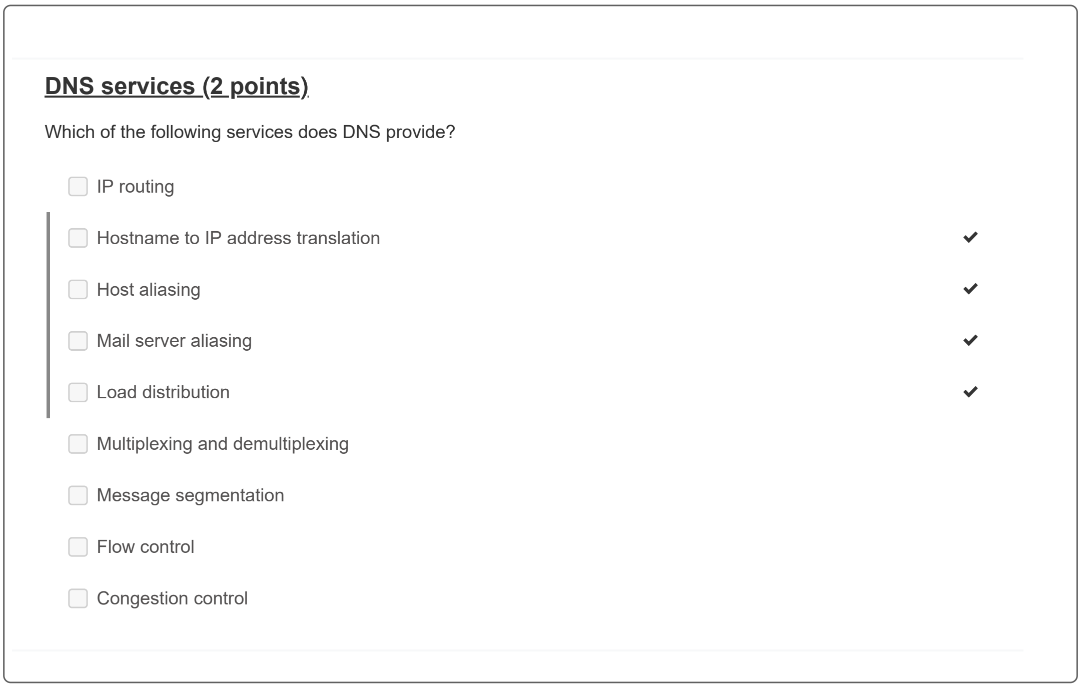
Item 1



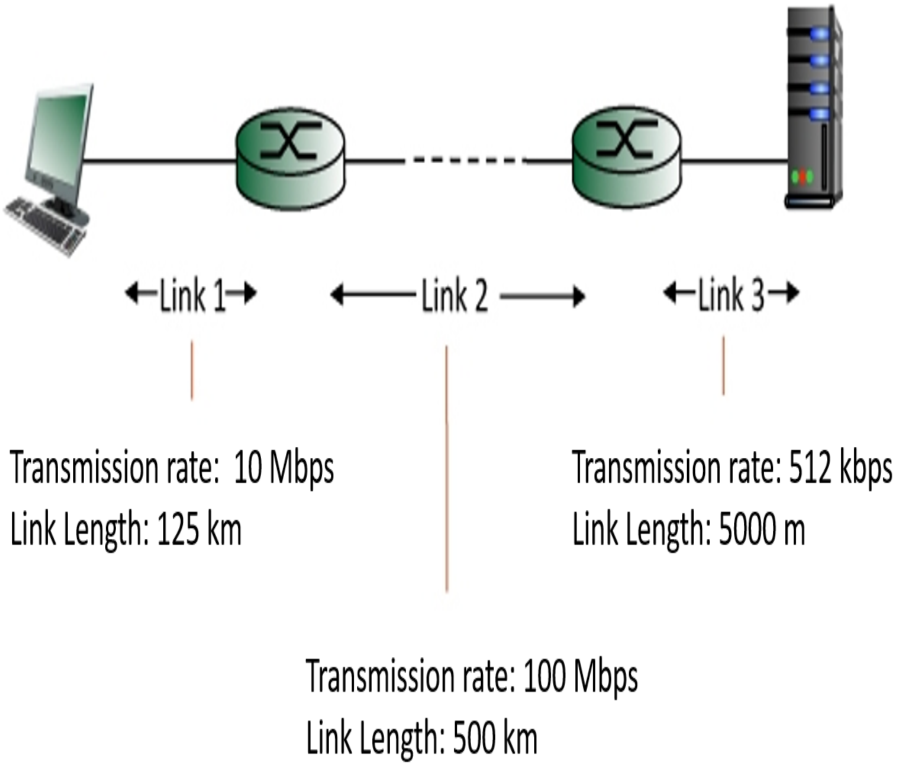
DNS services (2 points)

Which of the following services does DNS provide?

- □ IP routing
- □ Hostname to IP address translation ✓
- □ Host aliasing ✓
- □ Mail server aliasing ✓
- □ Load distribution ✓
- □ Multiplexing and demultiplexing
- □ Message segmentation
- □ Flow control
- □ Congestion control

Item 2

Delays (5 points)


Link 1
Link 2
Link 3
Transmission rate: 10 Mbps
Link Length: 125 km
Transmission rate: 512 kbps
Link Length: 5000 m
Transmission rate: 100 Mbps
Link Length: 500 km

Find the end-to-end delay (including the transmission delays and propagation delays on each of the three links, but ignoring queueing delays and processing delays) from when the left host begins transmitting the first bit of a packet to the time when the last bit of that packet is received at the server at the right. The speed of light propagation delay on each link is 3x10^8 m/sec. Assume a packet length of 1000 bytes.

Fill in your answers in milliseconds (ms) with 2 decimal places (e.g. 1234.56).

(This question gives 5 points in total - partial points are given for parts that are answered correctly)

Link 1 transmission delay = 1 □ ms

Link 1 propagation delay = 2 □ ms

Link 2 transmission delay = 3 □ ms

Link 2 propagation delay = 4 □ ms

Link 3 transmission delay = 5 □ ms

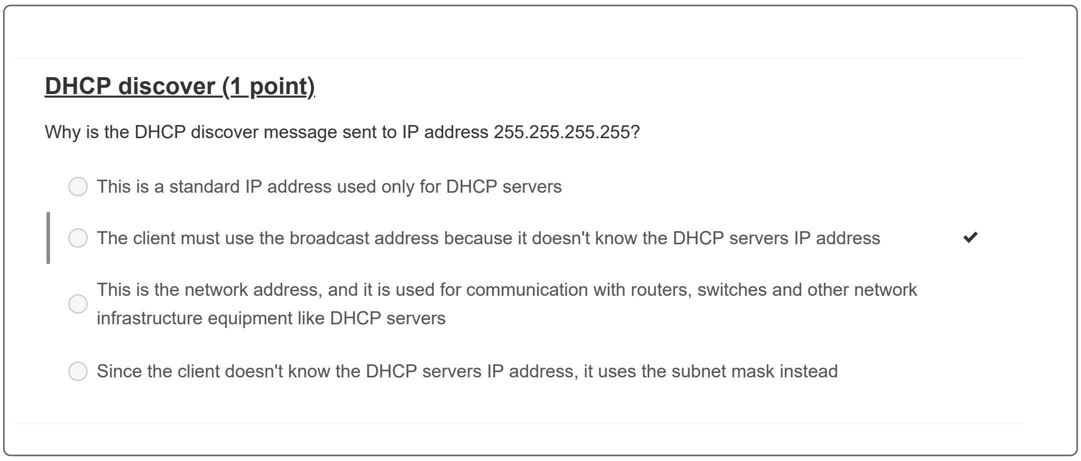
Link 3 propagation delay = 6 □ ms

Thus, the total end-to-end delay is the sum of these six delays: 7 □ ms.

Correct answers:

1 0.80 2 0.42 3 0.08 4 1.67 5 15.63 6 0.02 7 18.61

Item 3



DHCP discover (1 point)

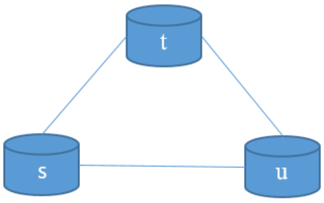
Why is the DHCP discover message sent to IP address 255.255.255.255?

- ○ This is a standard IP address used only for DHCP servers
- ○ The client must use the broadcast address because it doesn't know the DHCP servers IP address ✓
- ○ This is the network address, and it is used for communication with routers, switches and other network infrastructure equipment like DHCP servers
- ○ Since the client doesn't know the DHCP servers IP address, it uses the subnet mask instead

Item 4

Routing algorithm - Distance Vector (5 points)

The routers in the autonomous system below runs a distance vector routing algorithm.
The initial tables are shown for the three routers.



S	s	t	u		T	s	t	u		U	s	t	u
s	0	8	4		s	∞	∞	∞		s	∞	∞	∞
t	∞	∞	∞		t	8	0	3		t	∞	∞	∞
u	∞	∞	∞		u	∞	∞	∞		u	4	3	0

Show and calculate the Bellman-Ford equations.

$D_s(t) = \min(c(s,t) + D_t(t)\,,\ c(s,u) + D_u(t))$ $=$ min(1 + 2 , 3 + 4) = 5

$D_s(u) = \min(c(s,t) + D_t(u)\,,\ c(s,u) + D_u(u))$ $=$ min(6 + 7 , 8 + 9) = 10

Correct answers:

1	2	3	4	5	6	7	8	9	10
8	0	4	3	7	8	3	4	0	4

Distance Vector table:

Fill in the routing table in router s, as it looks like **after** the network has converged. Routers do **not** use poisened reverse.

S	s	t	u
s	1	2	3
t	4	5	6
u	7	8	9

Correct answers:

1	2	3	4	5	6	7	8	9
0	7	4	7	0	3	4	3	0

Item 5

Create Subnets (5 points)

An ISP has assigned the following IP range to your organisation

196.4.16.0/24

Give the binary representation of the IP address: 1 2
3 4

Give the binary representation of the subnet mask: 5 6
7 8

Correct answers:

1 11000100 2 00000100 3 00010000 4 00000000 5 11111111 6 11111111

7 11111111 8 00000000

Create subnet:

3 subnets are required; one for 2 hosts, one for 125 hoste and one for 65 hosts.

Notice: There are two equally correct solutions. Just show the one you prefer.

What will the network address of each subnet be? Use CIDR format (x.x.x.x/y).

Subnet	Network address
2 hosts	1 / 2
125 hosts	3 / 4
65 hosts	5 / 6

Correct answers:

1 196.4.16.0 2 30 3 196.4.16.128 4 25 5 196.4.16.0 6 25

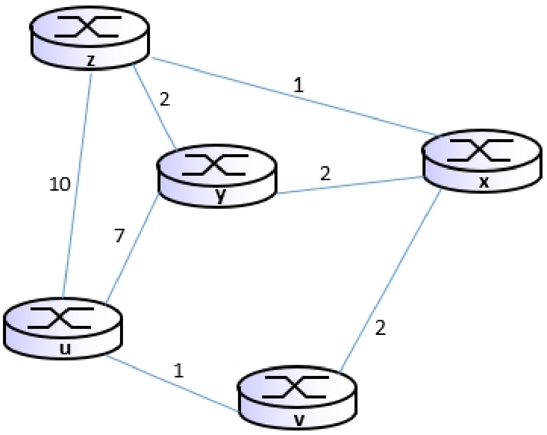
Item 6

Routing Algorithm - Link State (5 points)

Consider the following graph model of an Autonomous System.

With the indicated link costs, use Dijkstra's shortest-paht algorithm to compute the shortest path from **v** to all other network nodes.

NOTICE: Only fill in fields that change.



u v x y z 1 2 3 4 5

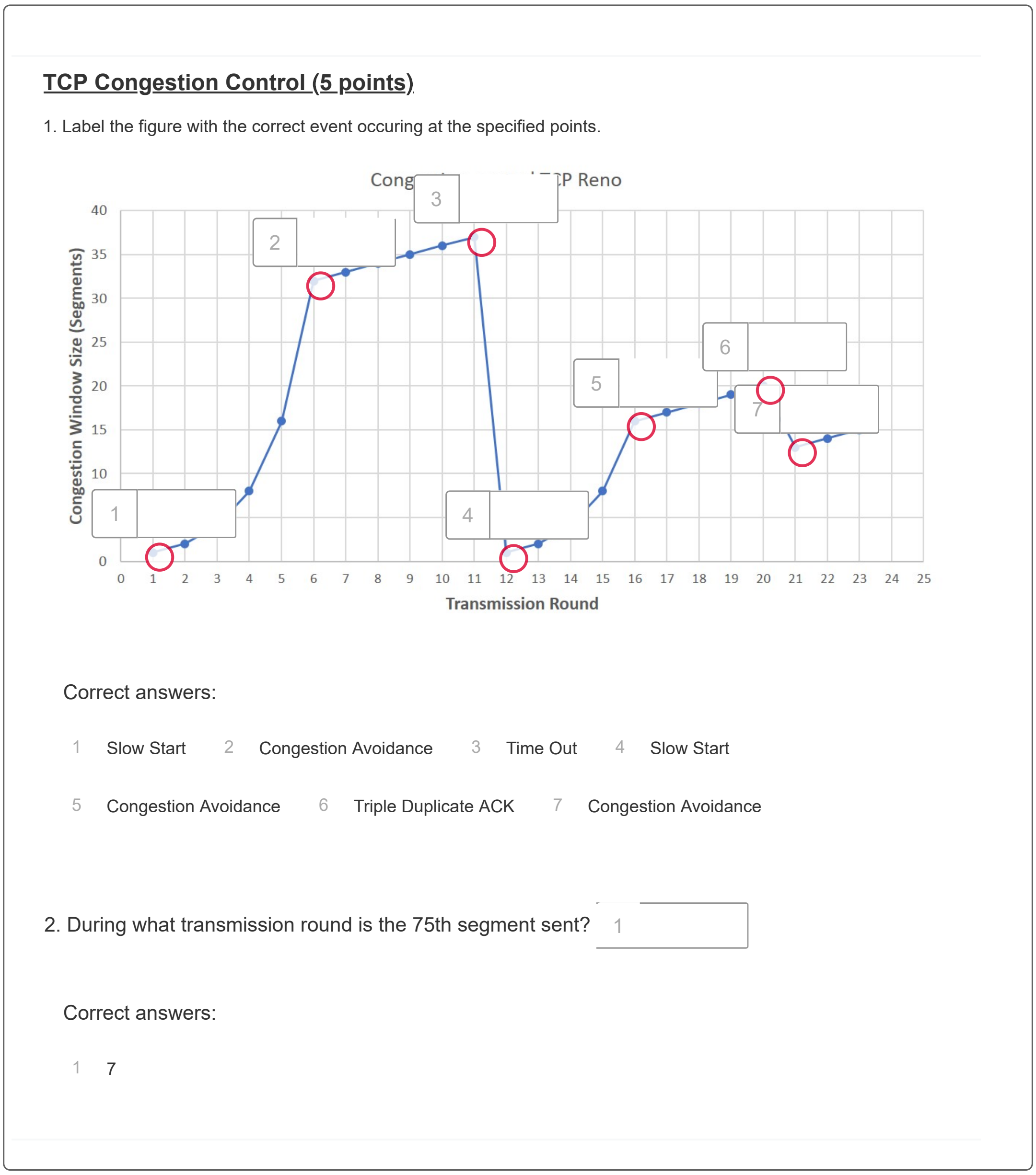
6 7 8 9 10 11 ∞

Iteration	Node added to N'	D(u),p(u)	D(z),p(z)	D(x),p(x)	D(y),p(y)
0	v	1 , v	2 ,v	3 ,v	4 ,v
1	5	6 7	8 9	10 11	12 13
2	14	15 16	17 18	19 20	21 22
3	23	24 25	26 27	28 29	30 31
4	32	33 34	35 36	37 38	39 40

Correct answers:

1	1	2	∞	3	2	4	∞	5	u	6		7		8	11	9	u	10	
11		12	8	13	u	14	x	15		16		17	3	18	x	19		20	
21	4	22	x	23	z	24		25		26		27		28		29		30	
31		32	y	33		34		35		36		37		38		39		40	

Item 7



TCP Congestion Control (5 points)

1. Label the figure with the correct event occuring at the specified points.

Correct answers:

1 Slow Start 2 Congestion Avoidance 3 Time Out 4 Slow Start

5 Congestion Avoidance 6 Triple Duplicate ACK 7 Congestion Avoidance

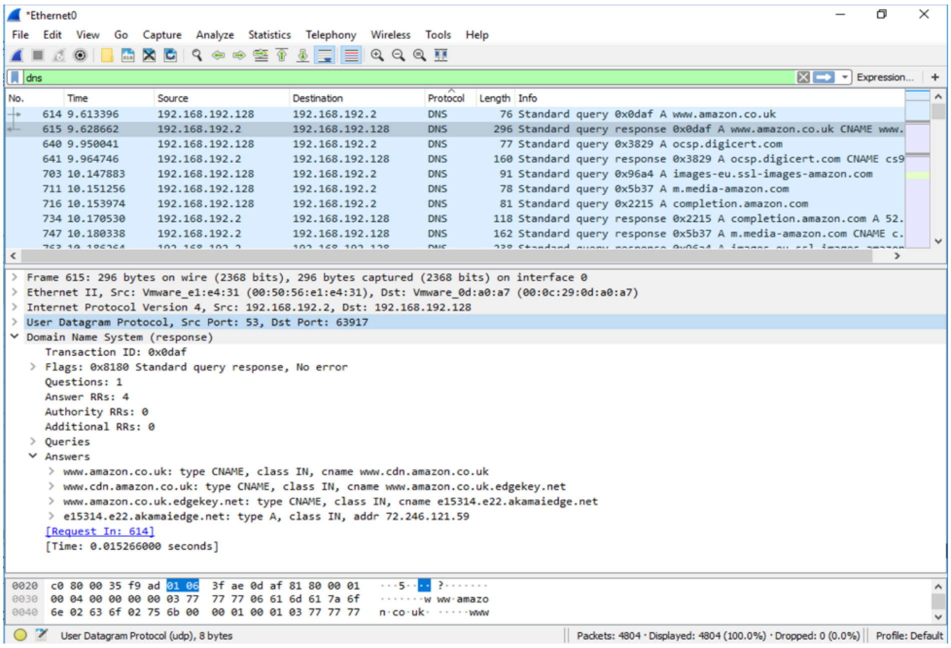
2. During what transmission round is the 75th segment sent? 1

Correct answers:

1 7

Item 8

Wireshark (5 points)



*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...

```
No.   Time        Source           Destination      Protocol Length Info
  614 9.613396    192.168.192.128  192.168.192.2    DNS        76 Standard query 0x0daf A www.amazon.co.uk
  615 9.628662    192.168.192.2    192.168.192.128  DNS       296 Standard query response 0x0daf A www.amazon.co.uk CNAME www.
  640 9.950041    192.168.192.128  192.168.192.2    DNS        77 Standard query 0x3829 A ocsp.digicert.com
  641 9.964746    192.168.192.2    192.168.192.128  DNS       160 Standard query response 0x3829 A ocsp.digicert.com CNAME cs9
  703 10.147883   192.168.192.128  192.168.192.2    DNS        91 Standard query 0x96a4 A images-eu.ssl-images-amazon.com
  711 10.151256   192.168.192.128  192.168.192.2    DNS        78 Standard query 0x5b37 A m.media-amazon.com
  716 10.153974   192.168.192.128  192.168.192.2    DNS        81 Standard query 0x2215 A completion.amazon.com
  734 10.170530   192.168.192.2    192.168.192.128  DNS       118 Standard query response 0x2215 A completion.amazon.com A 52.
  747 10.180338   192.168.192.2    192.168.192.128  DNS       162 Standard query response 0x5b37 A m.media-amazon.com CNAME c.
```

```
> Frame 615: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface 0
> Ethernet II, Src: Vmware_e1:e4:31 (00:50:56:e1:e4:31), Dst: Vmware_0d:a0:a7 (00:0c:29:0d:a0:a7)
> Internet Protocol Version 4, Src: 192.168.192.2, Dst: 192.168.192.128
> User Datagram Protocol, Src Port: 53, Dst Port: 63917
v Domain Name System (response)
    Transaction ID: 0x0daf
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > www.amazon.co.uk: type CNAME, class IN, cname www.cdn.amazon.co.uk
    > www.cdn.amazon.co.uk: type CNAME, class IN, cname www.amazon.co.uk.edgekey.net
    > www.amazon.co.uk.edgekey.net: type CNAME, class IN, cname e15314.e22.akamaiedge.net
    > e15314.e22.akamaiedge.net: type A, class IN, addr 72.246.121.59
    [Request In: 614]
    [Time: 0.015266000 seconds]
```

```
0020  c0 80 00 35 f9 ad 01 06  3f ae 0d af 81 80 00 01   ···5····?·······
0030  00 04 00 00 00 00 03 77  77 77 06 61 6d 61 7a 6f   ·······w ww·amazo
0040  6e 02 63 6f 02 75 6b 00  00 01 00 01 03 77 77 77   n·co·uk· ·····www
```

User Datagram Protocol (udp), 8 bytes | Packets: 4804 · Displayed: 4804 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

1. Is the first listed DNS message in the Wireshark trace below (No. 614) a query or a response?

1

Correct answers:

1 Query

2. What “Type” of DNS query is the first listed DNS message?

3. What is the IP address used by the client computer (source)? 1

Correct answers:

1 192.168.192.128

4. What is the IP address used by the the server (destination) (1 point)?

1

Correct answers:

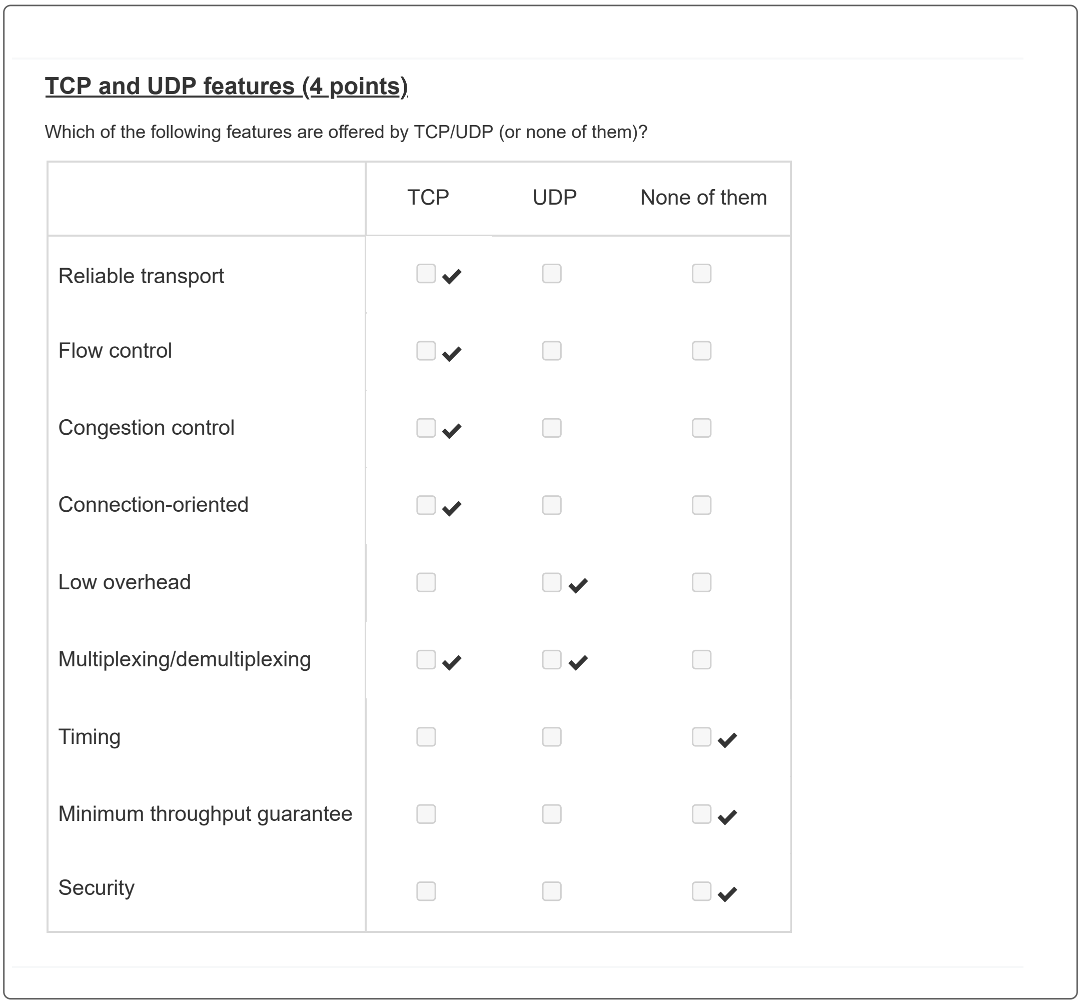
1 192.168.192.2

5. What is the source port of DNS response message? 1

Correct answers:

1 53

Item 9



TCP and UDP features (4 points)

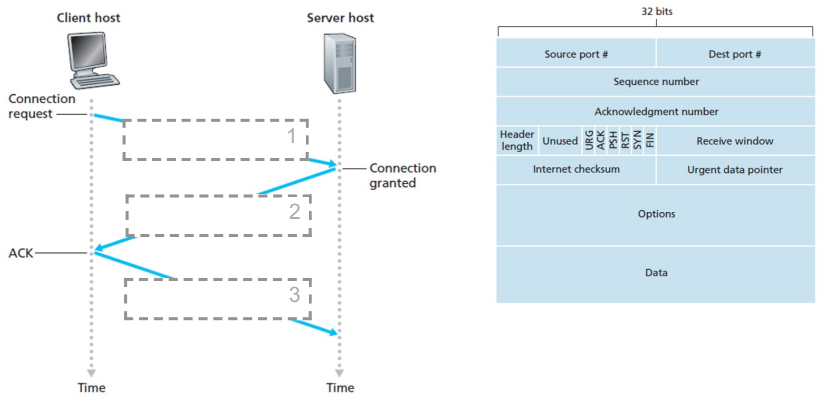
Which of the following features are offered by TCP/UDP (or none of them)?

	TCP	UDP	None of them
Reliable transport	□ ✓	□	□
Flow control	□ ✓	□	□
Congestion control	□ ✓	□	□
Connection-oriented	□ ✓	□	□
Low overhead	□	□ ✓	□
Multiplexing/demultiplexing	□ ✓	□ ✓	□
Timing	□	□	□ ✓
Minimum throughput guarantee	□	□	□ ✓
Security	□	□	□ ✓

Item 10

TCP 3-way handshake (4 points)

1. TCP performs a 3-way handshake when it establishes a connection. In each of the phases of the connection establishment, TCP sets the SYN and ACK bits in the TCP header. Drag and drop the correct values of each of the bits in the 3 phases of the TCP handshake in the figure below.



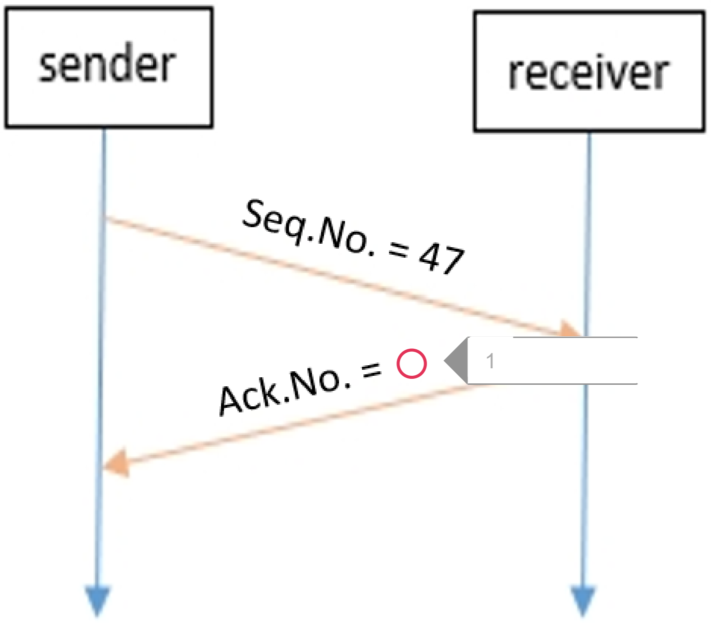
SYN=0 SYN=1 ACK=0 ACK=1

Correct answers:

1 SYN=1 ACK=0 2 SYN=1 ACK=1 3 SYN=0 ACK=1

2. The sender and receiver shown in the figure are establishing a TCP connection and are exchanging data for the connection setup (3-way handshake). The sender has chosen the initial sequence number to be 47.

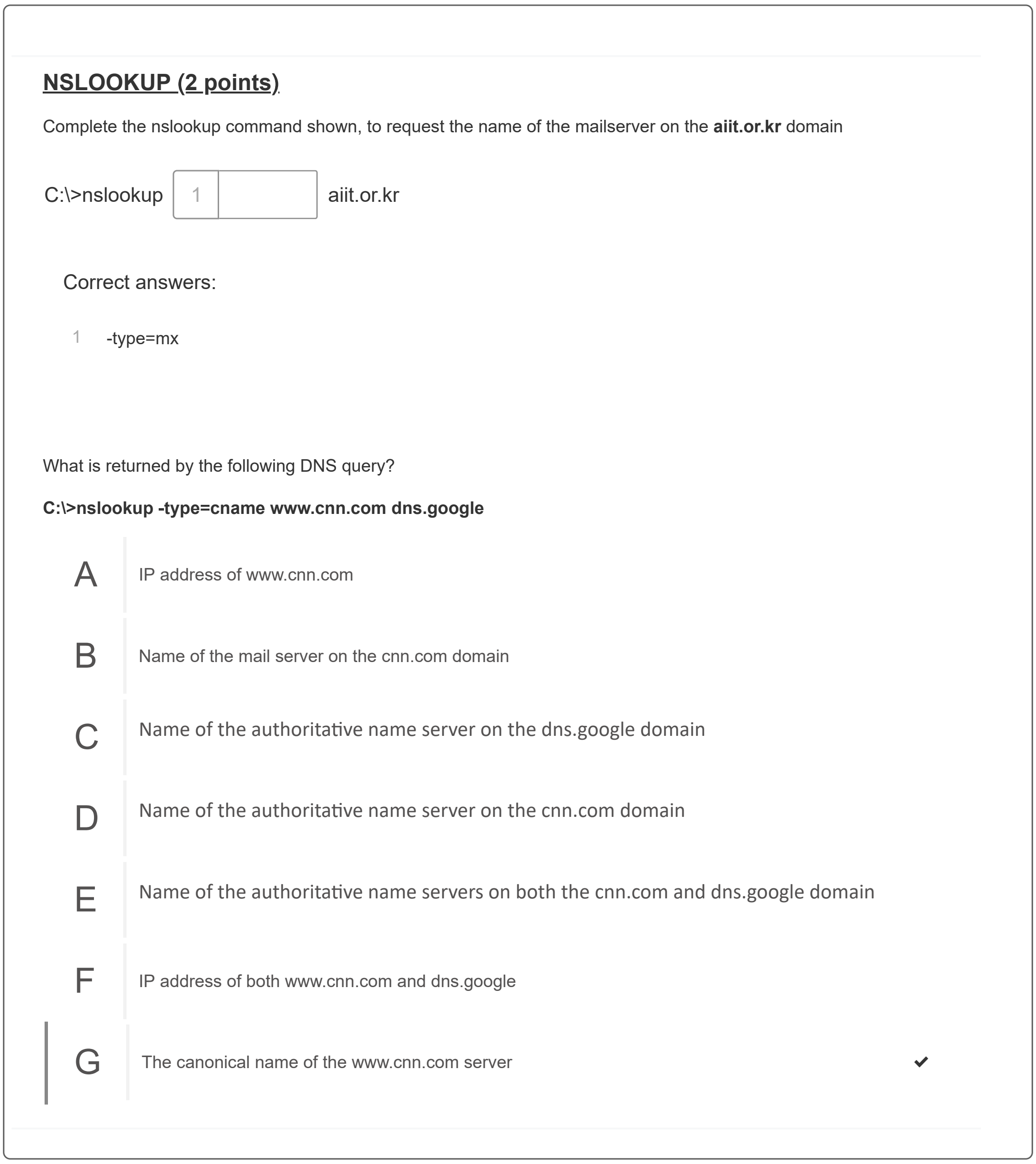
What is the Acknowledgement Number on the segment returned from the receiver?



Correct answers:

1 48

Item 11



NSLOOKUP (2 points)

Complete the nslookup command shown, to request the name of the mailserver on the **aiit.or.kr** domain

C:\>nslookup 1 aiit.or.kr

Correct answers:

1 -type=mx

What is returned by the following DNS query?

C:\>nslookup -type=cname www.cnn.com dns.google

A IP address of www.cnn.com

B Name of the mail server on the cnn.com domain

C Name of the authoritative name server on the dns.google domain

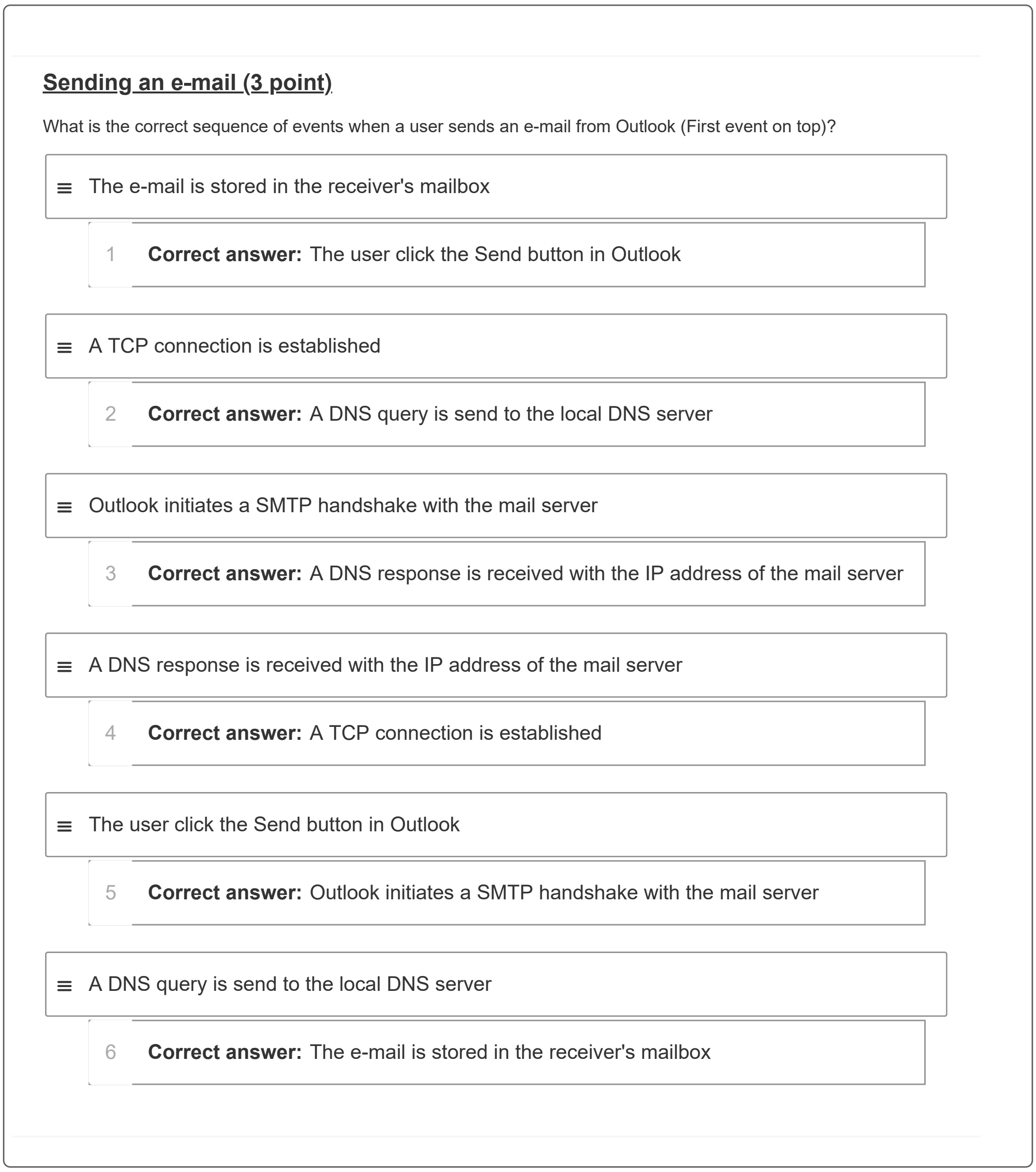
D Name of the authoritative name server on the cnn.com domain

E Name of the authoritative name servers on both the cnn.com and dns.google domain

F IP address of both www.cnn.com and dns.google

G The canonical name of the www.cnn.com server ✓

Item 12



Sending an e-mail (3 point)

What is the correct sequence of events when a user sends an e-mail from Outlook (First event on top)?

≡ The e-mail is stored in the receiver's mailbox

1 **Correct answer:** The user click the Send button in Outlook

≡ A TCP connection is established

2 **Correct answer:** A DNS query is send to the local DNS server

≡ Outlook initiates a SMTP handshake with the mail server

3 **Correct answer:** A DNS response is received with the IP address of the mail server

≡ A DNS response is received with the IP address of the mail server

4 **Correct answer:** A TCP connection is established

≡ The user click the Send button in Outlook

5 **Correct answer:** Outlook initiates a SMTP handshake with the mail server

≡ A DNS query is send to the local DNS server

6 **Correct answer:** The e-mail is stored in the receiver's mailbox

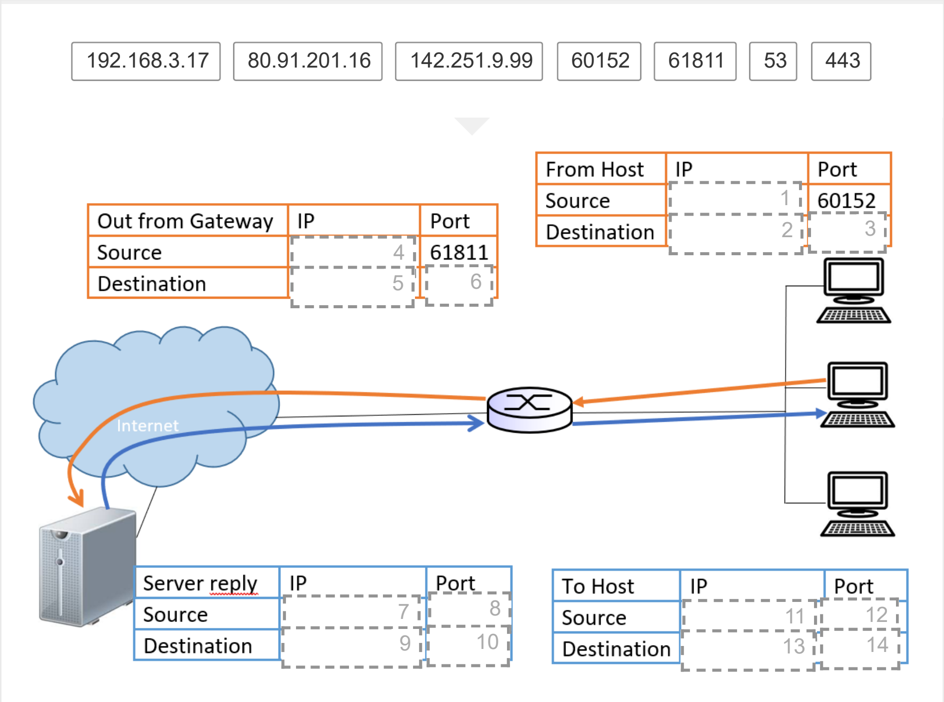
Item 13

Network Address Translation (2 points)

A host on the LAN requests a document from a HTTPS (443) server on the Internet.
The request has to pass the local gateway which has NAT enabled. The WAN interface on the gateway has a public IP address.

LAN host IP address: 192.168.3.17, Port 60152
Gateway public IP address: 80.91.201.16
Web server IP address: 142.251.9.99

Show the IP addresses and port numbers of the request and reply packets.



From Host	IP	Port
Source	1	60152
Destination	2	3

Out from Gateway	IP	Port
Source	4	61811
Destination	5	6

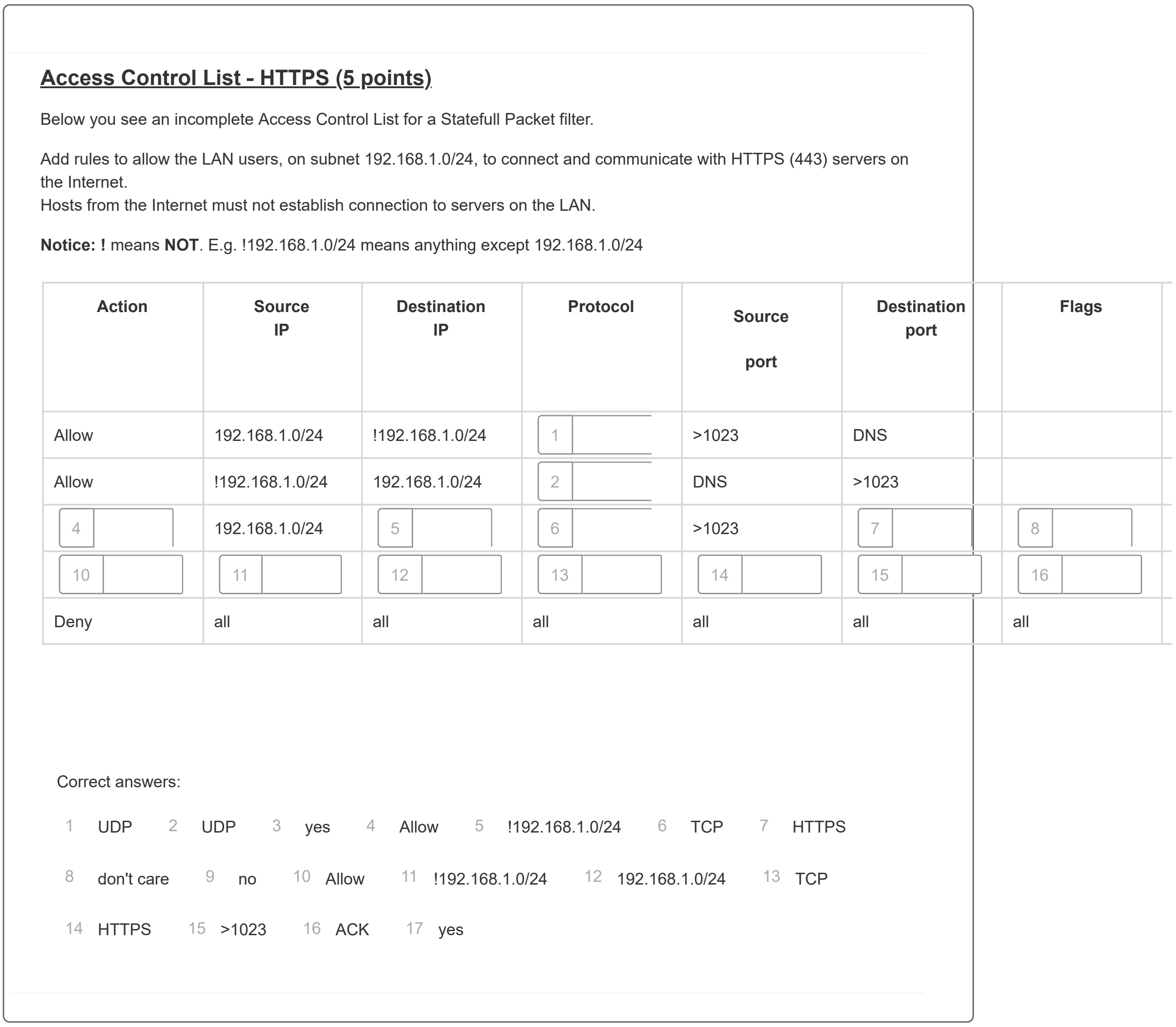
Server reply	IP	Port
Source	7	8
Destination	9	10

To Host	IP	Port
Source	11	12
Destination	13	14

Correct answers:

1	192.168.3.17
2	142.251.9.99
3	443
4	80.91.201.16
5	142.251.9.99
6	443
7	142.251.9.99
8	443
9	80.91.201.16
10	61811
11	142.251.9.99
12	443
13	192.168.3.17
14	60152

Item 14



Access Control List - HTTPS (5 points)

Below you see an incomplete Access Control List for a Statefull Packet filter.

Add rules to allow the LAN users, on subnet 192.168.1.0/24, to connect and communicate with HTTPS (443) servers on the Internet.
Hosts from the Internet must not establish connection to servers on the LAN.

Notice: ! means **NOT**. E.g. !192.168.1.0/24 means anything except 192.168.1.0/24

Action	Source IP	Destination IP	Protocol	Source port	Destination port	Flags
Allow	192.168.1.0/24	!192.168.1.0/24	1	>1023	DNS	
Allow	!192.168.1.0/24	192.168.1.0/24	2	DNS	>1023	
4	192.168.1.0/24	5	6	>1023	7	8
10	11	12	13	14	15	16
Deny	all	all	all	all	all	all

Correct answers:

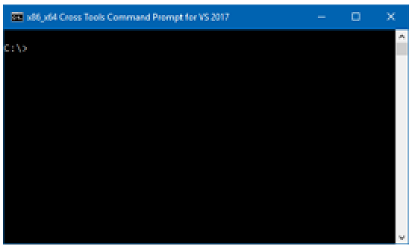
1 UDP 2 UDP 3 yes 4 Allow 5 !192.168.1.0/24 6 TCP 7 HTTPS

8 don't care 9 no 10 Allow 11 !192.168.1.0/24 12 192.168.1.0/24 13 TCP

14 HTTPS 15 >1023 16 ACK 17 yes

Item 15

Ping (2 points)

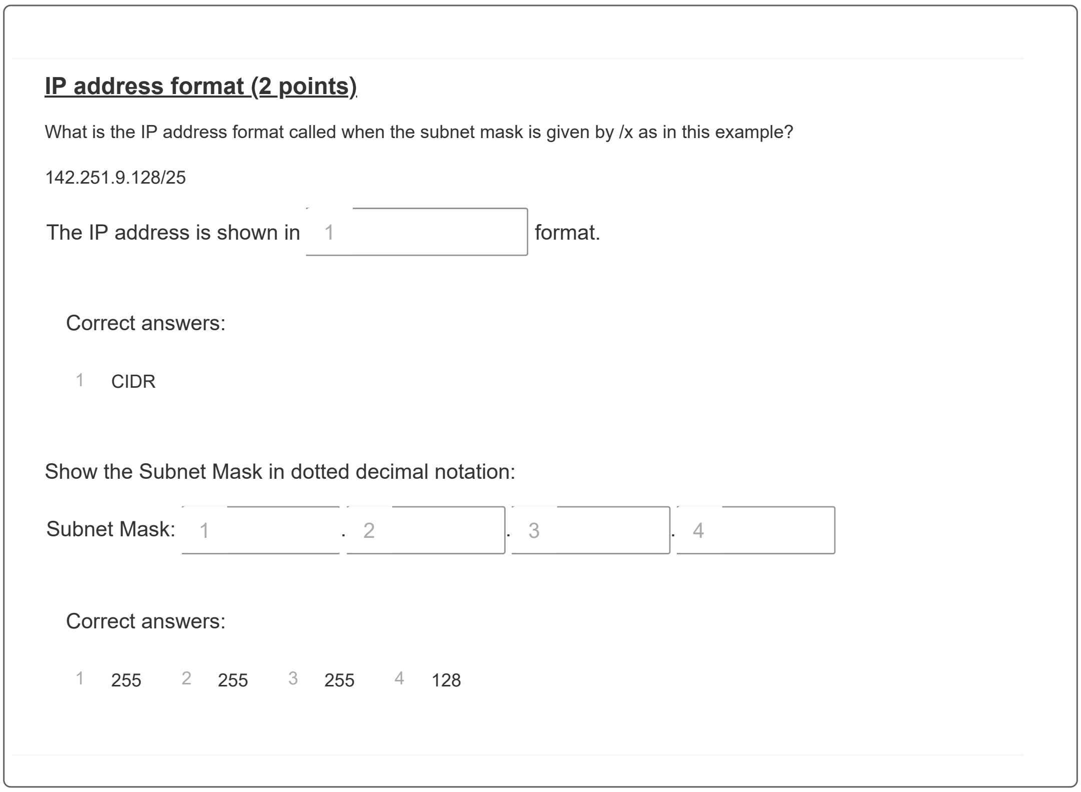


```
C:\>
```

Tick all the statements that are correct for the *ping* command.

- □ Verify that the physical connection works ✓
- □ Verify that the IP address configuration works ✓
- □ Verify that a server name, e.g. www.goggle.com, can be translated into an IP address via DNS ✓
- □ Measure RTT to the destination ✓
- □ count routers passed
- □ display which organisation an IP address belongs to

Item 16



IP address format (2 points)

What is the IP address format called when the subnet mask is given by /x as in this example?

142.251.9.128/25

The IP address is shown in 1 format.

Correct answers:

1 CIDR

Show the Subnet Mask in dotted decimal notation:

Subnet Mask: 1 . 2 . 3 . 4

Correct answers:

1 255 2 255 3 255 4 128

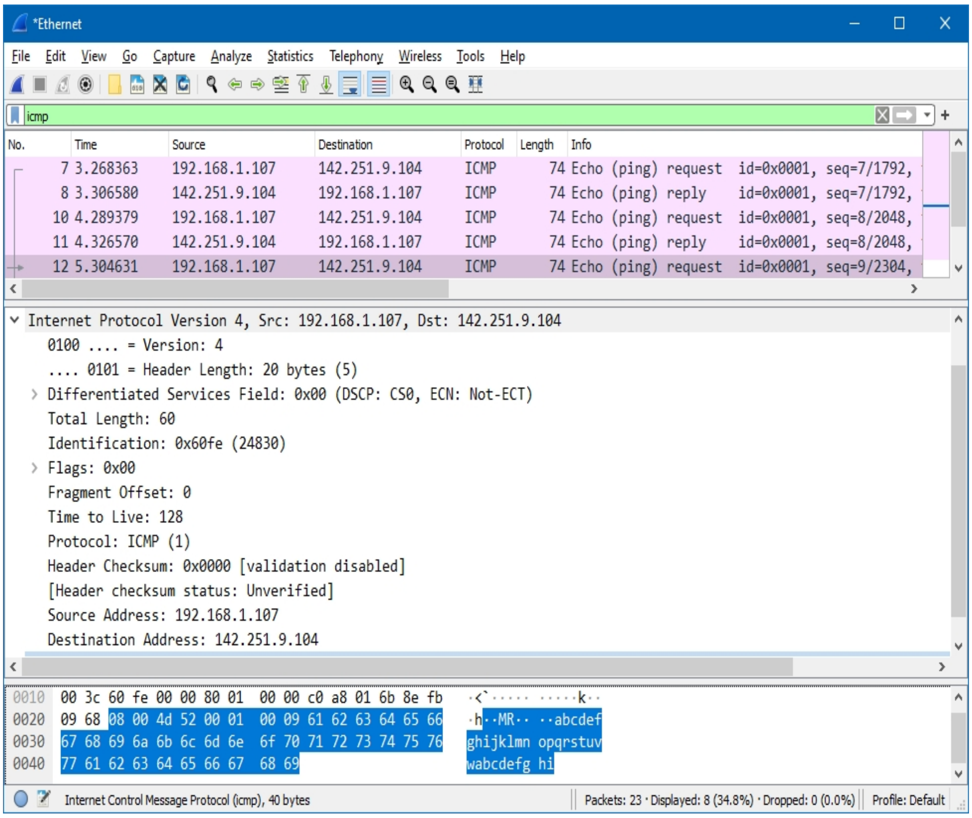
Item 17

IP Header (5 points)

Wireshark has picked up the shown packet from the network.

Find the relevant information in the figure and fill-in the missing fields in the IP header.

NOTICE: all values must be in decimal notation.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

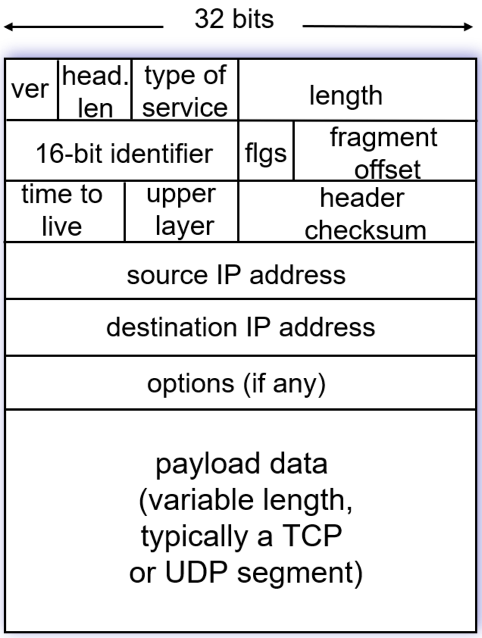
No.	Time	Source	Destination	Protocol	Length	Info
7	3.268363	192.168.1.107	142.251.9.104	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792,
8	3.306580	142.251.9.104	192.168.1.107	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792,
10	4.289379	192.168.1.107	142.251.9.104	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048,
11	4.326570	142.251.9.104	192.168.1.107	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048,
12	5.304631	192.168.1.107	142.251.9.104	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304,

```
Internet Protocol Version 4, Src: 192.168.1.107, Dst: 142.251.9.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x60fe (24830)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.107
    Destination Address: 142.251.9.104
```

```
0010  00 3c 60 fe 00 00 80 01  00 00 c0 a8 01 6b 8e fb   ·<`····· ·····k··
0020  09 68 08 00 4d 52 00 01  00 09 61 62 63 64 65 66   ·h··MR·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Control Message Protocol (icmp), 40 bytes | Packets: 23 · Displayed: 8 (34.8%) · Dropped: 0 (0.0%) | Profile: Default

IP header:



1	2	type of service	3
4		flags	5
6	7	8	
9			

10
options (if any)

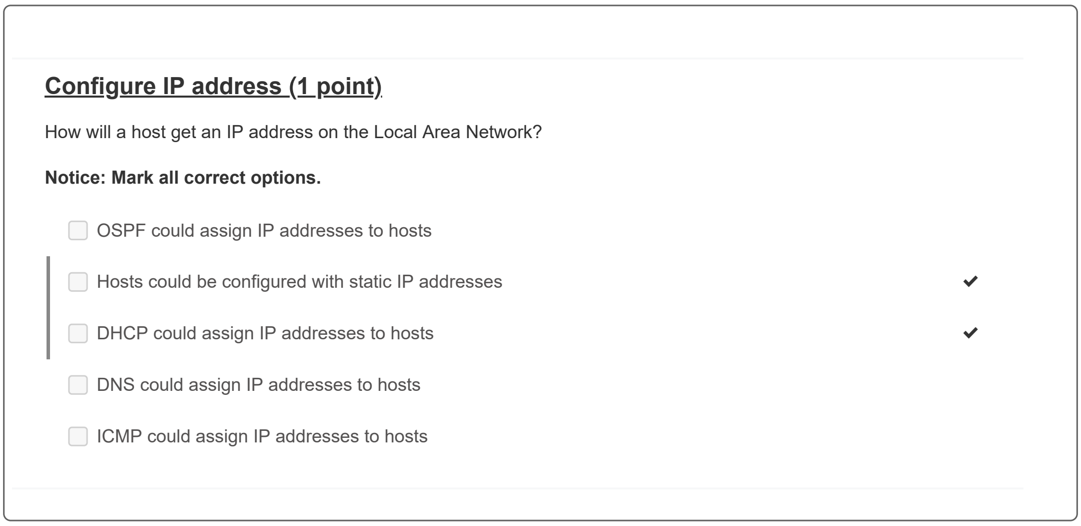
What is the length of the payload? 11 Bytes

Correct answers:

1 4 2 20 3 60 4 24830 5 0 6 128 7 1 8 0

9 192.168.1.107 10 142.251.9.104 11 40

Item 18



Configure IP address (1 point)

How will a host get an IP address on the Local Area Network?

Notice: Mark all correct options.

- □ OSPF could assign IP addresses to hosts
- □ Hosts could be configured with static IP addresses ✓
- □ DHCP could assign IP addresses to hosts ✓
- □ DNS could assign IP addresses to hosts
- □ ICMP could assign IP addresses to hosts

Item 19

HTTP (3 points)

Take a look at the following transcript of a packet caputred by Wireshark and answer the questions below.

```
    -
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Transfer-Encoding: chunked\r\n
    Content-Type: application/json\r\n
    Server: Microsoft-HTTPAPI/2.0\r\n
    Responsetime: 28\r\n
    ServerUtilization: 35\r\n
    RequestIpAddress: 87.49.146.179\r\n
    x-Unencrypted-Content-Length: 41\r\n
    CallCenter: False\r\n
    NetworksETag: e2dce6efbbf71606a7b803d2b82e7c73\r\n
    Date: Mon, 13 Dec 2021 08:25:55 GMT\r\n
    Connection: close\r\n
    \r\n
    [HTTP response 1/1]
    HTTP chunked response
        Data chunk (41 octets)
            Chunk size: 41 octets
            Data (41 bytes)
0000  7b 0d 0a 20 20 22 73 65 6c 65 63 74 65 64 22 3a   {..  "selected":
0010  20 5b 5d 2c 0d 0a 20 20 22 63 6f 6d 6d 61 6e 64    [],..  "command
0020  73 22 3a 20 5b 5d 0d 0a 7d                        s": []..}
                Data: 7b0d0a20202273656c6563746564223a205b5d2c0d0a2020…
                [Length: 41]
            Chunk boundary: 0d0a
        End of chunked encoding
            Chunk size: 0 octets
        \r\n
    File Data: 41 bytes
JavaScript Object Notation: application/json
    Object
        Member Key: selected
            Array
            Key: selected
        Member Key: commands
            Array
            Key: commands
```

The transcript shows a 1 message.

The status of the message means 2 .

The message contains 3 data Bytes

The **Date** header-field shows 4

The connection type is 5

Correct answers:

1 HTTP response 2 message is OK 3 41 4 the time the message was sent

5 non-persistent

Item 20

Elgamal Signing (6 points)

Let $q = 167$ and $\alpha = 55$ be the public parameters, and let $X_A = 60$ be your private key. Using the Elgamal signature scheme sign $m = 100$. You must use one of the following as your ephemeral key K:
$101,\ 82,\ 83,\ 92,\ 106.$
Note, S_1 and S_2 are scored independently (3 points each). State all answers as integers between 0 and 9999999.

The first part of the signature is

$$S_1 = \square^{\square}\ mod\ \square \equiv \square$$

Correct answers:

> $S_1 = 55^{101}\ mod\ 167\ \equiv 109$

The second part of the signature is

$$S_2 = \square \times \left(\square - 60 \times \square\right)\ mod\ \square \equiv \square$$

Correct answers:

> $S_2 = 143 \times (100 - 60 \times 109)\ mod\ 166 \equiv 48$

Item 21

Diffie-Hellman (3 points, all numbers must be correct to score)

Alice and Bob share the prime number 479 and the primitiv root 17.
Alice private key is 112 and she receives Bob's public key 116.

Find the secret key K by filling out the formular below:

$$K = \boxed{}^{\boxed{}} \, mod \, \boxed{} = \boxed{}$$

Correct answers:

> $K \; = 116^{112} \, mod \, 479 \; = 453$

Item 22

RSA Key Generation (5 points)

You must generate an RSA-key. You must choose p and q (primes) amongst the following values such that $p < q$:

125, 131, 147, 183, 199, 207

Also, when choosing the public key, you must choose between

5, 21, 27, 49, 82, 5349, 5373

Based on this information, fill in the blanks below. Write all answers as integers between 0 and 9999999. All answers must be correct to score.

$p =$ 1 □ and $q =$ 2 □.

$n =$ 3 □

$\phi(n) =$ 4 □

$e =$ 5 □

$d =$ 6 □

Correct answers:

1 131 2 199 3 26069 4 25740 5 49 6 6829

Item 23

RSA Encryption and Decryption (5 points)

You are given an RSA-key where the modulus is 14263, the public key is 15, and the private key is 7151. Using A = 00, B = 01,…J = 09…Z = 25, such that ‘GO’ is 0614 = 614 and ‘SE’ is 1804, encrypt and decrypt ‘NE’ using the RSA-key pair. Note that encryption and decryption are scored independently. Using the key and message supplied, fill in the blanks in the below formulas, making them correct RSA encryptions/decryptions. State all answers as integers between 0 and 9999999. All numbers in each equation must be correct to score.

Encryption (3 points):

$$c = \square^{\square}\ mod\ \square \equiv \square$$

Correct answers:

> $c = 1304^{15}\ mod\ 14263 \equiv 4192$

Decryption (2 points):

$$m = \square^{\square}\ mod\ \square \equiv \square$$

Correct answers:

> $m = 4192^{7151}\ mod\ 14263 \equiv 1304$

Item 24

Cipher Block Chaining (CBC) encryption (3 points)

A 3 bit block encryption E(m) = c is given with the following function:

m	c
000	011
001	110
010	101
011	100
100	001
101	000
110	111
111	010

E.g. if m=001 then c=110 because E(001)=110

Given the message 000101000 and an IV = 001 fill out the equations below:
Each equation is scored independently and gives 1 points if all numbers are correct.

$$c_1 = E\left(\square\, XOR\, \square\right) = E\left(\square\right) = \square$$

Correct answers:

> $c_1 = E(001\ XOR\ 000) = E(001) = 110$

m	c
000	011
001	110
010	101
011	100
100	001
101	000
110	111
111	010

$$c_2 = E\left(\square\, XOR\, \square\right) = E\left(\square\right) = \square$$

Correct answers:

> $c_2 = E(110\ XOR\ 101) = E(011) = 100$

m	c
000	011
001	110
010	101
011	100
100	001
101	000
110	111
111	010

$$c_3 = E\left(\square \, XOR \, \square\right) = E\left(\square\right) = \square$$

Correct answers:

> $c_3 = E(100\ XOR\ 000)\ = E(100)\ = 001$

Item 25

Cipher Block Chaining (CBC) decryption (3 points)

A 3 bit block encryption E(m) = c is given with the following function:

m	c
000	011
001	110
010	101
011	100
100	001
101	000
110	111
111	010

E.g. if m=001 then c=110 because E(001)=110

Decrypt the ciphertext 000001010 given IV = 001 and fill out the equations below:
Each equation is scored independently and gives 1 point if all numbers are correct.

$$m_1 = \boxed{} XOR\ D\left(\boxed{}\right) = \boxed{}$$

Correct answers:

> $m_1 = 001\ XOR\ D(000) = 100$

m	c
000	011
001	110
010	101
011	100
100	001
101	000
110	111
111	010

$$m_2 = \boxed{} XOR\ D\left(\boxed{}\right) = \boxed{}$$

Correct answers:

> $m_2 = 000\ XOR\ D(001) = 100$

m	c
000	011
001	110
010	101
011	100
100	001
101	000
110	111
111	010

$m_3 = \square \, XOR \; D(\square) = \square$

Correct answers:

> $m_3 = 001 \; XOR \; D(010) \; = \; 110$

Item 26

Elgamal Verification (4 points)

In an Elgamal signature scheme, the following are given:

- The message is 100
- 55 is a generator of the group Z_{167}^{*}
- The public key Y_A of the sender is 4
- The parameters of the signature are $S_1 = 109$and $S_2 = 48$.

Based on this information, demonstrate how to validate the signature. State all answers as integers between 0 and 9999999.
Each equation gives 2 point if all numbers in the equation are correct.

$$V_1 = \square^{\square}\ mod\ \square \equiv \square$$

Correct answers:

> $V_1 = 55^{100}\ mod\ 167 \equiv 87$

vs.

$$V_2 = \square^{\square}\square^{48}\ mod\ \square \equiv \square$$

Correct answers:

> $V_2 = 4^{109}\,109^{48}\ mod\ 167\ \equiv 87$

Item 27

Elgamal Key Generation (2 points)

Let 14 be the primitive root (i.e. generator) of 241 and let 50 be your private key. Assuming you want to build an Elgamal digital signature, what is the value of the public key? State your answer as an integer between 0 and 9999999.

1

Correct answers:

1 2

Item 28

Cryptographic hash functions (3 points)

Mark if the following statements are true or false (correct answers 0.5 points, wrong answers -0.5)

A hash function can be preimage and second preimage resistant.	○ True ✓	○ False
If a hash function is preimage and second preimage resistant then it must also be collision resistant.	○ True	○ False ✓
If a hash function is collision resistant it must also be second preimage resistant.	○ True ✓	○ False
If a hash function is collision resistant it must also be primage resistant.	○ True	○ False ✓
A cryptographic hash function can take input of any size.	○ True ✓	○ False
A cryptographic hash function produces output of any size.	○ True	○ False ✓