

LAYERED ARCHITECTURES:
ADDRESSING, ENCAPSULATION AND
LAYERS WORKING TOGETHER

JAYATILAKA G.C.

E/14/118

GROUP 06

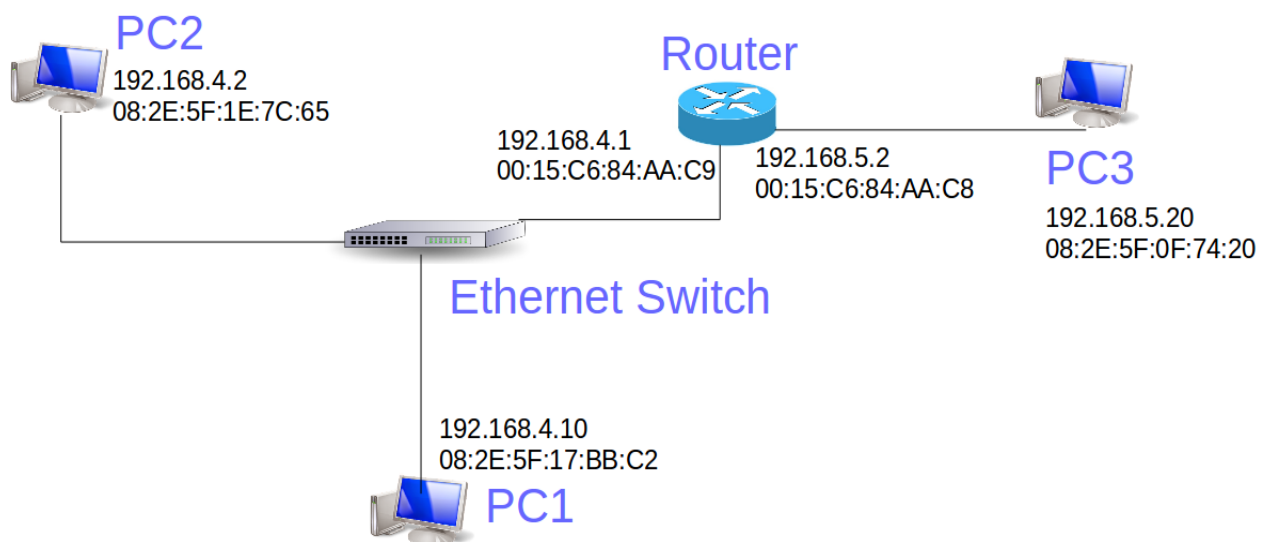
SEMESTER 03

13/03/2017

PART-1: IP addresses and MAC addresses

IP Addresses	
Subnet-1	192.168.4.0/24
Subnet-2	192.168.5.0/24
PC1	192.168.4.10
PC2	192.168.4.2
Router's interface on Subnet-1	192.168.4.1
Router's interface on Subnet-2	192.168.5.2
PC3	192.168.5.20

MAC Addresses	
PC1	08:2E:5F:17:BB:C2
PC2	08:2E:5F:1E:7C:65
PC3	08:2E:5F:0F:74:20
Router: Subnet-1 interface	00:15:C6:84:AA:C9
Router: Subnet-2 interface	00:15:C6:84:AA:C8



PART-2: Routing tables (IP tables)

```
network@network-HP-Compaq-6200-Pro-MT-PC:~$ netstat -r
Kernel IP routing table
Destination        Gateway           Genmask          Flags        MSS Window  irtt Iface
default            192.168.4.1      0.0.0.0          UG           0  0        0 eth0
192.168.4.0        *                255.255.255.0    U            0  0        0 eth0
network@network-HP-Compaq-6200-Pro-MT-PC:~$
```

Routing table @ PC1

CA Select Administrator: Command Prompt

```
Tunnel adapter isatap.{F0599A79-E477-4823-A125-57ACC3B94E63}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 
Description . . . . . : Microsoft ISATAP Adapter #3
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Administrator>show interface
'show' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>netstat -r
=====
Interface List
 5...08 2e 5f 17 bb c2 .....Intel(R) 82579LM Gigabit Network Connection
 1.....Software Loopback Interface 1
 3...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.4.1      192.168.4.10     266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
192.168.4.0                255.255.255.0    On-link          192.168.4.10     266
192.168.4.10               255.255.255.255  On-link          192.168.4.10     266
192.168.4.255              255.255.255.255  On-link          192.168.4.10     266
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          192.168.4.10     266
255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
255.255.255.255            255.255.255.255  On-link          192.168.4.10     266
=====
Persistent Routes:
Network Address          Netmask    Gateway Address  Metric
0.0.0.0                  0.0.0.0    192.168.4.1      Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 306 ::1/128                  On-link
5 266 fe80::/64                On-link
5 266 fe80::71d2:b254:e20b:663a/128
On-link
1 306 ff00::/8                  On-link
5 266 ff00::/8                  On-link
=====
Persistent Routes:
None

C:\Users\Administrator>
```

Routing table @ PC2

```

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.5.2      192.168.5.20     266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127.255.255.255           255.255.255.255  On-link          127.0.0.1        306
192.168.5.0                255.255.255.0    On-link          192.168.5.20     266
192.168.5.20               255.255.255.255  On-link          192.168.5.20     266
192.168.5.255              255.255.255.255  On-link          192.168.5.20     266
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          192.168.5.20     266
255.255.255.255           255.255.255.255  On-link          127.0.0.1        306
255.255.255.255           255.255.255.255  On-link          192.168.5.20     266
=====
Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
0.0.0.0                    0.0.0.0          192.168.5.2      Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 306 ::1/128                      On-link
2 266 fe80::/64                    On-link
2 266 fe80::904b:12b9:7f64:f26e/128
                                On-link
1 306 ff00::/8                     On-link
2 266 ff00::/8                     On-link
=====
Persistent Routes:
None

```

Routing table @ PC3

```

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, GigabitEthernet0/1
C    192.168.5.0/24 is directly connected, GigabitEthernet0/0
S    192.168.2.0/24 [1/0] via 192.168.3.1
S    192.168.3.0/24 [1/0] via 192.168.5.1
                                [1/0] via 192.168.2.1
r2#

```

Routing table @ router

Columns

The columns in the PCs are different because netstat gives slightly different outputs in linux and windows.

Network destination: This is the ip address of the destination for a packet. If a packet coming to this device has a particular destination ip in a row of this table, that packet is routed according to what is specified in that row.

Netmask/Gen mask: This is the subnet mask of the destination address. This can give an idea of the range of ip addresses for a particular subnet.

Gateway: This column has the ip address of the next hop for a packet.

Interface: The IP address of the local interface that the packet should pass through to go to the gateway.

Metric: The number of hops a packet has to jump in order to reach the destination by this path.

Flags: Gives some information about a particular row of the routing table such as whether this path is working as of now.

MSS: The maximum segment size which is the largest packet size that could be sent using this path.

Window: The maximum data the system is ready to accept at once.

Irrt: Initial round trip time – the time taken by the packet to be transmitted, acknowledged and returned in the initial condition when the connection was set up.

The columns in the router has no topics displayed. The first column is the subnet mask and the second is the gateway.

Rows

All PC routing tables have 0.0.0.0 or Default destination row which refers to the path a packet should take if it does not match with any other record in the routing table.

127.0.0.0 row deals with the traffic that should go to the localhost (that should not be directed somewhere else).

Other rows has the routing paths for packets.

PART-3: Encapsulation, the use of routing tables, and Layers working together.

Web request from PC2 to PC3

Filter: **http.request** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
13	10.671818	192.168.4.12	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
14	11.686580	192.168.4.12	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
20	12.154862	192.168.4.12	192.168.5.20	HTTP	360	GET /imm/ HTTP/1.1
23	12.686637	192.168.4.12	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
24	13.686684	192.168.4.12	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
26	15.161225	192.168.4.2	192.168.5.20	HTTP	513	GET /imm/Meteosat7-full-scan.png.jpg HTTP/1.1

Frame 20: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface 0
Ethernet II, Src: HewlettP_1e:7c:65 (08:2e:5f:1e:7c:65), Dst: Cisco_84:aa:c9 (00:15:c6:84:aa:c9)
Internet Protocol Version 4, Src: 192.168.4.2, Dst: 192.168.5.20
Transmission Control Protocol, Src Port: 54806, Dst Port: 80, Seq: 1, Ack: 1, Len: 294
Source Port: 54806
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 294]
Sequence number: 1 (relative sequence number)
[Next sequence number: 295 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 32 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 229
[Calculated window size: 29312]
[Window size scaling factor: 128]
Checksum: 0x8bb3 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
Hypertext Transfer Protocol
GET /imm/ HTTP/1.1
[Expert Info (Chat/Sequence): GET /imm/ HTTP/1.1
Request Method: GET
Request URI: /imm/
Request Version: HTTP/1.1
Host: 192.168.5.20
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Full request URI: http://192.168.5.20/imm/
[HTTP request 1/2]
[Response in frame: 21]
[Next request in frame: 26]

0040 af 69 47 45 54 20 2f 69 6d 6d 2f 20 48 54 54 50 .iGET /i mm/ HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e /1.1..Ho st: 192.
0060 31 36 38 2e 35 2e 32 30 0d 0a 55 73 65 72 2d 41 168.5.20 ..User-A
0070 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5.
0080 30 20 28 58 31 31 3b 20 55 62 75 6e 74 75 3b 20 0 (X11; Ubuntu;
0090 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 76 Linux x8 6 64; rv
00a0 3a 32 38 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 :28.0) G ecko/201
00b0 30 30 31 20 31 20 45 60 73 65 65 6f 70 2f 32 30 30 101 Firefox/28.0

Text item (text), 20 bytes Packets: 384 · Displayed: 6 (1.6%) · Load time: 0:00.051

The frame no 20 is associated with the HTTP request.

HTTP request data

The keyword GET at the beginning of the description states that this is a request. This request has the directory where the data is requested from as “/imm” and also the host from which the data is requested as 102.168.5.20

Further more the request contains the details of the client PC such as the web browser, operating system and the language.

Size of data portion is 20 bytes.

Different levels of encapsulation

First level encapsulation

Transmission Control Protocol, Src Port: 54806, Dst Port: 80, Seq: 1, Ack: 1, Len: 294

- Source Port: 54806
- Destination Port: 80
- [Stream index: 0]
- [TCP Segment Len: 294]
- Sequence number: 1 (relative sequence number)
- [Next sequence number: 295 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)
- Header Length: 32 bytes
- Flags: 0x018 (PSH, ACK)
- Window size value: 229
- [Calculated window size: 29312]
- [Window size scaling factor: 128]
- Checksum: 0x8bb3 [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
- [SEQ/ACK analysis]

Hypertext Transfer Protocol

0020	05 14 d6 16 00 50 57 f6 07 4a d1 e4 18 85 80 18PW. .J.....
0030	00 e5 8b b3 00 00 01 01 08 0a 00 10 0a 46 00 44F.D
0040	af 69 47 45 54 20 2f 69 6d 6d 2f 20 48 54 54 50	.iGET /i mm/ HTTP
0050	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e	/1.1..Ho st: 192.
0060	31 36 38 2e 35 2e 32 30 0d 0a 55 73 65 72 2d 41	168.5.20 ..User-A

Transmission Control Protocol (tcp), 32 bytes Packets: 384 · Displayed: 6 (1.6%) · Load time: 0:00.051

Second level encapsulation

Internet Protocol Version 4, Src: 192.168.4.2, Dst: 192.168.5.20

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 346
- Identification: 0x0d11 (3345)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 64
- Protocol: TCP (6)
- Header checksum: 0xa226 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.4.2
- Destination: 192.168.5.20

Transmission Control Protocol, Src Port: 54806, Dst Port: 80, Seq: 1, Ack: 1, Len: 294

Hypertext Transfer Protocol

0000	00 15 c6 84 aa c9 08 2e 5f 1e 7c 65 08 00 45 00 e..E.
0010	01 5a 0d 11 40 00 40 06 a2 26 c0 a8 04 02 c0 a8	.Z..@.@. .&.....
0020	05 14 d6 16 00 50 57 f6 07 4a d1 e4 18 85 80 18PW. .J.....
0030	00 e5 8b b3 00 00 01 01 08 0a 00 10 0a 46 00 44F.D
0040	af 69 47 45 54 20 2f 69 6d 6d 2f 20 48 54 54 50	.iGET /i mm/ HTTP

Internet Protocol Version 4 (ip), 20 bytes Packets: 384 · Displayed: 6 (1.6%) · Load time: 0:00.051

Third level encapsulation

Ethernet II, Src: HewlettP_1e:7c:65 (08:2e:5f:1e:7c:65), Dst: Cisco 84:aa:c9 (00:15:c6:84:aa:c9)

- Destination: Cisco 84:aa:c9 (00:15:c6:84:aa:c9)
- Address: Cisco_84:aa:c9 (00:15:c6:84:aa:c9)
- 0. = LG bit: Globally unique address (factory default)
- 0. = IG bit: Individual address (unicast)
- Source: HewlettP_1e:7c:65 (08:2e:5f:1e:7c:65)
- Address: HewlettP_1e:7c:65 (08:2e:5f:1e:7c:65)
- 0. = LG bit: Globally unique address (factory default)
- 0. = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.4.2, Dst: 192.168.5.20

Transmission Control Protocol, Src Port: 54806, Dst Port: 80, Seq: 1, Ack: 1, Len: 294

Hypertext Transfer Protocol

0000	00 15 c6 84 aa c9 08 2e 5f 1e 7c 65 08 00 45 00 e..E.
0010	01 5a 0d 11 40 00 40 06 a2 26 c0 a8 04 02 c0 a8	.Z..@.@. .&.....
0020	05 14 d6 16 00 50 57 f6 07 4a d1 e4 18 85 80 18PW. .J.....
0030	00 e5 8b b3 00 00 01 01 08 0a 00 10 0a 46 00 44F.D
0040	af 69 47 45 54 20 2f 69 6d 6d 2f 20 48 54 54 50	.iGET /i mm/ HTTP

Ethernet (eth), 14 bytes Packets: 384 · Displayed: 6 (1.6%) · Load time: 0:00.051

	1 st level encapsulation	2 nd level encapsulation	3 rd level encapsulation
What is the payload of this layer	294 bytes	326 bytes	346 bytes
State where this encapsulation is done			
--Where in PC2	OS	OS + NIC	NIC
--At which layer	Transport	Network	Link
Details of control information (header files) added by this layer.			
--Associated protocol in this layer:	TCP	IPv4	Ethernet 2
--Source port no	54806		
--Destination port no	80		
--Protocol type	Connection oriented	Connectionless	Connectionless
--Source address		192.169.4.2	HewlettP_1e:7c:65 (08:2e:5f:1e:7c:65)
--Destination address:		192.168.5.20	Cisco_84:aa:c9 (00:15:c6:84:aa:c9)
--Addresses are IP or MAC?		IP	MAC
--Other control information		Time to live= 64s	
Size of control information added by this layer	32bytes	20 bytes	14 bytes
How do you call the payload + header	Segment	Packet	Frame

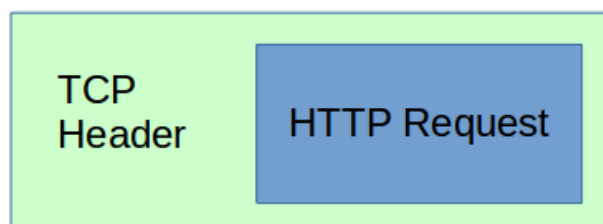
Header size to frame size percentage

= (Header size / Frame size) * 100%

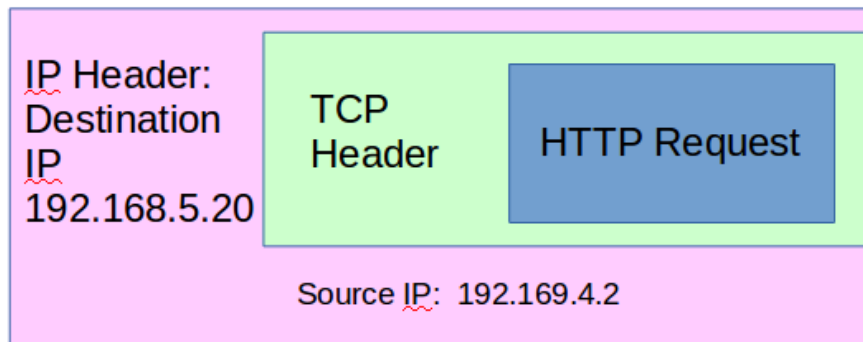
= (32 + 20 + 14) / 360 * 100%

= 18.33%

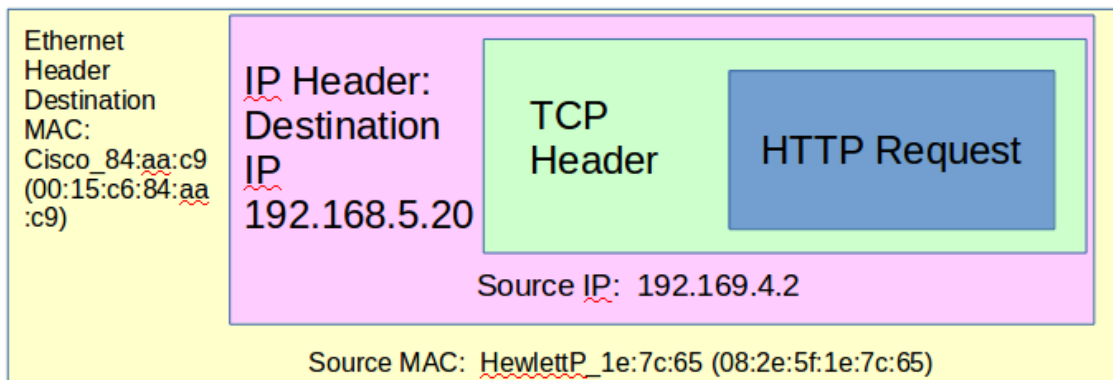
Different encapsulations



First level encapsulation: Segment



Second level encapsulation: Packet



Third level encapsulation: Frame

Reasons for the selection of the destination MAC address using the routing table @ PC2

Even though the packet is intended to be sent to PC3, since there is a router in between there is no way for PC2 to know the MAC address of the PC3. Therefore it looks up the routing table which has the MAC of the router's interface that the packet should be sent to.

How PC2 find the destination MAC address

Theoretically, there is another protocol called ARP (address resolution protocol) that could be used to determine the MAC address of a particular IP address in a subnet. But this was not seen in the wireshark save files. That is because the the routing table already knew the corresponding MAC addresses to the IP addresses (in that case the router does not need to use ARP to find MAC addresses).

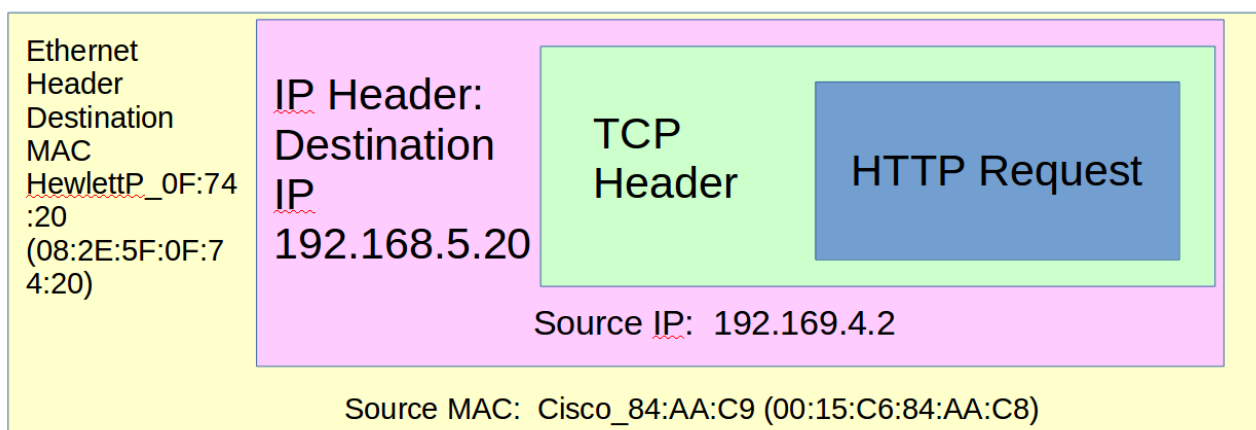
How Ethernet header is processed and the packet is passed on to the IP layer at the router.

When the frame is received by the cisco router it matches the destination MAC address (which is present in the link layer header) to the MAC address of the router. If the addresses match it removes the link layer header information and isolates the packet. Then the packet is passed up to the network layer of the router.

Actions that take place in the IP layer of the router

When the packet reaches the IP layer of the router it's destination is matched against the subnet masks in the routing table of the router. Since the destination IP 192.168.5.20 matches to 192.168.5.0/24 which is directly connected, the packet is sent to the corresponding interface GigabitEthernet 0/0.

Packet after encapsulation at router's interface



Analyzing the trace file at PC3

The packet could not be captured at the PC3 during the lab session. Therefore another request was sent by PC2 to download a new file (imm/a.zip). The next screen capture is of that request.

Frame no: 94169

No.	Time	Source	Destination	Protocol	Length	Info	
94169	8.456235	192.168.4.2	192.168.5.20	HTTP	365	GET /imm/a.zip HTTP/1.1	
<div>94169 8.456235 192.168.4.2 192.168.5.20 HTTP 365 GET /imm/a.zip HTTP/1.1</div> <div>▶ Frame 94169: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) on interface 0</div> <div>▼ Ethernet II, Src: Cisco 84:aa:c8 (00:15:c6:84:aa:c8), Dst: HewlettP_0f:74:20 (08:2e:5f:0f:74:20)</div> <div>▶ Destination: HewlettP_0f:74:20 (08:2e:5f:0f:74:20)</div> <div>▶ Source: Cisco 84:aa:c8 (00:15:c6:84:aa:c8)</div> <div>Type: IPv4 (0x0800)</div> <div>▼ Internet Protocol Version 4, Src: 192.168.4.2, Dst: 192.168.5.20</div> <div>0100 = Version: 4</div> <div>.... 0101 = Header Length: 20 bytes (5)</div> <div>▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> <div>Total Length: 351</div> <div>Identification: 0x145e (5214)</div> <div>▶ Flags: 0x02 (Don't Fragment)</div> <div>Fragment offset: 0</div> <div>Time to live: 63</div> <div>Protocol: TCP (6)</div> <div>Header checksum: 0x9bd4 [validation disabled]</div> <div>[Header checksum status: Unverified]</div> <div>Source: 192.168.4.2</div> <div>Destination: 192.168.5.20</div> <div>▼ Transmission Control Protocol, Src Port: 53041, Dst Port: 80, Seq: 1, Ack: 1, Len: 299</div> <div>Source Port: 53041</div> <div>Destination Port: 80</div> <div>[Stream index: 1]</div> <div>[TCP Segment Len: 299]</div> <div>Sequence number: 1 (relative sequence number)</div> <div>[Next sequence number: 300 (relative sequence number)]</div> <div>Acknowledgment number: 1 (relative ack number)</div> <div>Header Length: 32 bytes</div> <div>▶ Flags: 0x018 (PSH, ACK)</div> <div>Window size value: 229</div> <div>[Calculated window size: 29312]</div> <div>[Window size scaling factor: 128]</div> <div>Checksum: 0x2db4 [unverified]</div> <div>[Checksum Status: Unverified]</div> <div>Urgent pointer: 0</div> <div>▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps</div> <div>▶ [SEQ/ACK analysis]</div> <div>▼ Hypertext Transfer Protocol</div> <div>▼ GET /imm/a.zip HTTP/1.1\r\n</div> <div>▶ [Expert Info (Chat/Sequence): GET /imm/a.zip HTTP/1.1\r\n]</div> <div>Request Method: GET</div> <div>Request URI: /imm/a.zip</div> <div>Request Version: HTTP/1.1</div> <div>Host: 192.168.5.20\r\n</div> <div>User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0</div> <div>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n</div> <div>Accept-Language: en-US,en;q=0.5\r\n</div>							of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] [CK] Seq=300 Ack=5793 W of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] [CK] Seq=300 Ack=13033 of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] [CK] Seq=300 Ack=17377 of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] of a reassembled PDU] [CK] Seq=300 Ack=28961

How both IP and MAC addressing schemes are effectively used in order to transmit data through different networks/subnets

In this lab session a packet is sent from PC2 in a subnet to PC3 in another subnet. Destination and source IP addresses are added in the PC2 and not changed throughout the route. IP address scheme keeps the data about where the packet originated and where it should go.

MAC address scheme is used to take the packet between two routers. The MAC destination and source data keeps changing at every hop in the route. This scheme enables the transmission in link layer.

How different layers work together in transmission from PC2 to PC3

The http request is on the application layer of PC2 and PC3. But this request is sent through the transport layer using the TCP protocol. In order to send the TCP segments between the PC2 and PC3, the IP protocol in network layer is used. The http request actually leave the PC2 as an IP packet. But again IP itself cannot transmit the data to PC3 so it depends on the services supplied by the linked layer below it.

The data is first transmitted by the link layer (using the physical layer to transmit the electrical signals) up to the switch and then up to the router. The router's link layer passes the data up to its network layer where it is routed to the correct pathway to go to PC3 and again the link layer undertakes the transmission to PC3 from the router using the physical layer to transmit bits as electrical signals.

Web surfing: Downloading web contents

Filter:	http	Expression...	Clear	Apply	Save	
No.	Time	Source	Destination	Protocol	Length	Info
20	12.154862	192.168.4.2	192.168.5.20	HTTP	360	GET /imm/ HTTP/1.1
21	12.167936	192.168.5.20	192.168.4.2	HTTP	1296	HTTP/1.1 200 OK (text/html)
26	15.161225	192.168.4.2	192.168.5.20	HTTP	513	GET /imm/Meteosat7-full-scan.png.jpg HTTP/1.1
353	15.235828	192.168.5.20	192.168.4.2	HTTP	1242	HTTP/1.1 200 OK (JPEG JFIF image)

Checksum: 0x18a8 [Unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▶ [SEQ/ACK analysis]

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n
▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
Date: Mon, 13 Feb 2017 09:52:31 GMT\r\nServer: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28\r\n▶ Content-Length: 1000\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n\r\n[HTTP response 1/2]
[Time since request: 0.013074000 seconds]
[\[Request in frame: 20\]](#)
[\[Next request in frame: 26\]](#)
[\[Next response in frame: 353\]](#)
File Data: 1000 bytes

▶ Line-based text data: text/html

0000 08 2e 5f 1e 7c 65 00 15 c6 84 aa c9 08 00 45 00 ...|e..E.
0010 05 02 36 e9 40 00 7f 06 35 a6 c0 a8 05 14 c0 a8 ..6.@... 5.....
0020 04 02 00 50 d6 16 d1 e4 18 85 57 f6 08 70 80 18 ...P.....W.p..
0030 01 04 f8 a8 00 00 01 01 08 0a 00 44 af 76 00 10D.v..
0040 0a 46 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f .FHTTP/1 .1 200 0
0050 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 31 33 K..Date: Mon, 13
0060 20 46 65 62 20 32 30 31 37 20 30 39 3a 35 32 3a Feb 201 7 09:52:
0070 33 31 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 31 GMT.. Server:
0080 41 70 61 63 68 65 2f 32 2e 34 2e 32 33 20 28 57 Apache/2 .4.23 (W
0090 69 6e 33 32 29 20 4f 70 65 6e 53 53 4c 2f 31 2e in32) Op enSSL/1.
00a0 30 2e 32 68 20 50 48 50 2f 35 2e 36 2e 32 38 0d 0.2h PHP /5.6.28.
00b0 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a .Content -Length:
00c0 20 31 30 30 30 0d 0a 4b 65 65 70 2d 41 6c 69 76 1000..K eep-Aliv
00d0 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 e: timeo ut=5, ma
00e0 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f x=100..C onnectio
00f0 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 n: Keep- Alive..C
0100 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 ontent-T ype: tex
0110 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 55 t/html;c harset=U
0120 54 46 2d 38 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 TF-8.... <!DOCTYPE
0130 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d E HTML P UBLIC "-
0140 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 //W3C//D TD HTML
0150 33 2e 32 20 46 69 6e 61 6c 2f 2f 45 4e 22 3e 0a 3.2 Fina l//EN">.
0160 3c 68 74 6d 6c 3e 0a 20 3c 68 65 61 64 3e 0a 20 <html>. <head>.
0170 20 3c 74 69 74 6c 65 3e 49 6e 64 65 78 20 6f 66 <title> Index of

Percentage of header size to frame size

=(TCP header size + IP header size + Ethernet header size)/ Frame size *100%

=(32+20+14)/(1296)*100%

=5.09%

Reasons

The header size to frame size is higher in the HTML data frame than the HTTP request frame.

That is because whether the packet is only a request to a address which has only few characters saying the address or else a long text of a web page source, approximately the same header information is required. So the http request packet with smaller useful data has a bigger ratio for header size to frame size.