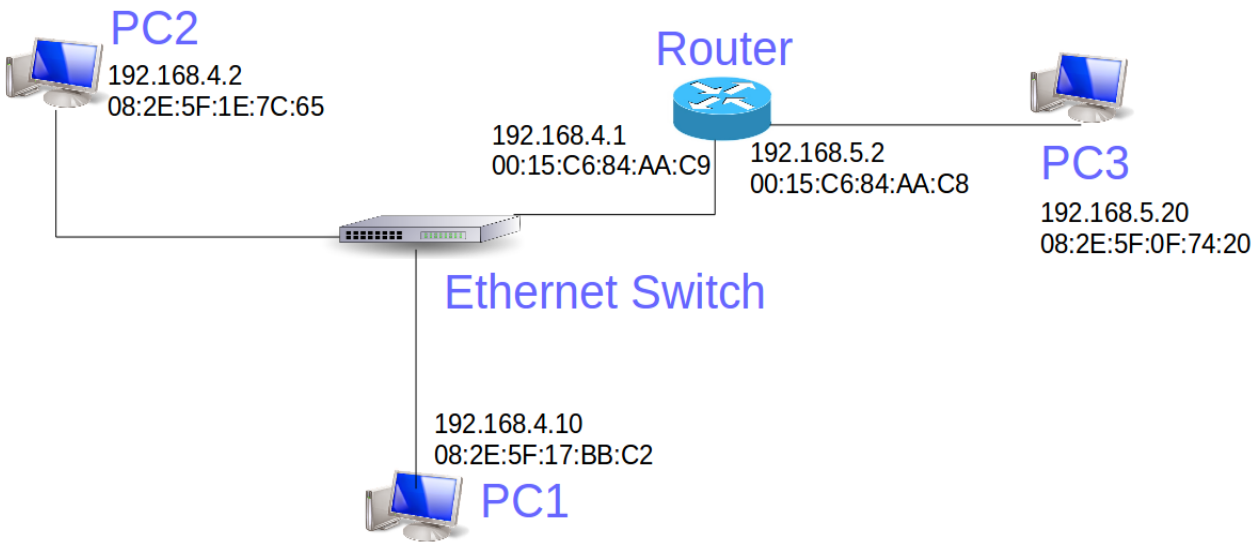
LAYERED ARCHITECTURES: ADDRESSING, ENCAPSULATION AND LAYERS WORKING TOGETHER

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)

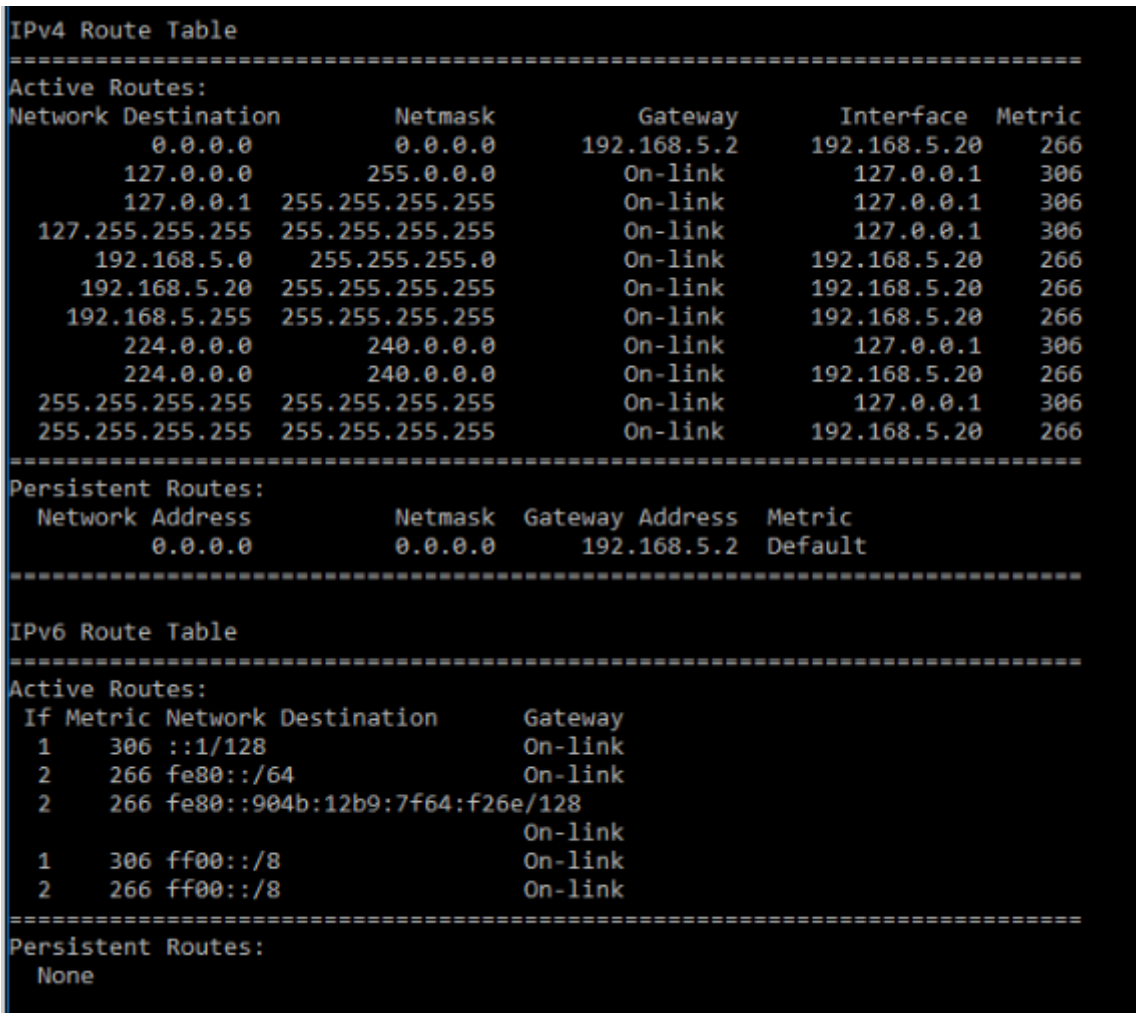
```
network@network-HP-Compaq-6200-Pro-MT-PC:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.4.1     0.0.0.0         UG        0 0          0 eth0
192.168.4.0     *               255.255.255.0   U         0 0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

Routing table @ PC1

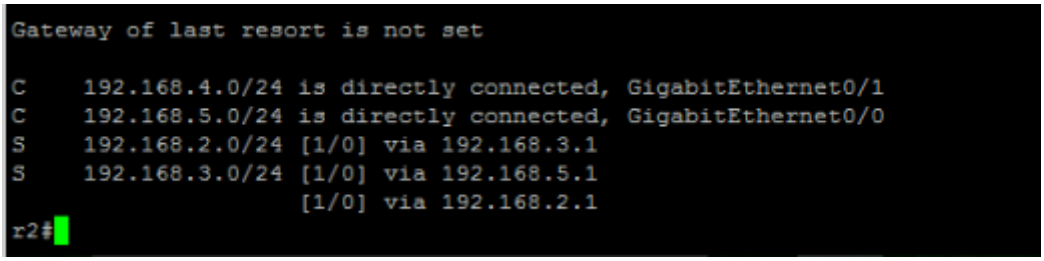
Select Administrator: Command Prompt

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

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #3
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-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



Routing table @ PC3



Routing table @ router

Columns

The columns in the PCs are different because netstat gives slihtly 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 inteface 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.

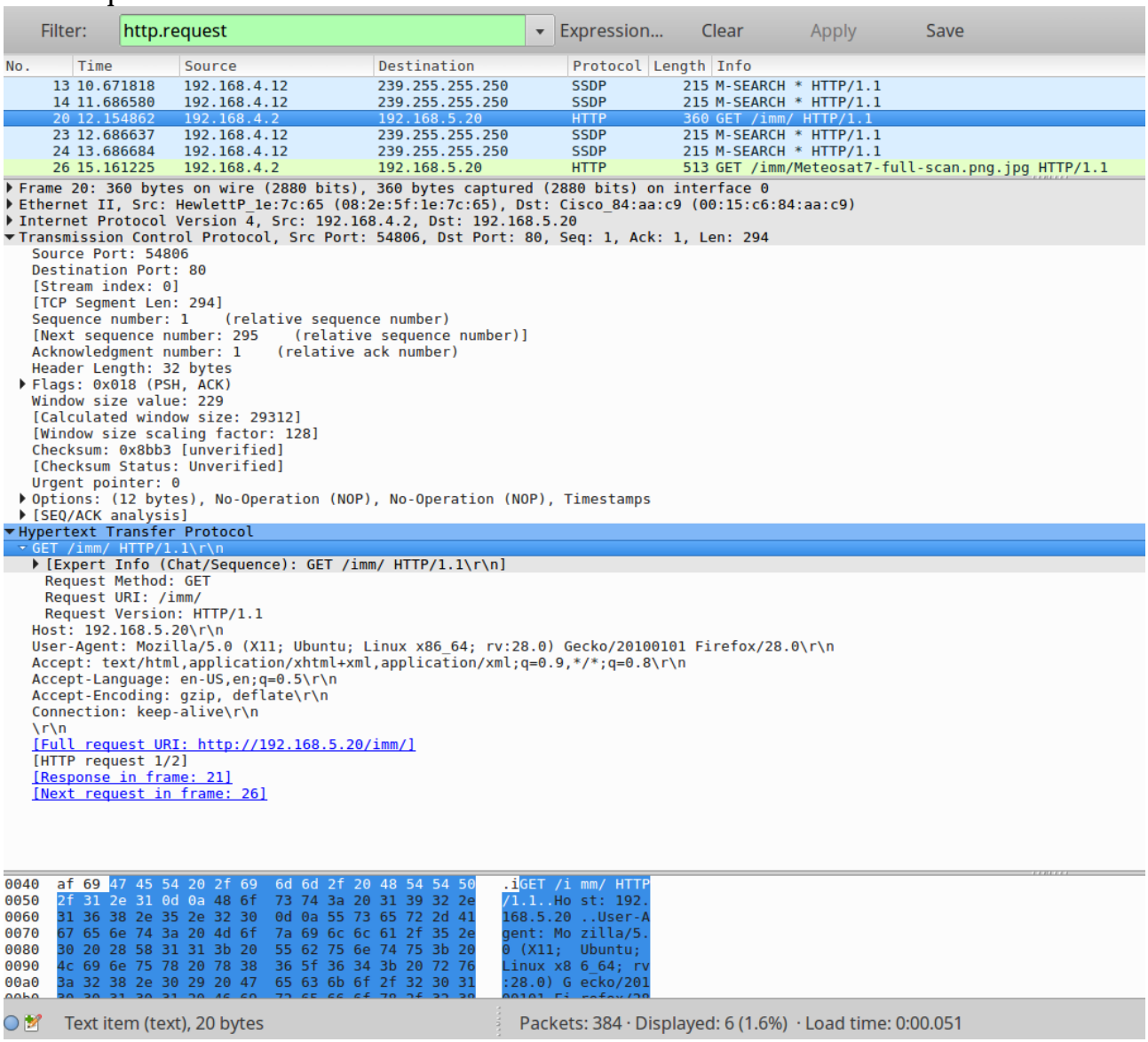
The columns in the router has no topics displayed. The first column is the subnet mask and the second is the gateway.

Rows

All PC routing tables have 0.0.0.0 or Defalut 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



The frame no 20 is associated with the HTTP request.

HTTP request data

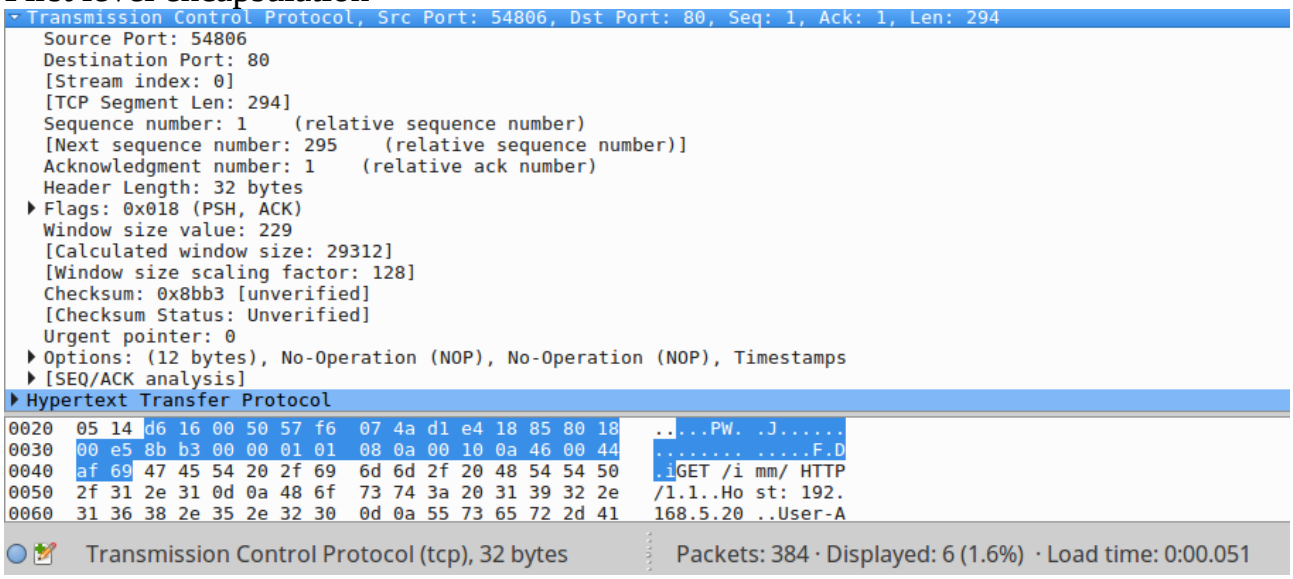
The keyword GET at the beginning of the description states that this is a request. This request has the directory where the data is requested from as “/imm” and also the host from which the data is requested as 102.168.5.20

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

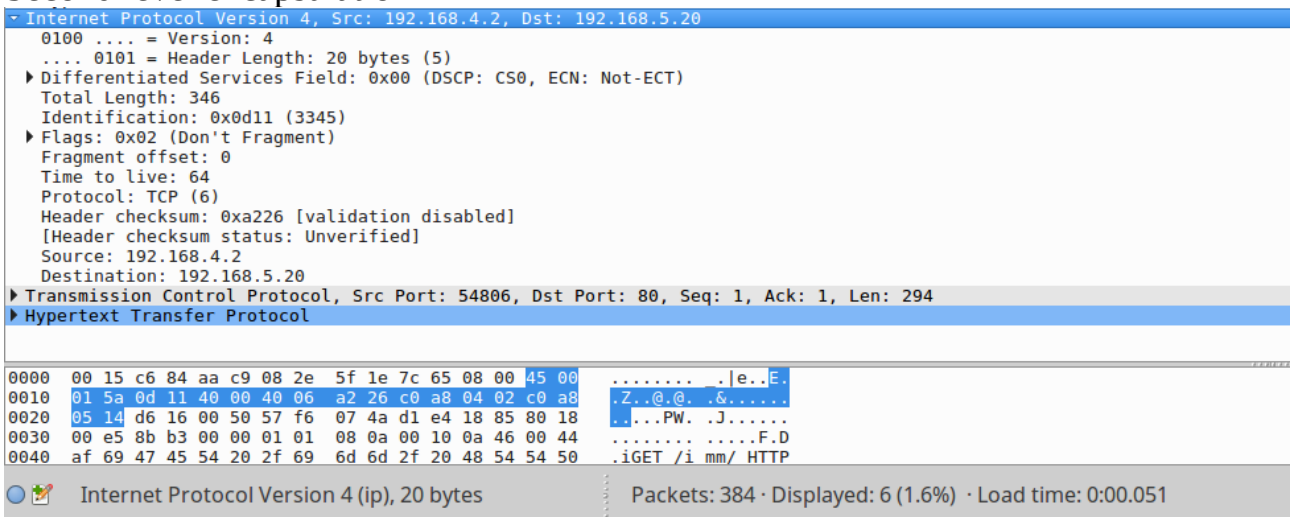
Size of data portion is 20 bytes.

Different levels of encapsulation

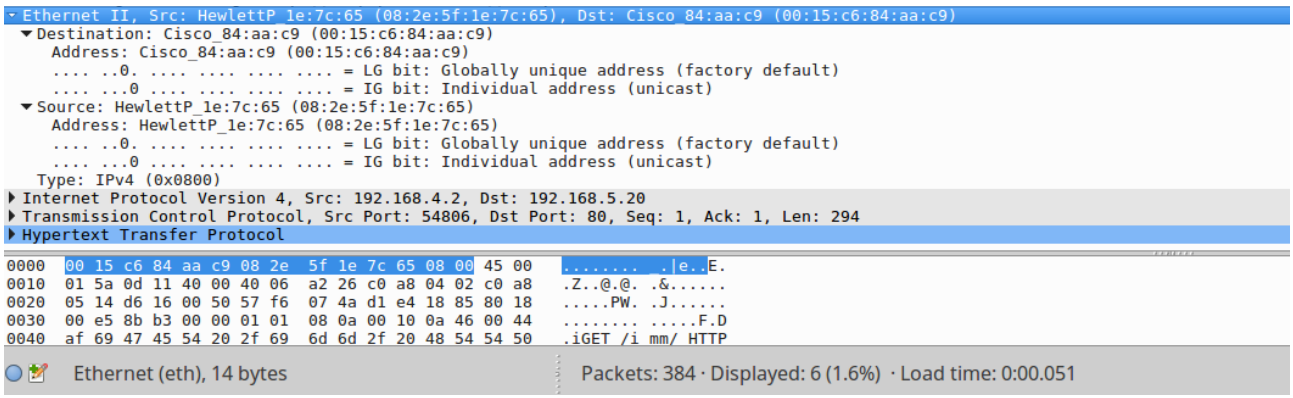
First level encapsulation



Second level encapsulation



Third level encapsulation



	1st level encapsulation	2nd level encapsulation	3rd 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

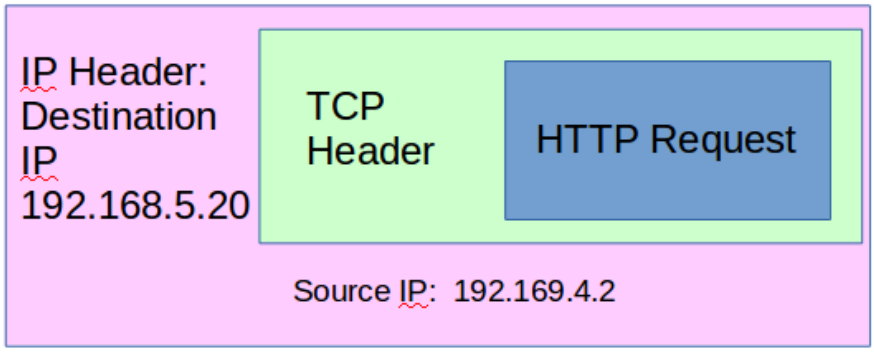
=(Header size/Frame size)*100%

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

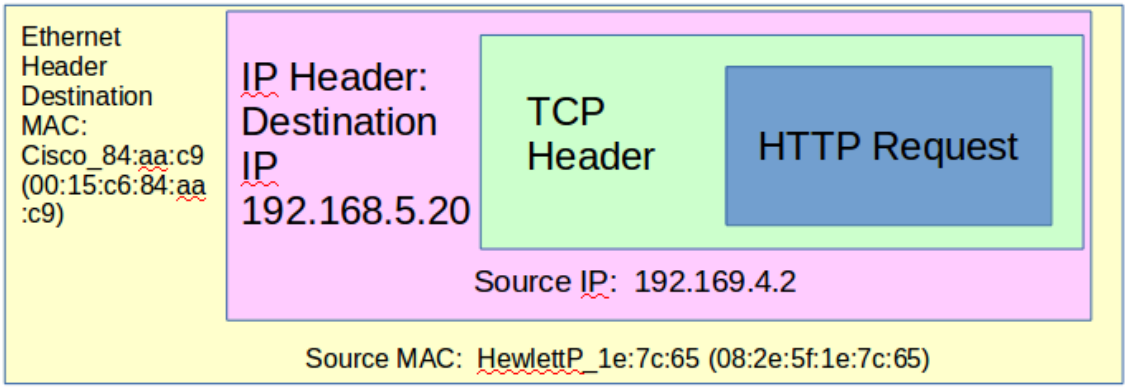
=18.33%

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).

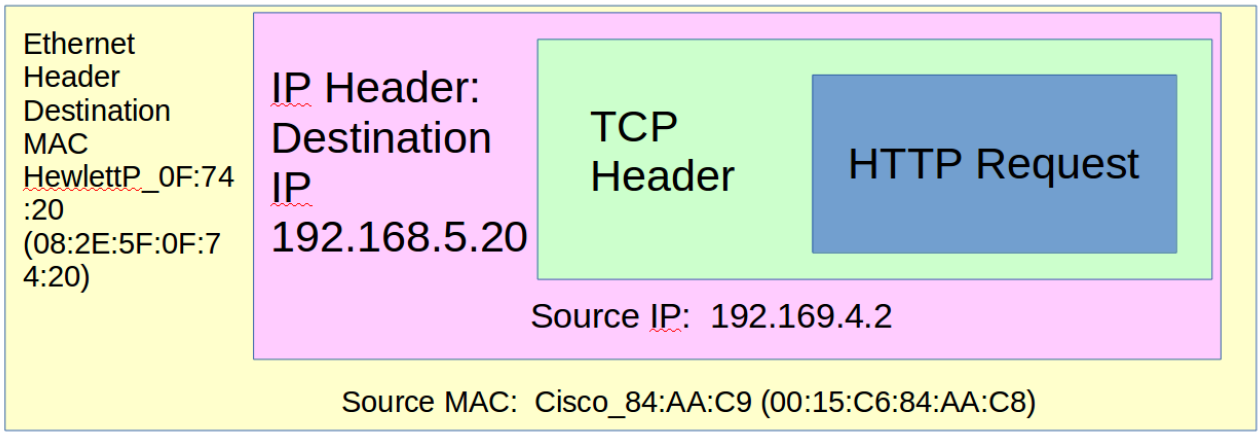
How Ethernet header is processed and the packet is passed on to the IP layer at the router.

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 IP192.168.5.20 matches to 192.168.5.0/24 which is directly connected, the packet is sent to the corresponding interface GigabitEthernet 0/0.

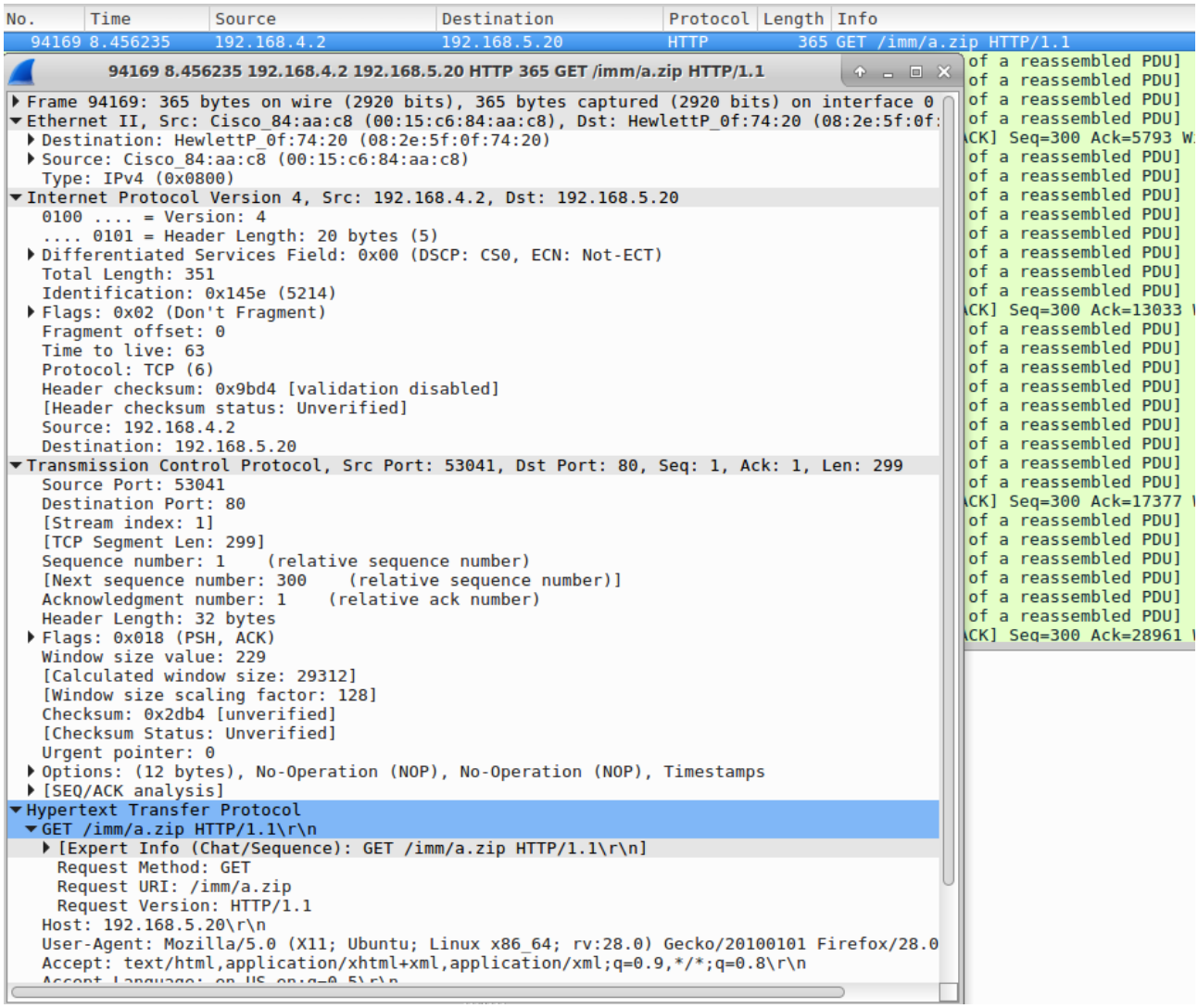
Packet after encapsulation at router's interface



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



The MAC and IP addresses (both destination and source) are the same as in “Packet after encapsulation at router’s interface”

Components associated to the addresses seen when sending data

Sending data from PC2 to Router	
Component associated to the “source IP address”	PC2
Component associated to the “destination IP address”	PC3
Component associated to the “source MAC address”	PC2
Component associated to the “destination IP address”	Router-NIC1

Sending data from Router to PC3	
Component associated to the “source IP address”	PC2
Component associated to the “destination IP address”	PC3
Component associated to the “source MAC address”	Router-NIC2
Component associated to the “destination IP address”	PC3

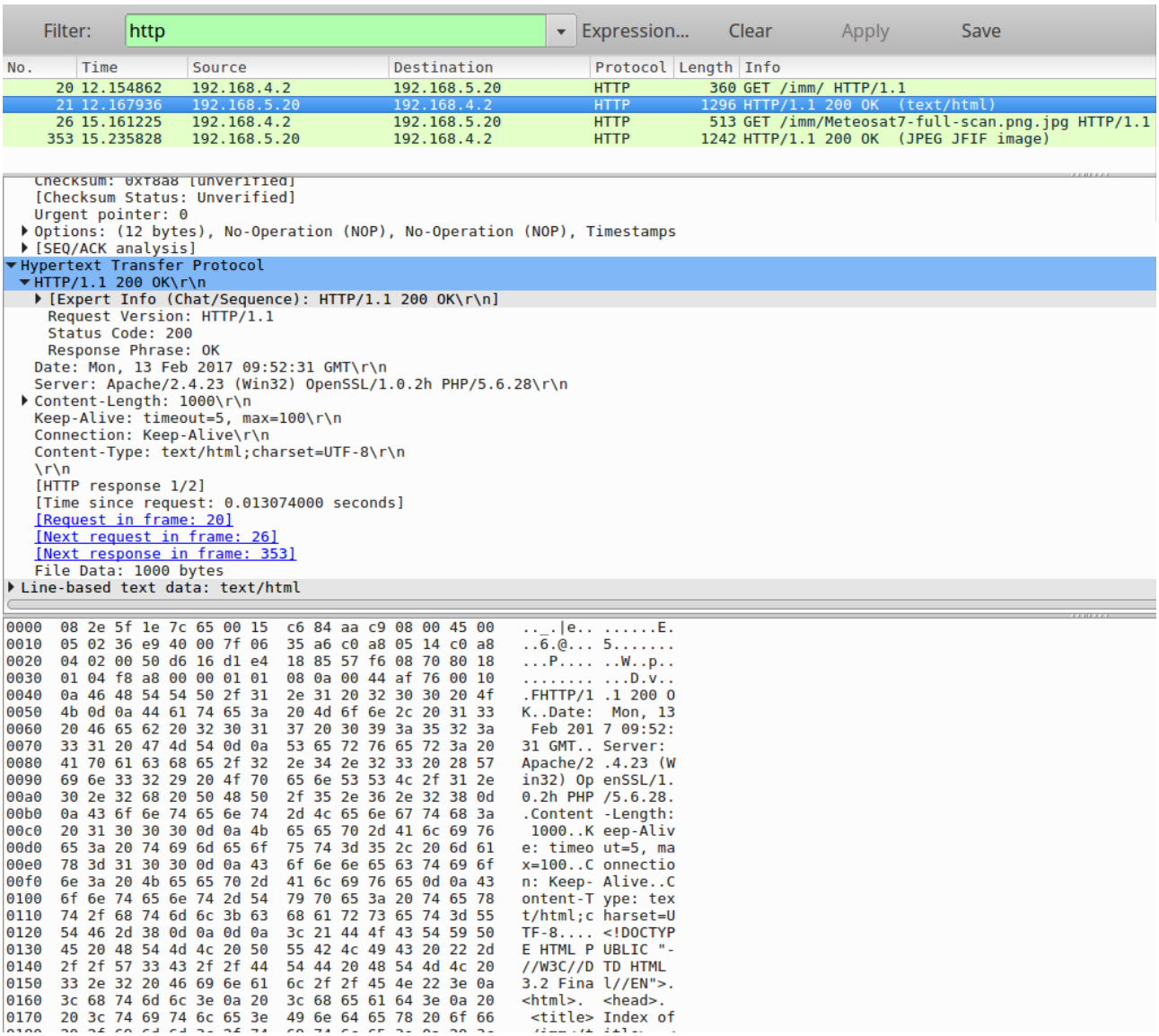
How both IP and MAC addressing schemes are effectively used in order to transmit data through different networks/subnets

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. Inorder 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 upto 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 form the router using the physical layer to transmit bits as electrical signals.

Web surfing: Downloading web contents



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.