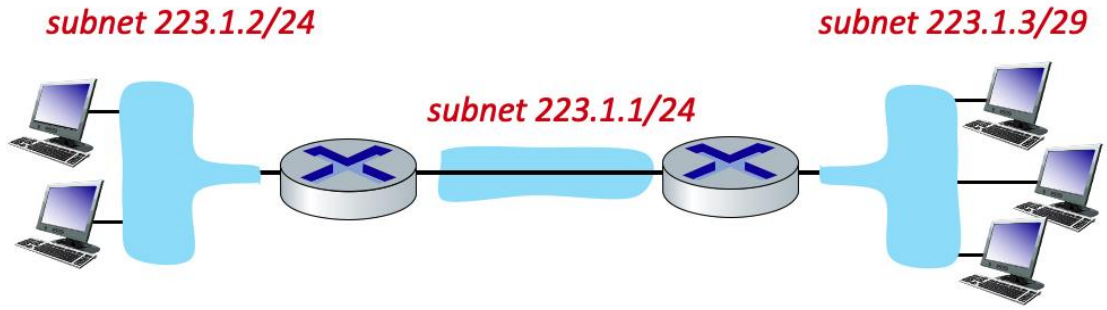


What is the maximum # of interfaces in the 223.1.2/24 network?

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

SUBNETTING(B).

Consider the three subnets in the diagram below.

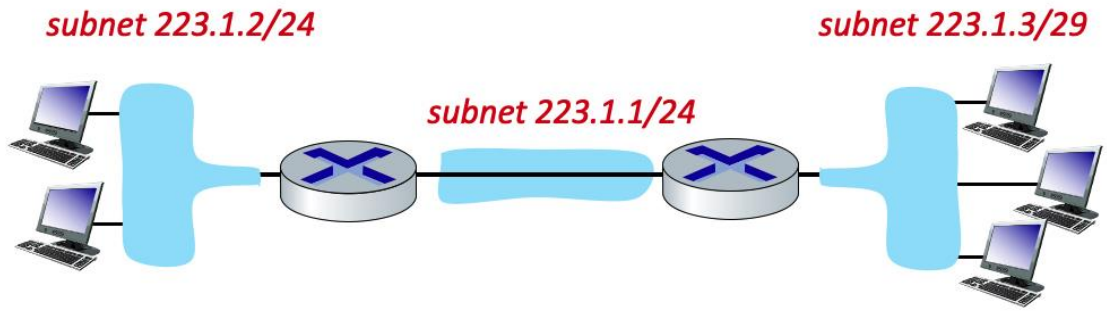


What is the maximum # of interfaces in the 223.1.3/29 network?

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

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.

- ☐ 223.1.3.6
- ☑ 223.1.3.28
- ☑ 223.1.3.16
- ☑ 223.1.2.6
- ☐ 223.1.3.2

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
- ○ The network provides an Ethernet jack for a host’s Ethernet adapter.
- ◉ No manual configuration is needed for the host to join the network.

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

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

PURPPSE OF DHCP.

What is the purpose of the Dynamic Host Configuration Protocon

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

4. **Generalized Forwarding**

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 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 decide whether or not to drop that datagram.
- ... 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 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 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 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.

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.

- [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 forward the datagram to the output port associated with that destination IP address.
- [ ] ... 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 decide whether or not to drop that datagram.
- [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.

☑ … 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.
☑ … 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.

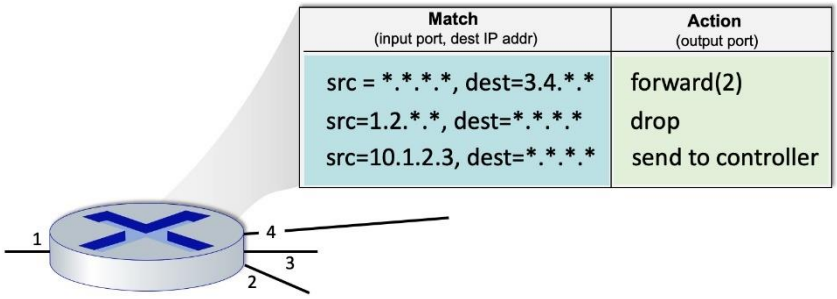
WHAT FIELDS CAN BE MATCHED IN GENERALIZED MATCH+ACTION.

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

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

MATCH+ACTION IN OPENFLOW 1.0.

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

A

Source: 65.92.15.27 Destination: 3.4.65.76

D

Source: 10.1.2.3 Destination: 7.8.9.2

B

Source: 10.1.34.56 Destination: 54.72.29.90

C

ANSWER LIST:

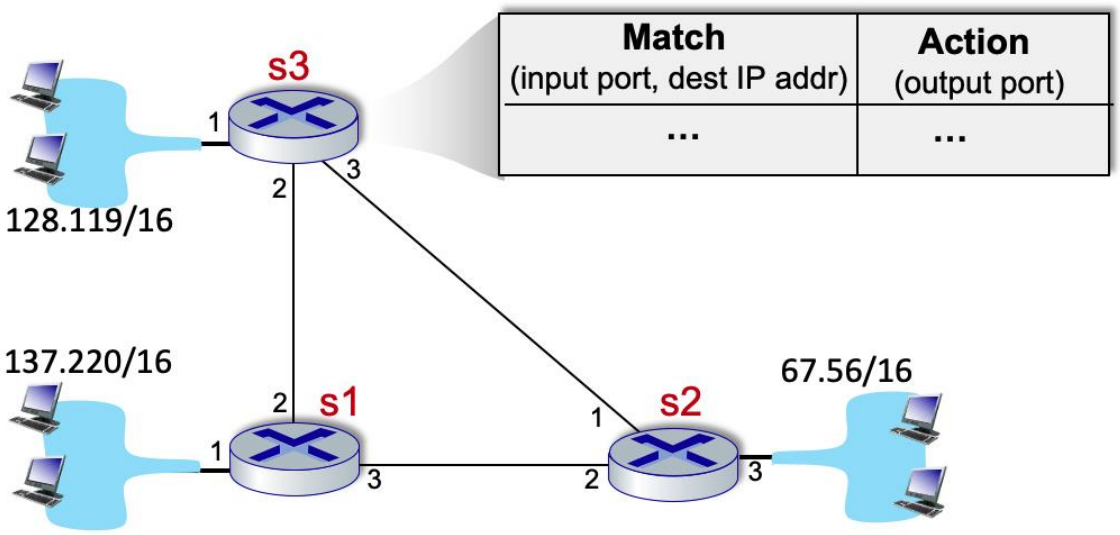
A. Rule 2, with action *drop*
B. Rule 3, with action *send to controller*
C. No match to any rule.
D. Rule 1, with action *forward(2)*

CRAFTING NETWORK-WIDE FORWARDING USING FLOW TABLES.

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.

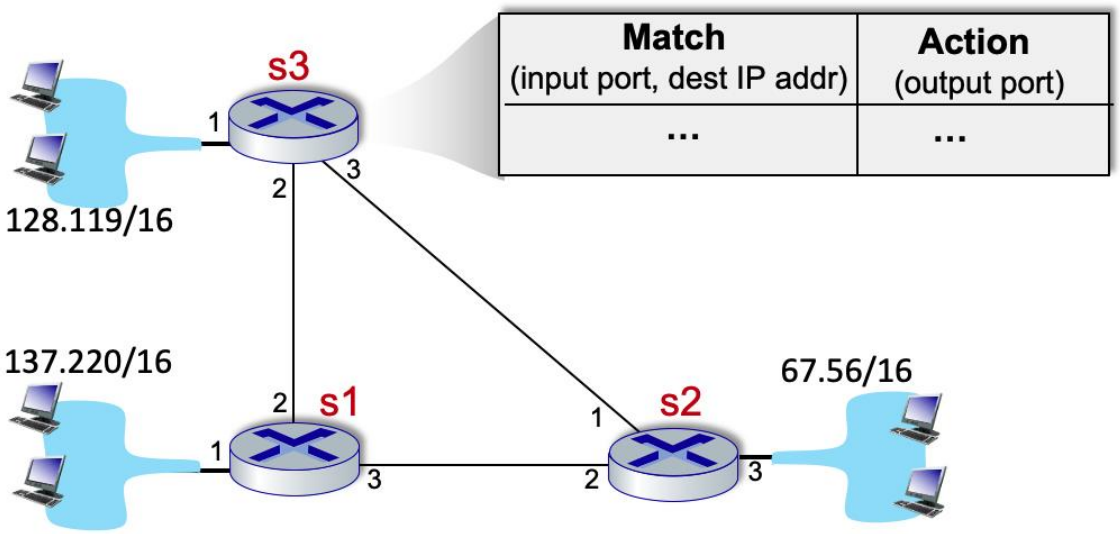
From the list of match+action rules below, select the rules to include in s3's flow table to implement this forwarding behavior. Assume that if a packet arrives and finds no matching rule, it is dropped.



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

CRAFTING NETWORK-WIDE FORWARDING USING FLOW TABLES (MORE).

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

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.
- ( ) 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).
- ( ) None of the other answers is a correct definition of generalized forwarding.

5. **Middleboxes and Summary**

WHAT'S A "MIDDLEBOX"?

Which of the following network devices can be thought of as a "middlebox"? Check all that apply.

- [ ] SDN controller
- [ ] IP router
- [x] HTTP cache
- [ ] WiFi base station
- [x] Network Address Translation box
- [x] HTTP load balancer

THE "THIN WAIST" OF THE INTERNET.

What protocol (or protocols) constitutes the "thin waist" of the Internet protocol stack? Check all that apply.

- [ ] WiFi
- [x] IP
- [ ] HTTP
- [ ] DNS
- [ ] TCP
- [ ] Ethernet

THE END-TO-END PRINCIPLE.

Which of the statements below are true statements regarding the "end-to-end principle"? Check all that apply.

- [ ] The end-to-end argument advocates placing functionality at the network edge to optimize performance, such as end-end delay.
- [x] The end-to-end argument advocates placing functionality at the network edge because some functionality cannot be completely and correctly implemented in the network, and so needs to be placed at the edge in any case, making in-network implementation redundant.
- [x] The end-to-end argument allows that some redundant functionality might be placed both in-network and at the network edge in order to enhance performance.

THE INTERNET HOURGLASS.

What is meant when it is said that the Internet has an “hourglass” architecture? See the picture below if you are unfamiliar with an "hourglass".

An hourglass

- Packets flow from top to bottom down the stack, like sand in an hour glass. Then, on the receiver side, if the hourglass is reversed, packets flow up the stack, like sand flowing in the opposite direction.
- ... 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.
- The Internet protocol stack has a “thin waist” in the middle, like an hourglass. The Internet Protocol (IP) is the only network-layer protocol in the middle layer of the stack. Every other layer has multiple protocols at that layer.

FEDERAL REGULATION AND THE INTERNET.

In the US, which of the following services has been regulated by the Federal Communications Commission (FCC) going back into the 20th century?

- Information services.
- Neither telecommunications services (broadly) nor information services; the FCC's jurisdiction is only on over-the-air (e.g., wireless) links.
- Both telecommunications services and information services.
- Telecommunication services

CHAPTER 5: NETWORK LAYER: CONTROL PLANE

1. **Introduction to the Network-layer control plane**

ROUTING VERSUS FORWARDING.

Which of the following statements correctly identify the differences between routing and forwarding. Select one or more statements.

☑ *Forwarding* refers to moving packets from a router's input to appropriate router output, and is implemented in the data plane.
☑ *Routing* refers to determining the route taken by packets from source to destination, and is implemented in the control plane.
☐ *Routing* refers to moving packets from a router's input to appropriate router output, and is implemented in the data plane.
☐ *Routing* refers to determining the route taken by packets from source to destination, and is implemented in the data plane.
☐ *Forwarding* refers to determining the route taken by packets from source to destination, and is implemented in the control plane.
☐ *Forwarding* refers to moving packets from a router's input to appropriate router output, and is implemented in the control plane.
☐ *Routing* refers to moving packets from a router's input to appropriate router output, and is implemented in the control plane.
☐ *Forwarding* refers to determining the route taken by packets from source to destination, and is implemented in the data plane.

APPROACHES TOWARDS IMPLEMENTING THE CONTROL PLANE.

Match the name of the approach towards implementing a control plane with a description of how this approach works.

QUESTION LIST:

Per-router control plane.

B

Software-defined networking (SDN).

C

ANSWER LIST:

A. The network operator installs forwarding tables using the Simple Network Management Protocols (SNMP).
B. Individual routing algorithm components - with a component operating in each and every router - interact with each other in the control plane. The individual routing algorithm component executing in a given router computes the local fowarding table fir that router.
C. A (typically) remote controller gathers information from routers, and then computes and installs the forwarding tables in routers.

2. **Routing Algorithms**

WHAT'S A "GOOD" PATH?

What is the definition of a "good" path for a routing protocol? Chose the best single answer.

- ○ A path that has little or no congestion.
- ○ A high bandwidth path.
- ◉ Routing algorithms typically work with abstract link weights that could represent any of, or combinations of, all of the other answers.
- ○ A low delay path.
- ○ A path that has a minimum number of hops.

DIJKSTRA'S LINK-STATE ROUTING ALGORITHM.

Consider Dijkstra's link-state routing algorithm that is computing a least-cost path from node a to other nodes b, c, d, e, f. Which of the following statements is true. (Refer to Section 5.2 in the text for notation.)

- ☑ The values computed in the vector D(v), the currently known least cost of a path from a to any node v, will never increase following an iteration.
- ☐ The values computed in the vector D(v), the currently known least cost of a path from a to any node v, will always decrease following an iteration.
- ☑ In the initialization step, the initial cost from a to each of these destinations is initialized to either the cost of a link directly connecting a to a direct neighbor, or infinity otherwise.
- ☑ Suppose nodes b, c, and d are in the set N'. These nodes will remain in N' for the rest of the algorithm, since the least-cost paths from a to b, c, and d are known.
- ☐ Following the initialization step, if nodes b and c are directly connected to a, then the least cost path to b and c will never change from this initial cost.

WHAT TYPE OF ROUTING?

Match the name of a general approach to routing with characteristics of that approach.

QUESTION LIST:

Centralized, global routing.

A

Decentralized routing.

C

Static routing.

B

Dynamic routing.

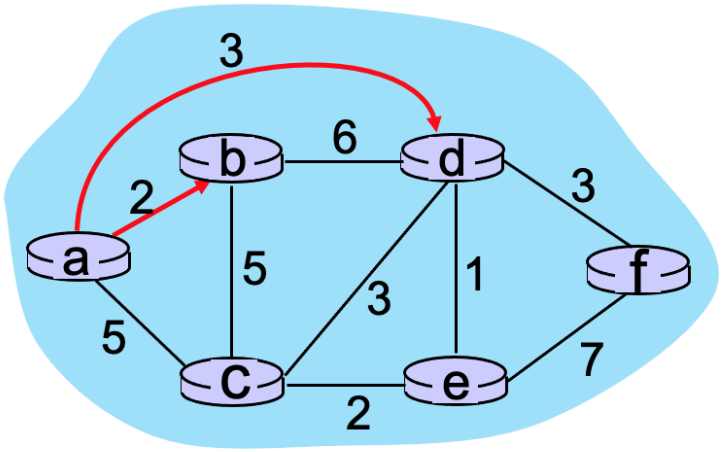
D

ANSWER LIST:

A. All routers have complete topology, and link cost information.
B. Routes change slowly over time.
C. An iterative process of computation, exchange of informatoin with neighbors. Routers may initially only know link costs to directly-attached neighbors.
D. Routing changes quickly over time.

DIJKSTRA'S LINK-STATE ROUTING ALGORITHM (PART 1).

Consider the graph shown below and the use of Dijkstra's algorithm to compute a least cost path from a to all destinations. Suppose that nodes b and d have already been added to N'. What is the next node to be added to N' (refer to the text for an explanation of notation).

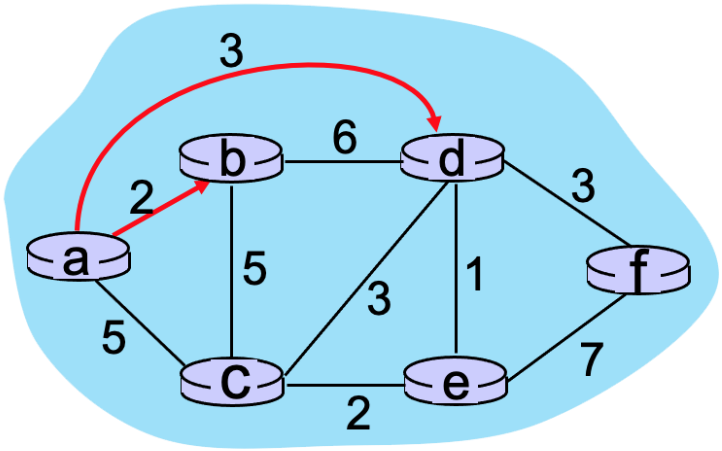


[Note: You can find more examples of problems similar to this here.]

- e
- c
- f

DIJKSTRA'S LINK-STATE ROUTING ALGORITHM (PART 2).

Consider the graph shown below and the use of Dijkstra's algorithm to compute a least cost path from a to all destinations. Suppose that nodes b and d have already been added to N'. What is the *path cost* to the next node to be added to N' (refer to the text for an explanation of notation).



[Note: You can find more examples of problems similar to this here.]

- 6
- 4
- 5
- 7

3. **Intra-AS Routing in the Internet: OSPF**

ROUTING WITHIN OR AMONG NETWORKS.

Match the terms "interdomain routing" and intradomain routing" with their definitions. Recall that in Internet parlance, an “AS” refers to “Autonomous System” – a network under the control of a single organization.

QUESTION LIST:

Interdomain routing.

C

Intradomain routing.

B

ANSWER LIST:

A. Forwarding packets between two interfaces in different but adjacent subnetworks.
B. Routing among routers within same AS (“network”).
C. Routing among different ASes (“networks”).
D. Forwarding packets between two physically connected interfaces in a common subnetwork.

OPEN SHORTEST PATH FIRST (OSPF).

Check the one or more of the following statements about the OSPF protocol that are true.

- [ ] OSPF is an interdomain routing protocol.
- [ ] The Open Shortest Path First (OSPF) Internet routing protocol implements a Bellman-Ford distance-vector routing algorithm.
- [x] OSFP uses a Dijkstra-like algorithm to implement least cost path routing.
- [x] OSPF is an intra-domain routing protocol.
- [x] OSPF implements hierarchical routing

OPEN SHORTEST PATH FIRST (OSPF).

Consider the OSPF routing protocol. Which of the following characteristics are associated with OSPF (as opposed to BGP)?

- [ ] Policy, rather than performance (e.g., least cost path), determines paths that used.
- [ ] Is an inter-domain routing protocol.
- [x] Floods link state control information.
- [x] Is an intra-domain routing protocol.
- [x] Finds a least cost path from source to destination.

4. **Routing Among the ISPs: BGP**

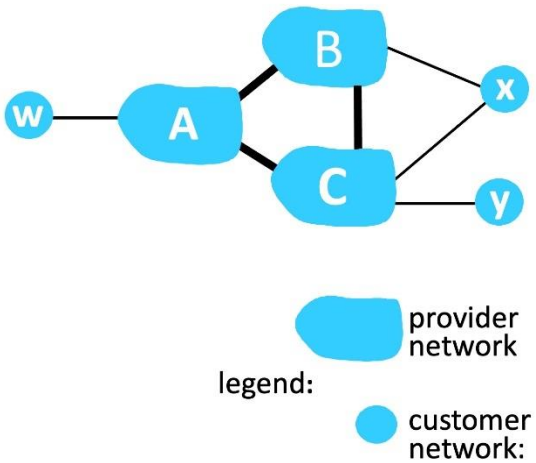
ROUTING WITHIN NETWORKS?

Among the following protocols, terminology or considerations, indicate those that are associated with "routing within a single network (typically owned and operated by one organization)."

- [ ] BGP
- [x] Driven more by performance than by routing policy
- [ ] Driven more by routing policy than end-end routing performance
- [x] OSPF
- [ ] inter-domain routing
- [x] intra-domain routing
- [x] intra-AS routing
- [ ] inter-AS routing

ATH ADVERTISEMENT AND POLICY (PART 1).

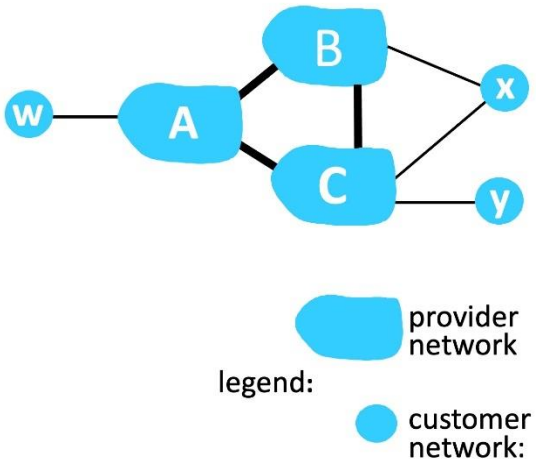
Suppose a provider network only wants to carry traffic to/from its customer networks (i.e., to provide no transit service), and customer networks only want to carry traffic to/from itself. Consider the figure below. To implement this policy, to which of the following networks would network C advertise the path Cy?



- [x] A
- [x] x
- [ ] w
- [x] B

PATH ADVERTISEMENT AND POLICY (PART 2).

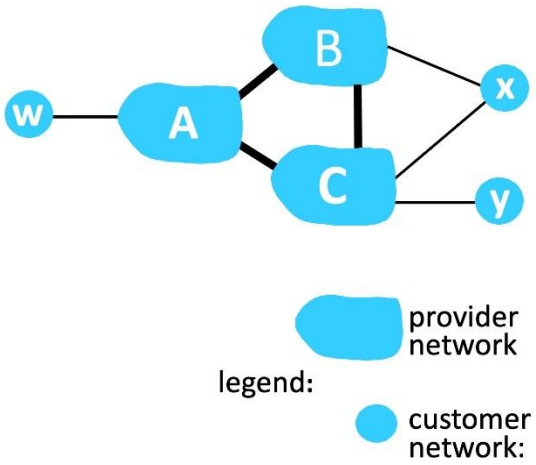
Again, suppose a provider network only wants to carry traffic to/from its customer networks (i.e., to provide no transit service), and customer networks only want to carry traffic to/from itself. Suppose C has advertised path Cy to A. To implement this policy, to which of the following networks would network A advertise the path ACy?



- [ ] C
- [ ] x
- [x] w
- [ ] B

PATH ADVERTISEMENT AND POLICY (PART 3).

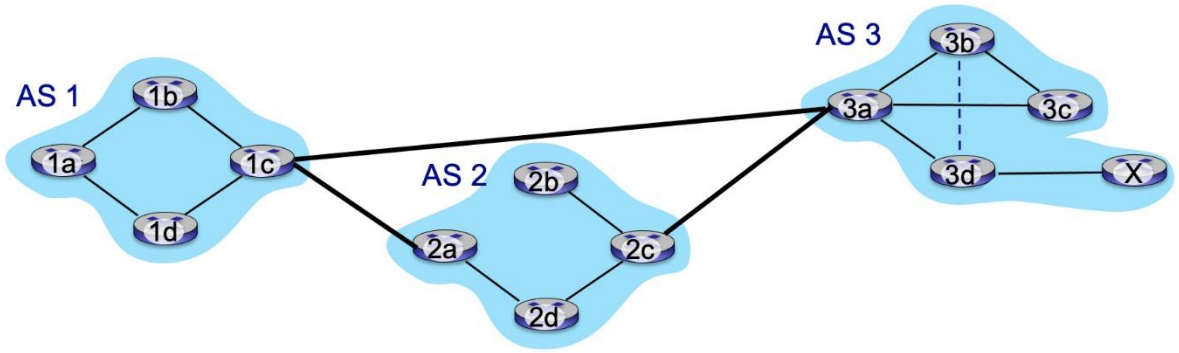
Again, suppose a provider network only wants to carry traffic to/from its customer networks (i.e., to provide no transit service), and customer networks only want to carry traffic to/from itself. Suppose C has advertised path Cy to x. To implement this policy, to which of the following networks would network x advertise the path xCy?



- [ ] B
- [ ] A
- [ ] C
- [ ] w
- [x] None of these other networks

EBGP OR IBGP?

Consider routers 2c and 2d in Autonomous System AS2 in the figure below. Indicate the flavor of BGP and the router from which each of 2c and 2d learns about the path to destination x.



QUESTION LIST:

How does router 2c learn of the path AS3, X to destination network X?

C

How does router 2d learn of the path AS3, X to destination network X?

A

ANSWER LIST:

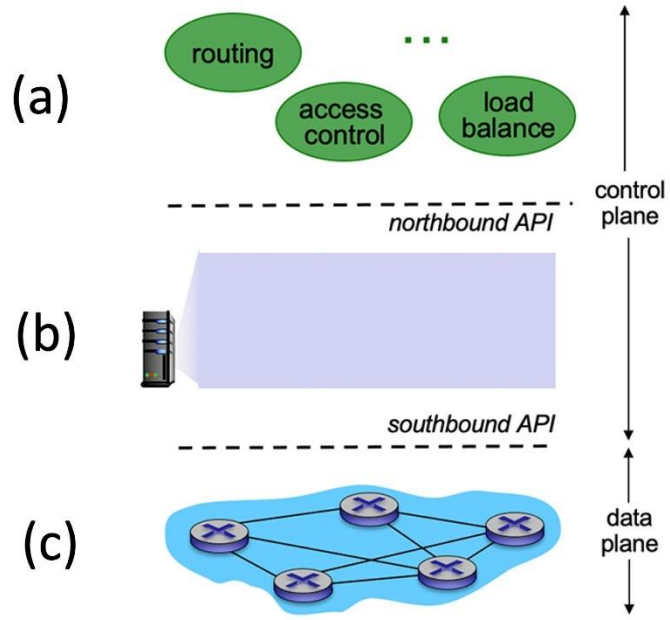
A. From 2c via iBGP.
B. From 3a via iBGP.
C. From 3a via eBGP.
D. From 2c via eBGP.
E. From x via eBGP.

5. **The SDN Control Plane**

KNOWLEDGE CHECKS

SDN LAYERS.

Consider the SDN layering shown below. Match each layer name below with a layer label (a), (b) or (c) as shown in the diagram.



QUESTION LIST:

SDN Controller (network operating system)

B

SDN-controlled switches

A

Network-control applications

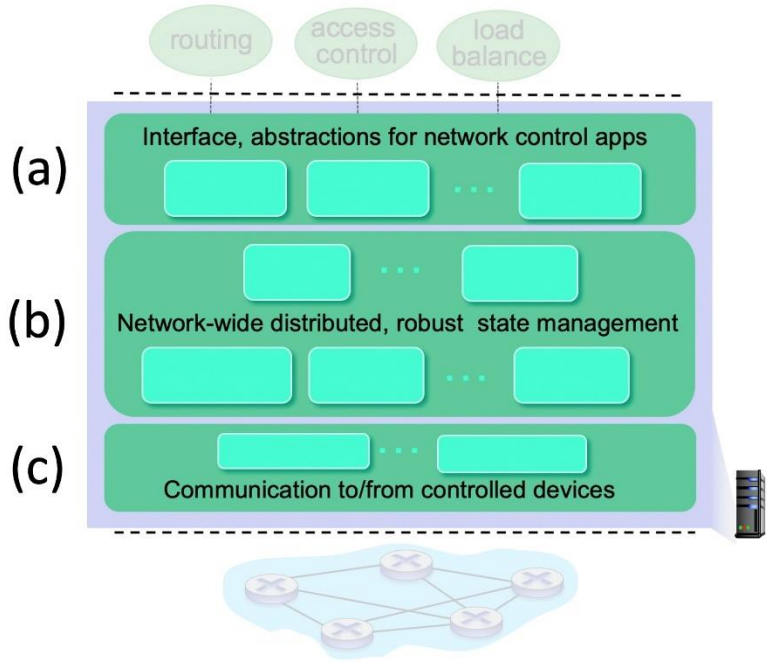
C

ANSWER LIST:

A. (c)
B. (b)
C. (a)

INTERNAL STRUCTURE OF THE SDN CONTROLLER (1).

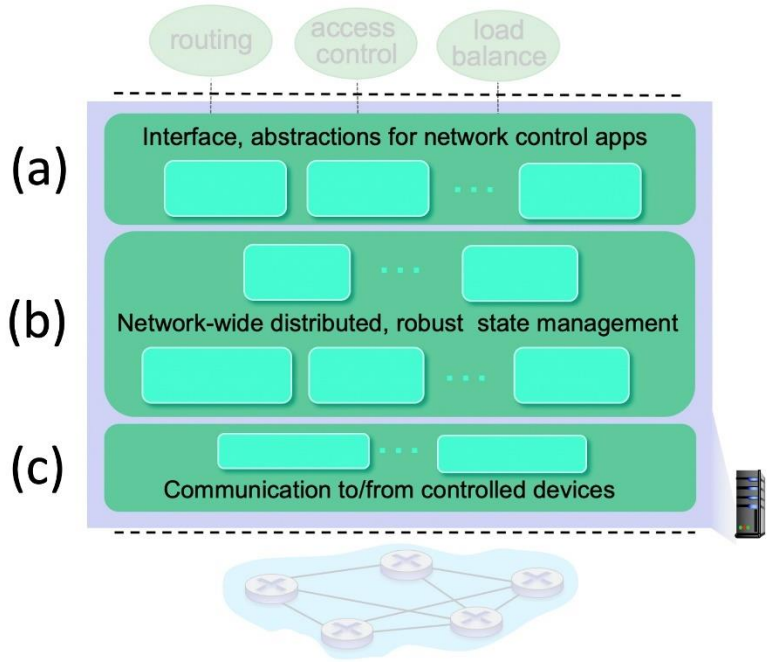
Which of the functions below belong in the controller layer labeled "Interface, abstractions for network control apps"? Check all below that apply.



- [ ] Link-state information
- [x] Network graph
- [x] Intent
- [ ] Host information
- [ ] Flow tables
- [ ] Switch information
- [ ] OpenFlow protocol
- [ ] Statistics

INTERNAL STRUCTURE OF THE SDN CONTROLLER (2).

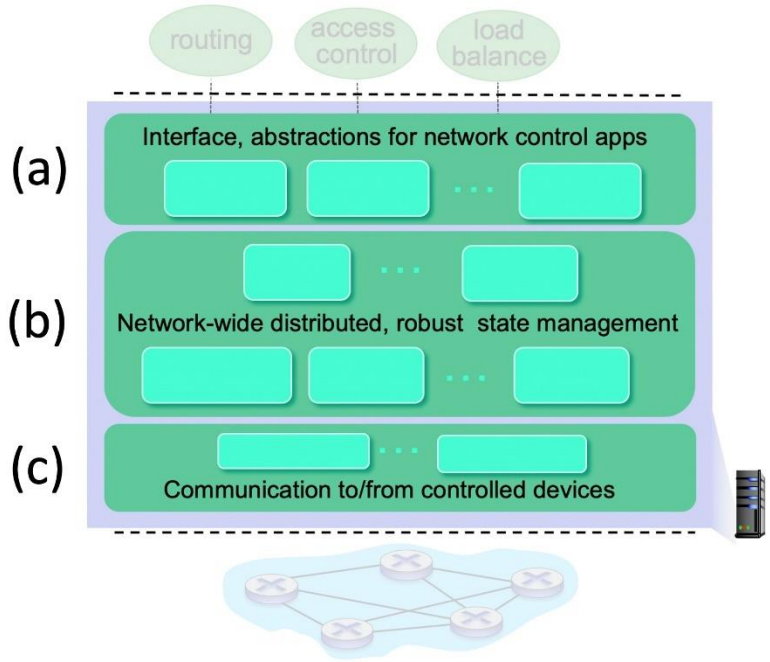
Which of the functions below belong in the controller layer labeled "Network-wide distributed, robust state management"? Check all below that apply.



- [x] Statistics
- [ ] OpenFlow protocol
- [ ] Intent
- [x] Flow tables
- [x] Switch information
- [x] Host information
- [ ] Network graph
- [x] Link-state information

INTERNAL STRUCTURE OF THE SDN CONTROLLER (3).

Which of the functions below belong in the controller layer labeled "Communication to/from controlled device"? Check all below that apply.



- [x] OpenFlow protocol
- [ ] Intent
- [ ] Network graph
- [ ] Switch information
- [ ] Flow tables
- [ ] Statistics
- [ ] Link-state information
- [ ] Host information

6. **ICMP: The Internet Control Message Protocol**

ICMP: INTERNET CONTROL MESSAGE PROTOCOL.

Which of the statements below about ICMP are true?

- [x] ICMP messages are carried directly in IP datagrams rather than as payload in UDP or TCP segments.
- [x] ICMP is used by hosts and routers to communicate network-level information.
- [x] The TTL-expired message type in ICMP is used by the traceroute program.
- [ ] ICMP communicates information between hosts and routers by marking bits in the IP header.
- [ ] ICMP messages are carried in UDP segments using port number 86.

CHAPTER 6: LINK LAYER

1. **Introduction to the Link Layer**

LINK-LAYER SERVICES.

Which of the following services may be implemented in a link-layer protocol? Select one or more statements.

- [x] Multiplexing down from / multiplexing up to a network-layer protocol.
- [x] Flow control between directly connected nodes.
- [x] Bit-level error detection and correction.
- [x] Coordinated access to a shared physical medium.
- [x] Reliable data transfer between directly connected nodes.
- [ ] TLS security (including authentication) between directly connected nodes.
- [ ] Lookup and forwarding on the basis of an IP destination address.
- [ ] End-end path determination through multiple IP routers.

---

2. **Error-Detection and -Correction Techniques**

TWO DIMENSIONAL PARITY.

Which of the following statements is true about a two-dimensional parity check (2D-parity) computed over a payload?

- [x] 2D-parity can detect any case of a single bit flip in the payload.
- [x] 2D-parity can detect and correct any case of a single bit flip in the payload.
- [ ] 2D-parity can detect and correct any case of two bit flips in the payload.
- [x] 2D-parity can detect any case of two bit flips in the payload.

---

3. **Multiple Access Links and Protocols**

CHANNEL PARTITIONING PROTOCOLS.

Which of the following statements is true about channel partitioning protocols?

- [ ] Channel partitioning protocol can achieve 100% utilization, in the case that there is only one node that always has frames to send
- [x] Channel partitioning protocols can achieve 100% channel utilization, in the case that all nodes always have frames to send.
- [ ] There can be simultaneous transmissions resulting in collisions.
- [x] There can be times when the channel is idle, when a node has a frame to send, but is prevented from doing so by the medium access protocol.

PURE ALOHA AND CSMA.

Which of the following statements is true about **both** Pure Aloha, and CSMA (both with and without collision detection?

- [ ] Pure Aloha and CSMA can achieve 100% channel utilization, in the case that all nodes always have frames to send.

☑ Pure Aloha and CSMA can achieve 100% utilization, in the case that there is only one node that always has frames to send

☐ There can be times when the channel is idle, when a node has a frame to send, but is prevented from doing so by the medium access protocol.

☑ There can be simultaneous transmissions resulting in collisions.

POLLING AND TOKEN-PASSING PROTOCOLS.

Which of the following statements is true about polling and token-passing protocols?

☑ These protocol can achieve close 100% utilization, in the case that there is only one node that always has frames to send (the fact that the utilization is close to, but not exactly, 100% is due to a small amount of medium access overhead but not due to collisions)

☑ These protocol can achieve close to 100% channel utilization, in the case that all nodes always have frames to send (the fact that the utilization is close to, but not exactly, 100% is due to a small amount of medium access overhead but not due to collisions)

☐ There can be times when the channel is idle for more than a short period of time, when a node has a frame to send, but is prevented from doing so by the medium access protocol.

☐ There can be simultaneous transmissions resulting in collisions.

CHARACTERISTICS OF MULTIPLE ACCESS PROTOCOLS (A).

Consider the following multiple access protocols that we've studied: (1) TDMA, and FDMA (2) CSMA (3) Aloha, and (4) polling. Which of these protocols are **collision-free** (e.g., collisions will never happen)?

☐ CSMA and CSMA/CD

☑ TDMA and FDMA

☐ Aloha

☑ Polling

CHARACTERISTICS OF MULTIPLE ACCESS PROTOCOLS (B).

Consider the following multiple access protocols that we've studied: (1) TDMA, and FDMA (2) CSMA (3) Aloha, and (4) polling. Which of these protocols requires some form of **centralized control** to mediate channel access?

- [x] Polling
- [ ] CSMA and CSMA/CD
- [ ] Aloha
- [x] TDMA and FDMA

CHARACTERISTICS OF MULTIPLE ACCESS PROTOCOLS (C).

Consider the following multiple access protocols that we've studied: (1) TDMA, and FDMA (2) CSMA (3) Aloha, and (4) polling. For which of these protocols is the maximum channel utilization 1 (or very close to 1)?

- [x] TDMA and FDMA
- [ ] CSMA and CSMA/CD
- [ ] Aloha
- [x] Polling

CHARACTERISTICS OF MULTIPLE ACCESS PROTOCOLS (D).

Consider the following multiple access protocols that we've studied: (1) TDMA, and FDMA (2) CSMA (3) Aloha, and (4) polling. For which of these protocols is there a maximum amount of time that a node knows that it will have to wait until it can successfully gain access to the channel?

- [x] Polling
- [ ] Aloha
- [ ] CSMA and CSMA/CD
- [x] TDMA and FDMA

4. **Switched Local Area Networks**

DIFFERENT TYPES OF ADDRESSING (A).

We've now learned about both IPv4 addresses and MAC addresses. Consider the address properties below, and use the pulldown menu to indicate which of these properties is *only* a property of MAC addresses (and therefore is **not** a property of IPv4 addresses - careful!).

- [x] This is a 48-bit address.
- [ ] This is a network-layer address.
- [x] This is a link-layer address.
- [ ] This address must be unique among all hosts in a subnet.
- [x] This address remains the same as a host moves from one network to another.
- [ ] This is a 32-bit address.
- [ ] This is a 128-bit address.
- [ ] This address is allocated by DHCP.

DIFFERENT TYPES OF ADDRESSING (B).

We've now learned about both IPv4 addresses and MAC addresses. Consider the address properties below, and use the pulldown menu to indicate which of these properties is *only* a property of IPv4 addresses (and therefore is **not** a property of MAC addresses - careful!).

- [x] This address is allocated by DHCP.
- [x] This is a 32-bit address.
- [ ] This is a link-layer address.
- [x] This is a network-layer address.
- [ ] This address must be unique among all hosts in a subnet.
- [ ] This is a 128-bit address.
- [ ] This address remains the same as a host moves from one network to another.
- [ ] This is a 48-bit address.

DIFFERENT TYPES OF ADDRESSING (C).

We've now learned about both IPv4 addresses and MAC addresses. Consider the address properties below, and use the pulldown menu to indicate which of these properties is a property of *both* IPv4 addresses *and* MAC addresses.

- [ ] This address remains the same as a host moves from one network to another.
- [x] This address must be unique among all hosts in a subnet.
- [ ] This is a link-layer address.
- [ ] This is a 48-bit address.
- [ ] This is a network-layer address.
- [ ] This address is allocated by DHCP.
- [ ] This is a 128-bit address.
- [ ] This is a 32-bit address.

FIELDS IN AN ETHERNET FRAME.

Use the pulldown menus below to match the name of the field with the function/purpose of a field within an Ethernet frame.

QUESTION LIST:

Cyclic redundancy check (CRC) field

G

Source address field

E

Data (payload) field

D

Type field.

F

Sequence number field

G

ANSWER LIST:

A. Used for flow control.
B. Used only to detect, but never correct, bit-level errors in the frame.
C. This field does not exist in the Ethernet frame
D. The contents of this field is typically (bit not always) a network-layer IP datagram.
E. 48-bit MAC address of the sending node.
F. Used to demultiplex the payload up to a higher level protocol at the receiver.
G. Used to detect and possibly correct bit-level errors in the frame.

SWITCH FORWARDING AND FILTERING.

Suppose an Ethernet frame arrives to an Ethernet switch, and the Ethernet switch does not know which of its switch ports leads to the node with the given destination MAC address? In this case, what does the switch do?

- Drop the frame without forwarding it.
- Choose a port randomly and forward the frame there.
- Flood the frame on all ports except the port on which the frame arrived.
- Use the address resolution protocol (ARP) to determine the appropriate outgoing port.

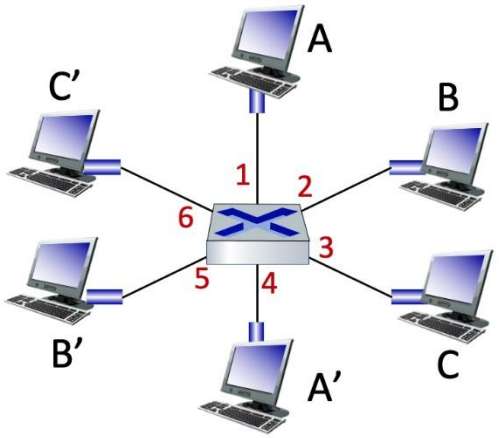
SELF-LEARNING SWITCHES.

Which of the following statements are true about a self learning switch?

- [x] A self-learning switch will age-out (forget) a self-learned association of a MAC address x and switch port y if it doesn't see a frame with MAC address x incoming on switch port y after some amount of time.
- [ ] A self-learning switch never forgets a self-learned association of a MAC address x and switch port y.
- [x] A self learning switch associates the source MAC address on an incoming frame with the port on which it arrived, and stores this matching in a table. The switch has now learned the port that leads to that MAC address.
- [x] A self-learning switch frees a network manager from a least one configuration task that might be associated with managing a switch

LEARNING SWITCH SCENARIO.

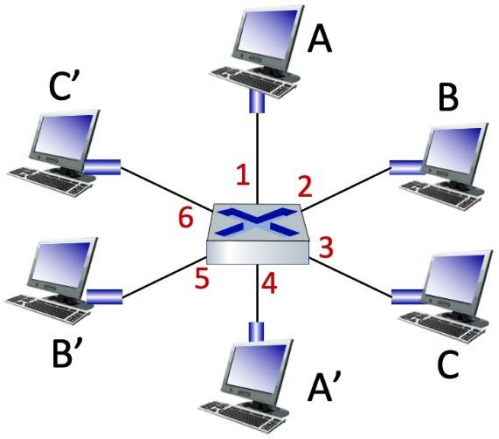
Consider the simple star-connected Ethernet LAN shown below, and suppose the Ethernet switch is a learning switch, and that the switch table is initially empty. Suppose C sends an Ethernet frame address to C' and C ' replies back to C. How many of these two frames are also received at B's interface?



- 2
- 0
- 1
- 4

LEARNING SWITCH STATE REMOVAL.

Consider the simple star-connected Ethernet LAN shown below, and suppose the switch table contains entries for each of the 6 hosts. How will those entries be removed from the switch table?



◉ An entry for a hostwill be removed if that host doesn't transmit any frames for a certain amount of time (that is, table entries will timeout).

○ The table entry can *only* be removed by the network manager, who would use the SNMP protocol to remove the entry.

○ They'll remain in the switch forever (or until it is re-booted).

○ A table entry for a host will be removed by the STPP (Switch Table Purge Protocol) which will be used by a host to signal the switch when it (the host) is shutting down or otherwise leaving the network.

MAC ADDRESSES (VERSUS OTHER TYPES OF ADDRESSES AND IDENTIFIERS).

Which of the following statements are true about MAC (link-layer) addresses? Select one or more statements below.

☐ A portion of the address bits are associated with the network to which the device is attached, and so changes as the device moves from one network to another.

☐ Is contained in a SIM card and used when a device identifies itself and connects to an LTE network.

☑ Generally does not change, and is associated with a device when it is manufactured/created.

☑ Generally stays unchanged as a device moves from one network to another.

☐ Has 32 bits.

☑ Has 48 bits.

CHAPTER 7: WIRELESS AND MOBILE NETWORKS

1. **Introduction**

HOW FAST IS THAT WIRELESS TECHNOLOGY?

Use the pulldown menus below to match the approximate transmission rate with the the wireless technology that achieves that rate. Of course, sender/receiver distance, noise and other factors determine actual transmission speed, so "your mileage may vary" (YMMV)

QUESTION LIST:

802.11 ax

D

5G celluar

D

802.11 ac

G

4G LTE

F

802.11 g

H

Bluetooth

B

ANSWER LIST:

A. 256 Kbps
B. 2 Mbps
C. 1 Tbps
D. 14 Gbps
E. 10 Gbps
F. hundreds of Mbps
G. 3.5 Gbps
H. 54 Mbps

INFRASTRUCTURE MODE.

What is meant when we say that a network of devices is operating in "infrastructure mode"?

- The mobile device is operating in a reduced power mode, forcing the network base station and routers to take on additional functionality that would normally be done by the mobile.
- Devices communicate with each other and to the larger outside world via a base station (also known as an access point).
- All network equipment, except the mobile devices, must be racked in a temperature-controlled and power-smoothed building.
- Network devices can communicate directly with each other, with no need for messages to be relayed through a base station. The devices are the "infrastructure".

---

2. **Wireless Links and Network Characteristics**

CHARACTERISTICS OF WIRELESS LINKS.

Which of the following statements about the characteristics of wireless links are true?

- [x] **Multipath propagation** occurs when portions of the electromagnetic wave reflect off objects and the ground taking paths of different lengths between the sender and a receiver, and thus arriving at the receiver at slightly different points in time.
- [ ] The "hidden terminal problem" refers to the fact that many people can never seem to find their mobile phones.
- [x] The "hidden terminal problem" happens when A sends to B over a wireless channel, and an observer, C (that can be even closer to A than B), does not detect/receive A's transmission because of physical obstacles in the path between A and C.
- [ ] The **"hidden terminal problem"** happens when A sends to B over a wireless channel, and an observer, C (that can be even closer to A than B), does not detect/receive A's transmission because of **physical obstacles** in the path between A and B.
- [ ] **Path loss** refers to the dropping of link-layer frames that are being relayed among wireless access points due to buffer overflow, just as network-layer datagrams are dropped at routers with full buffers.
- [ ] The **"hidden terminal problem"** happens when A sends to B over a wireless channel, and an observer, C (that is further away from A than B), does not detect/receive A's transmission because the **signal strength** of A's transmission has **faded** significantly by the time it reaches C.
- [ ] The **bit error rate (BER)** of a wireless channel *increases* as the **signal-to-noise ratio (SNR)** increases.
- [ ] **Multipath propagation** occurs when a sender sends multiple copies of a frame to a receiver, which is relayed over different by base stations or other wireless devices to the receiver.
- [x] The **bit error rate (BER)** of a wireless channel *decreases* as the **signal-to-noise ratio (SNR)** increases.

☐ **Path loss** refers to link-layer frames that are corrupted due to the higher bit error rates in wireless channels.

☑ **Path loss** refers to the decrease in the strength of a radio signal as it propagates through space.

---

3. **WiFi: 802.11 Wireless LANs**

BEACON FRAMES.

What is the purpose of a beacon frame in WiFi (802.11) networks?

○ A beacon frame allows a mobile node to determine the direction in which it should move in order to obtain an increasing signal strength.
◉ A beacon frame allows an access point to advertise its existence, and the frequency channel it is operating on, to devices that want to connect to an access point.
○ A beacon frame allows a node with a directional antenna to aim the antenna towards the beacon point to maximize the quality of the send and receive signal.
○ A beacon frame allows a mobile device to signal that it is ready to receive a frame.

USE OF ACKS IN WIFI.

Why are link-layer ACKs used in WiFi (802.11) networks? [Hint: check two of the boxes below].

☑ Because of the hidden terminal problem, a node that is transmitting and hears no collisions still doesn't know if there was a collision at the receiver.
☑ Wireless links are noisier than wired links, and so bit level errors are more likely to occur, making link-layer error recovery more valuable that in less-noisy wired links.
☐ Hearing a receiver ACK, all other stations will stop transmitting. This reduces collisions.
☐ The sender can used the differences in the signal strength in an ACK to infer whether the receiver is moving towards, or away from, the sender

---

WHY THREE ADDRESSES?

Why does the WiFi (802.11) link-layer frame have three addresses? [Note: WiFi actually has four MAC addresses in the frame, but we're only focusing here on the three widely used ones].

○ Because there may be two hosts or routers that are possible destinations for this link-layer frame and we need to identify which of these is the intended receiver.
○ Because the *sender* of this frame can be either the access point or a link-layer host or router interface, and we need to identify which of these two is the sender.
◉ Because both the access point that will relay this frame to the intended link-layer receiving host or router interface, as well as that intended destination host or router interface need to be specified.

RTS/CTS FRAMES.

What is the purpose of RTS (request to send) and CTS (clear to send) frames in WiFi (802.11) networks? Select one or more of the answers below. [Hint: check two answers below].

☐ A CTS allows a receiver to let the sender (who sent that RTS) know that it (the receiver) has enough buffers to hold a frame transmitted by that sender

☑ RTC/CTS frames helps nodes in a wireless network mitigate the effects of the hidden terminal problem.

☑ A CTS that is sent allows a receiver to force other nodes (other than the intended sender who sent the RTS) to refrain from transmitting, thus allowing the sender who sent the RTS to then transmit a frame with less likelihood of a collision.

☐ RTC/CTS frames allow a sender to gather CTS frames from all other network nodes, so that it knows it can then send without collisions.

THE 802.11 MEDIA ACCESS CONTROL PROTOCOL.

Which of the following statement are true about the 802.11 (WiFi) MAC protocol?

○ The 802.11 MAC protocol performs **collision avoidance.** That is, an 802.11 sender and receiver can use approaches such as RTS/CTS, inter-frame spacing, and explicit acknowledgments to try avoid, rather than detect, colliding transmissions from another node.

○ The 802.11 MAC protocol performs **collision detection.** That is, an 802.11 sender will listen to the channel while it is transmitting, and stop transmitting when it detects a colliding transmission from another node.

○ The 802.11 MAC protocol performs **carrier sensing**. That is, it listens before transmitting and will only transmit if the channel is sensed idle.

BLUETOOTH.

Which of the following statement are true about the Bluetooth protocol?

○ Bluetooth transmits all frames in the same frequency band.

○ Bluetooth transmission rates can be as high as in WiFi networks.

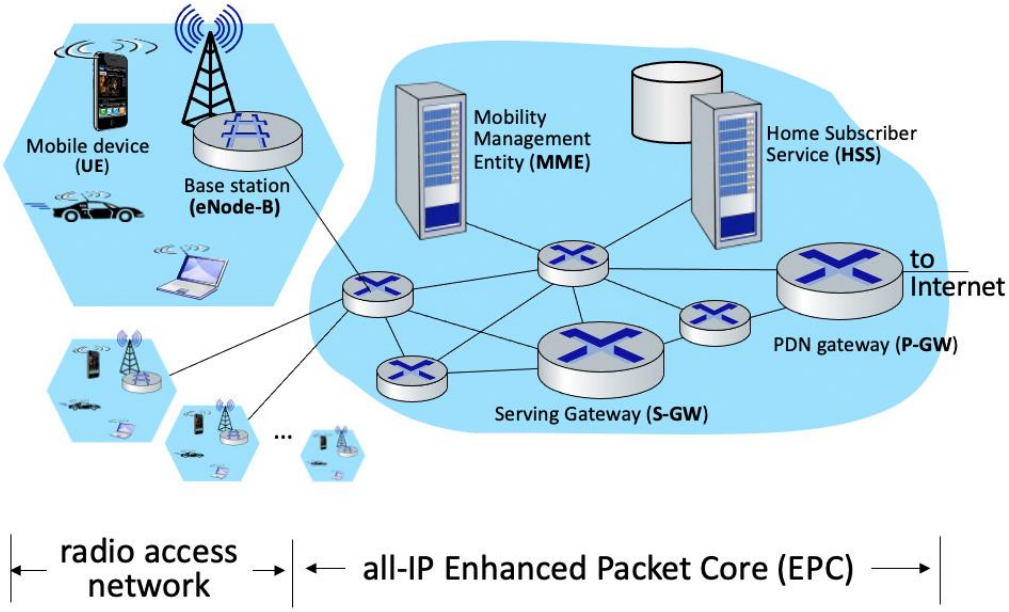
○ Bluetooth networks have a centralized controller that serves to coordinate the various client devices in a Bluetooth piconet.

○ Bluetooth uses TDM, FDM, polling, error detection and correction, and has sleep modes to conserve device power. Pretty sophisticated for a consumer technology!

4. **Cellular Networks: 4G and 5G**

ELEMENTS OF 4G ARCHITECTURE.

Match the function of an element in the 4G LTE architecture with its name, using the pulldown menus.



QUESTION LIST:

Located in a mobile device's home network, this element provides authentication, access privileges in home and visited networks.

G

This router in a cellular carrier's network, coordinates packet forwarding and routing to outside the carrier's network.

B

This element coordinates mobile device services - authentication, mobility management - for a mobile resident in that network.

C

This element is on the network side of wireless link into the LTE network.

A

This element is the wireless link between mobile device and a base station

E

ANSWER LIST:

A. Base Station (eNode-B)
B. Serving Gateway (S-GW)
C. Mobility Management Entity (MME)
D. PDN-Gateway (P-GW)
E. Radio Access Network (RAN)
F. Mobile device
G. Home Subscriber Server (HSS)

IMSI.

In 4G LTE cellular systems, what is an International Mobile Subscriber Identity (IMSI)?

○ Assigned by a mobile carrier network to a device, when the device attaches to the radio access network, serving a similar link-layer role as MAC addresses in a wired network.

○ A 64-bit identifier that identifies the cellular network to which an mobile subscriber is attaching. Somewhat analogous to the Autonomous System (AS) number used in BGP to identify/name networks.

○ A fancy name for a globally unique phone number, including country code.

◉ A 64-bit identifier stored on a cellular SIM (Subscriber Identity Module) card that identifies the subscriber in the worldwide cellular carrier network system.

COMPARING THREE WIRELESS NETWORK TYPES.

Consider three wireless networks that we learned about: WiFi (802.11), 4G LTE, and Bluetooth. Match each of these types of networks to a characteristic on the right.

QUESTION LIST:

WiFi (802.11)

A

4G/LTE

C

Bluetooth

B

ANSWER LIST:

A. Has the maximum link capacity (i.e., can deliver more bits/sec to the edge device).
B. Consumes the least amount of power.
C. Can provide the farthest coverage (i.e., longest range wireless communication) from a base station.

POWER CONSERVING “SLEEP MODES”.

Which of the following statements is true about “sleep modes” that allow a wireless device to “sleep” and occasionally “wake up” as a technique for saving battery life?

- (•) Both WiFi and LTE provide sleep modes.
- ( ) Neither WiFi nor LTE provide sleep modes.
- ( ) LTE provides sleep modes but WiFi does not.
- ( ) WiFi provides sleep modes but LTE does not.

CONNECTING 4G CELLULAR NETWORKS TOGETHER.

Which of the following statements is true about how 4G cellular networks (operated by different carriers/companies) connect together?

- ( ) In a 4G network, the radio access network connects to the legacy phone network for voice calls, but to the public Internet for data connections.
- ( ) 4G networks connect to each other using the existing phone interconnection networks from earlier 3G and 2G networks.
- (•) 4G networks are generally all-IP, and so cellular networks interconnect (peer) directly to each other, or peer at the cellular equivalents of the Internet Exchange Points that we saw used for interconnecting wired networks in the public Internet.

RELIABLE DATA TRANSFER AT THE LINK LAYER.

Which of the following statements is true about the link-level service of reliable data transfer (using ACKs) in WiFi (802.11) networks and in 4G cellular networks?

- (•) Both WiFi and LTE provide link-level reliable data transfer.
- ( ) WiFi provides link-level reliable data transfer but LTE does not.
- ( ) Neither WiFi nor LTE provide link-level reliable data transfer.
- ( ) LTE provides link-level reliable data transfer but WiFi does not.