Lab Assignment 1

Network Security VT2020

27-02-2020

Stockholm University

Submitted by:

Ranjana Ghimire, Efstathios Psyllakis, Justas Narusas

Group 221

2.1 The Network Simulation Environment

What is network simulation?

Basically simulation is the mirroring technique which represents the real life networking scenario though application . In this case, network simulation imitates the behavior of network scenario which it does by providing the interactions among the different network entities.[1]

What is host virtualization?

Virtualization, as the word depicts, represents/creating it in a virtual environment. Because of not needing as many hardware resources, virtualization is quite popular in the current IT scenario. Knowing or unknowingly , we have been working with virtual environments for example, in some earlier subject labs, we worked in Oracle Virtual Box which is a full virtualization implementation.

What are the differences between simulation, emulation and virtualization?

In simple terms, emulation executes the code which was meant for different architecture by changing the ASM language in term that the existing system' s CPU is able to process it.[2] This is performed in a different system than it was actually meant to be executed on.

Simulation, developed on top of emulation, is a scenario where you replicate the physical scenario in software applications. It is more of a software tool.

Virtualization is built on top of emulation concept as well but rather than just involved in executing code, virtualization is more focused on creating a virtual environment.

What is GNS3? What are the main parts of its GUI?

GNS3 is a network simulator application which we were familiarized with in Lab 1. GNS3 allows you to combine different tools in place including virtual machines, hubs , switches , hosts as well as routers. [3] The main parts of GUI include :- Workspace, Topology Summary, Servers Summary, GNS3 console and Device Toolbar.

3. Ethernet Frame Forwarding

3.1 Question 1

How many Ethernet adapters does the Windows 7 system have?

3 adapters

What are their name(s)/identifier(s)?

Local Area Connection
Tunnel Adapter isatap.
Tunnel Adapter Teredo Tunneling Pseudo-Interface

What does a network adapter represent?

The connections which are available to the hosts.

3.1 Question 2

What is the MAC address of these adapter(s)?

Local Area Connection: 08-00-27-18-26-A7
Tunnel Adapter Isatap: 00-00-00-00-00-00-00-E0
Tunnel Adapter Teredo Tunneling Pseudo-Interface: 00-00-00-00-00-00-00-EO

Based on the MAC value, can you identify the vendor of the network card(s)?

Intel for Local Area Connection: Intel is the vendor.
Tunnel Adapter Isatap: Microsoft is the vendor.
Tunnel Adapter Teredo Tunneling Pseudo-Interface: Teredo is the vendor for the last adapter.

What is a MAC address?

Mac address is the physical address of a host.

3.2 Question 3

How many Ethernet adapters does the system have?

The system has one adapter.

What are their name(s)/identifier(s)?

The name is eth5.

3.2 Question 4

What is the MAC address of the adapter(s)?

The MAC address of the adapter is 08:00:27:18:26:b0.

Which is the vendor of the network card(s)?

The vendor of the network card was not displayed by performing the ifconfig command.

3.2 Question 5

How can the MAC address of an adapter be used in network security?

We can use the MAC address of the adapter to create a simple MAC address filtering system and allowing only the required MAC addresses to pass through the network and deny access for the remaining MAC addresses.

3.3 Question 6

In which layer of the OSI model do Ethernet switches commonly operate?

An Ethernet switch operates at the **data link layer** (**layer 2**) of the OSI model to create a separate collision domain for each switch port.

3.3 Question 7

Examine the statistics of the port's column. How many frames have been sent? How many bytes in total?

Port 0: 3 frames sent, 180 bytes in total.

3.3 Question 8

Examine the MAC address table of your switch. What entry has been created?

Eth0 (windows): 08:00:27:97:d8:a6
Eth1(linux): 08:00:27:a7:42:6d

3.9 Question 9

Are the transmitted frames also captured on the link of the 'Kali' VM? Explain why or why not? Thoroughly explain your answer.

No, because the destination Mac address is used for windows.

4 Network Layer Packet Forwarding

4.1 Question 1

What does the above (sudo ping -l 51020 -f -s 51020 -a 127.0.0.1) ping command do?

-s -> Sends packet size of 51020
-l -> preloads packet size of 51020
-f -> requesting ICMP requests to prevent fragmentation
-a -> resolves the IP address
This command will send the non fragmented ICMP packets of 51020 size to localhost (128.0.0.1).

4.1 Question 2

Which network protocol does the ping utility use to craft the ping request and response packets?

Internet Control Message Protocol (ICMP)

On which layer of the TCP/IP stack does this network protocol belong?

TCP/IP belongs to the network layer of the OSI model.

4.2 Question 3

How many ping requests did the 'Windows7' system send?

4 ping requests were sent.

What options did you use?

We have used Ping command and destination IP. **Ping <destination IP>**

How many bytes of data did each request carry?

Each request carried 32 bytes.

What was the TTL value used, and what does the TTL abbreviation stand for?

TTL value used was 64.
TTL abbreviation stands for: “Time to live” [4]

What was the packet loss rate?

The packet loss rate was 0%.

What was the average round trip time (RTT)?

The average round trip time was 0ms.

4.2 Question 4

How many ping requests did the ‘LinuxClient’ system send (until you’ve decided to stop it)?

10 ping requests were made as we cancelled it after a short time.

What options did you use?

We have used ping commands and destination IP. **Ping <destination IP>**

How many bytes of data each request carried?

64 bytes each request.

What was the TTL value used?

The TTL value used was 128.

What were the packet loss rate and the average round trip time (RTT)?

The packet loss rate was 0% and the average round trip time was1.727ms.

4.3 Question 5

Which protocols are employed for sending a ping request from one system to another?

The Internet Control Message Protocol (ICMP) is employed.

Can you describe the order of protocol encapsulation applied according to the TCP/IP or OSI model?

Source Layer	Data	Destination Layer	Encapsulation Description
Application	Data	Application	Convert message to data
Presentation	Data	Presentation	
Session	Data	Session	
Transport	Data TCP	Transport	Converts data into segments
Network	Data TCP IP	Network	Converts segments to packets
Datalink	Data TCP IP Ethernet	Datalink	Converts packets to frames
Physical	111100000011111000011	Physical	Converts frames to binary

What are the values for the type and code fields of the ping request?

The type value was 8.
The code fields value was 0.

What is the ID value of the IP packet?

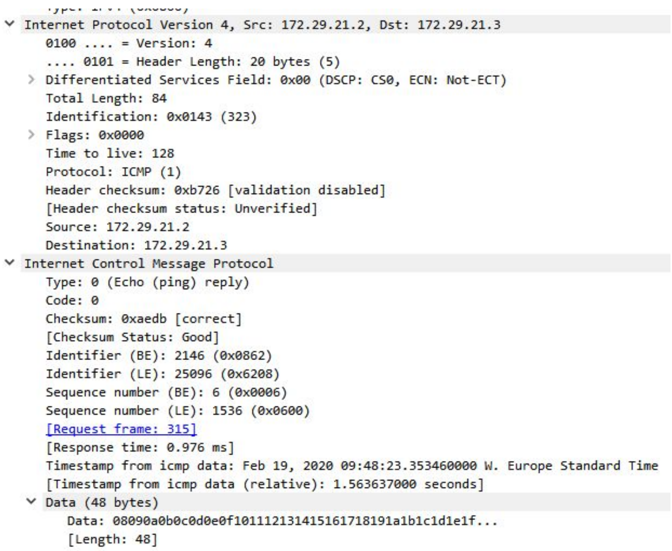
The ID value of the IP packet was *0X0000 (0)*.

What is the type of the Ethernet frame?

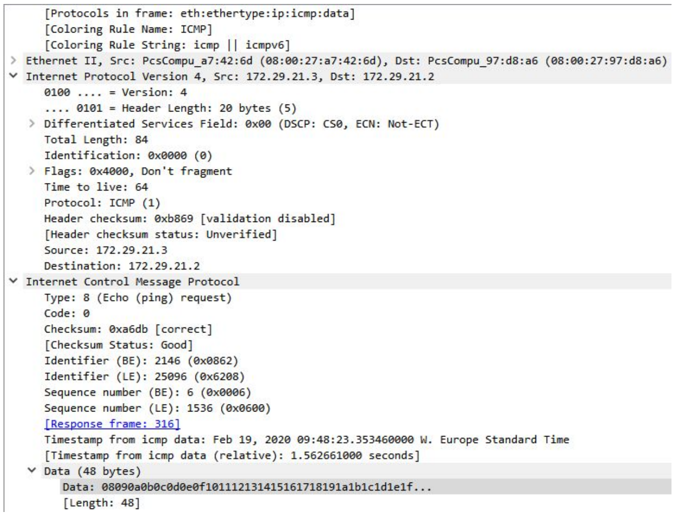
The ethernet frame type is Ethernet II.

4.3 Question 6

Highlight a ping reply packet below the previously selected frame. Examine the values of all protocol fields and compare them with those of a ping request packet. Which fields have the same value between them?



```
Internet Protocol Version 4, Src: 172.29.21.2, Dst: 172.29.21.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x0143 (323)
  > Flags: 0x0000
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0xb726 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.29.21.2
    Destination: 172.29.21.3
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xaedb [correct]
    [Checksum Status: Good]
    Identifier (BE): 2146 (0x0862)
    Identifier (LE): 25096 (0x6208)
    Sequence number (BE): 6 (0x0006)
    Sequence number (LE): 1536 (0x0600)
    [Request frame: 315]
    [Response time: 0.976 ms]
    Timestamp from icmp data: Feb 19, 2020 09:48:23.353460000 W. Europe Standard Time
    [Timestamp from icmp data (relative): 1.563637000 seconds]
  Data (48 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
      [Length: 48]
```



```
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
> Ethernet II, Src: PcsCompu_a7:42:6d (08:00:27:a7:42:6d), Dst: PcsCompu_97:d8:a6 (08:00:27:97:d8:a6)
Internet Protocol Version 4, Src: 172.29.21.3, Dst: 172.29.21.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x0000 (0)
  > Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xb869 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.29.21.3
    Destination: 172.29.21.2
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xa6db [correct]
    [Checksum Status: Good]
    Identifier (BE): 2146 (0x0862)
    Identifier (LE): 25096 (0x6208)
    Sequence number (BE): 6 (0x0006)
    Sequence number (LE): 1536 (0x0600)
    [Response frame: 316]
    Timestamp from icmp data: Feb 19, 2020 09:48:23.353460000 W. Europe Standard Time
    [Timestamp from icmp data (relative): 1.562661000 seconds]
  Data (48 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
      [Length: 48]
```

Code: 0
Identifier (BE) : 2146
Identifier (LE) : 25096
Sequence Number (BE) : 6
Sequence Number (LE) : 1536

What are the values for the type and code fields of the ping request?

Type=0
Code fields=0

What is the ID value of the IP packet?

0X0143 (323)

4.4 Question 7

What does ARP stand for?

ARP stands for Address Resolution Protocol.

In which layer of the TCP/IP stack does it belong?

Network/Link Layer.

Briefly describe its main function.

The main function of ARP is to create a mapping from MAC address to IP address and vice-versa.

Briefly describe and explain why this protocol is important in a switched network.

An IP address is a layer-3 address. Layer-3 packets get encapsulated into layer-2 frames, and layer-2 also has addressing (MAC addresses) which needs to be supplied. ARP (Address Resolution Protocol) resolves the layer-3 IP address to a layer-2 MAC address so that the layer-3 packet can be encapsulated into a layer-2 frame which is then sent out the layer-1 interface.

4.4 Question 8

What is the destination MAC address? Briefly explain this.

00:00:00:00_00:00:00 (00:00:00:00:00:00:00)
Since network host is not determined in request packet so all the mac is blank values

4.4 Question 9

Examine the ARP reply packet. What is the source MAC address of the frame and to which network host does it belong?

08:00:27:97:d8:a6 and it belongs to Windows server.

Does the ARP reply contain valid data?

Yes , all relevant values of windows host

4.4 Question 10

Does the ‘LinuxClient’ VM have an entry about the ‘Windows7’ VM?

Yes

What data about the remote machine does this entry have?

? (172.29.21.2) at 08:00:27:97:d8:a6

4.4 Question 11

Reissue the ping command at the 'LinuxClient' VM to the 'Windows7' one and examine the packet capture of the 'LinuxClient' VM's link. Can you find any ARP request packets this time? Why or why not?

Yes . with the earlier command arp -a , we setup arp value and in the next ping arp was called.

4.5 Self Assessment

What is the ping utility?

Ping , basically is a function that uses ICMP to check network reachability and connectivity. PING stands for Packet Internet Groper.[6]

What network protocol does it use?

ICMP

Are there differences in how a network protocol is implemented by different operating systems / applications?

The core logic is similar however implementation differs from OS to OS. Like for example , ping utility results and behaves differently in windows and Linux even though the logic is the same.

What is a network protocol header?

The Network protocol header or IP header is the beginning of an ip packet which contains the base / metadata of the packet.

What data might it contain?

- Version
- Header Length
- Priority and Type of Service
- Total Length
- Identification
- Flags
- Fragmented offset
- Time to live
- Protocol
- Header checksum
- Source IP
- Destination IP
- Option

How it can be used for security purposes (+/-)?

Authentication header can be used to provide data integrity.

What is the ARP protocol and what is its main function?

Address routing protocol is something like an address book, kind of a way we add a person's name with phone number. ARP maps IP address with MAC address.

What is the ARP cache that an OS maintains?

Collection of ARP entries

How is it populated and used?

It gets created after successful resolution of IP address to MAC address.

5.1 Question 1

Have the commands completed successfully? Why or why not?

21 port permission was denied while 30000 was doing nothing after executing the command

If a command has failed, how can the command be made to work?

21 doesn't work but works with sudo as it is a default FTP port.
30000 works

What does the ‘l’ parameter mean?

Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host. It is an error to use this option in conjunction with the -p, -s, or -z options. Additionally, any timeouts specified with the -w option are ignored.

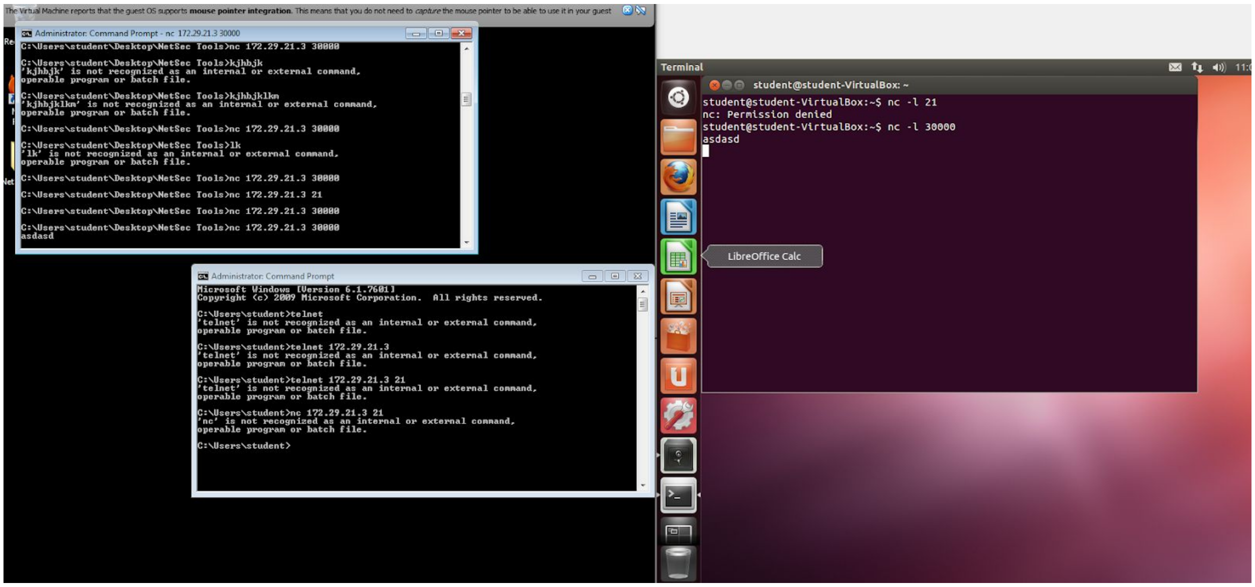
5.2 Question 2

C:\Users\student > nc 172.29.21.3 21

Which transport layer protocol has been used for communication?

TCP

Provide a screenshot showing that the communication has been properly established.


The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest
Administrator: Command Prompt - nc 172.29.21.3 30000
Administrator: Command Prompt
Terminal
student@student-VirtualBox: ~
LibreOffice Calc

```
C:\Users\student\Desktop\NetSec Tools>nc 172.29.21.3 30000

C:\Users\student\Desktop\NetSec Tools>kjhbjk
'kjhbjk' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student\Desktop\NetSec Tools>kjhbjklkm
'kjhbjklkm' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student\Desktop\NetSec Tools>nc 172.29.21.3 30000

C:\Users\student\Desktop\NetSec Tools>lk
'lk' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student\Desktop\NetSec Tools>nc 172.29.21.3 30000

C:\Users\student\Desktop\NetSec Tools>nc 172.29.21.3 21

C:\Users\student\Desktop\NetSec Tools>nc 172.29.21.3 30000

C:\Users\student\Desktop\NetSec Tools>nc 172.29.21.3 30000
asdasd
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Users\student>telnet 172.29.21.3
'telnet' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student>telnet 172.29.21.3 21
'telnet' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student>nc 172.29.21.3 21
'nc' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student>
```

```
student@student-VirtualBox:~$ nc -l 21
nc: Permission denied
student@student-VirtualBox:~$ nc -l 30000
asdasd
```

What are the client and server ports?

Windows: 49165
Server : 30000

How many packets flow from client to server and how many vice-versa?

2 packets , one from each machine.
In our situation packet 430 and packet 431

How many bytes are sent in each direction and in total?

115 bytes in total
61 bytes from windows and 54 bytes from linux

5.3 Question 3

Has the connection been established?

No

What combination of transport layer flags was enabled in the 'LinuxServer' VM's reply?

Syn flag was only set, everything else was not set

What are the client and server ports now?

Windows has 49166 and linux has 300000

5.4 Question 4

What are the client and server ports in each established session?

49167 -> 30000
49168 - > 30001

Can you recover the exchanged text using Wireshark?

Yes, we can see the message in the last 9 bytes of the “Packet Bytes” part of Wireshark

5.5 Question 5

Which fields and values of the captured packets give you an idea of which is the client and which is the server in each individual session?

In the IPV4 section, Src and Dst field gives us the idea about which is client and which is server

Identify which VM is the client and which the server?

Packet 519-520
Source: 179.29.21.3 Windows
Destination: 179.29.21.2 LinuxServer

Packet 525-526
Source: 179.29.21.2 LinuxServer
Destination: 179.29.21.3 Windows

5.6 Question 6

Has the session been successfully established?

The session has been established with UDP protocol

Why or why not?

No it did not work because windows was open in udp port while linux was trying to connect to tcp port

What does the ‘u’ argument specify?

Use UDP instead of the default option of TCP. For UNIX-domain sockets, use a datagram socket instead of a stream socket. If a UNIX-domain socket is used, a temporary receiving socket is created in /tmp unless the -s flag is given.

5.7 Question 7

Has communication been successful?

Yes
The session was not connected with **nc server port** but it connected when we specifically mentioned -u parameter while making connection from windows.

Which transport layer protocol is used?

UDP

How many packets have been exchanged and in which direction?

1 packet was only used for communication from Linux to windows

5.7 Question 8

What are some major differences between the experiments with and without the ‘-u’ parameter?

The TCP is transferring packets and data flow via flags while UDP is straightforward without exchanging flags.

5.8 Transport Layer: Self-assessment Questions

What is a network port and what is its role?

A communication endpoint for a process or an application. It creates a communication channel

How many ports can a host have and what is the possible range of values?

A host can have 65535 of TCP and 65535 of UDP ports and port ranges from 0-65535 (Port 0 is reserved so not counted)[7]

What are the most prominent transport layer protocols and which are their major differences and usage scenarios?

TCP and UDP are the most prominent transport layer protocols.

- TCP is connection oriented protocol while UDP is connectionless.
- Data sent through TCP is guaranteed to be delivered so it is more reliable, not the case with UDP
- TCP uses flow control, UDP uses continuous stream
- TCP is slower than UDP because of more steps to be performed.

TCP is used in HTTP, HTTPS,SSH,SMTP
UDP is used in video streaming, Online Games, DNS, VPN Tunnelling

Describe the client-server communication model applied by transport layer protocols.

The communication starts with the user (client server) entering the url. The DNS server looks up the address of the web server and responds with the found address. Browser sends the HTTPS/HTTP request to the web server's IP . Server sends the response. Browser renders the files sent via server and website gets available in client site.

6 Application Layer

6.1 Question 1

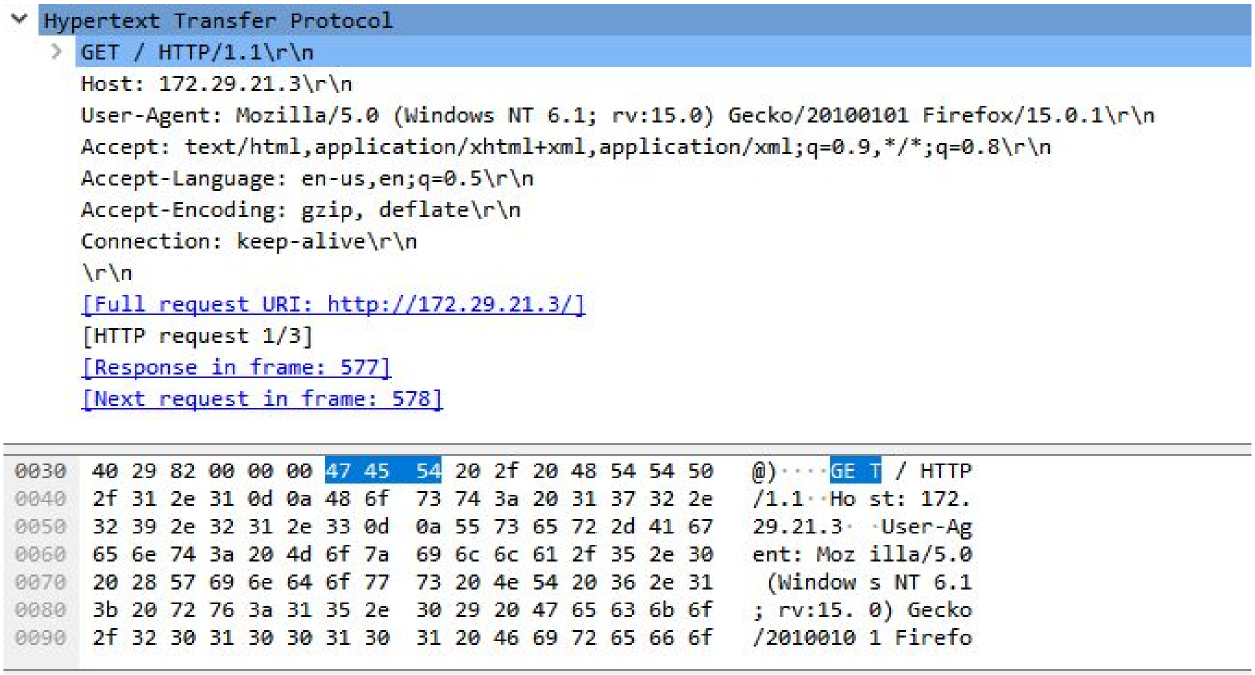
Which application layer protocol is used?

ARP , TCP and HTTP

Can you identify a packet that carries the initial web request?

Yes , it is the first HTTP get request which was captured running in packet 575

Write down which metadata fields appear in the request and what their value means?



```
⌄ Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: 172.29.21.3\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:15.0) Gecko/20100101 Firefox/15.0.1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://172.29.21.3/]
    [HTTP request 1/3]
    [Response in frame: 577]
    [Next request in frame: 578]
```

```
0030  40 29 82 00 00 00 47 45  54 20 2f 20 48 54 54 50   @)····GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 37 32 2e   /1.1··Ho st: 172.
0050  32 39 2e 32 31 2e 33 0d  0a 55 73 65 72 2d 41 67   29.21.3· ·User-Ag
0060  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
0070  20 28 57 69 6e 64 6f 77  73 20 4e 54 20 36 2e 31    (Window s NT 6.1
0080  3b 20 72 76 3a 31 35 2e  30 29 20 47 65 63 6b 6f   ; rv:15. 0) Gecko
0090  2f 32 30 31 30 30 31 30  31 20 46 69 72 65 66 6f   /2010010 1 Firefo
```

6.1 Question 2:

Can you identify the packet that carries the response?

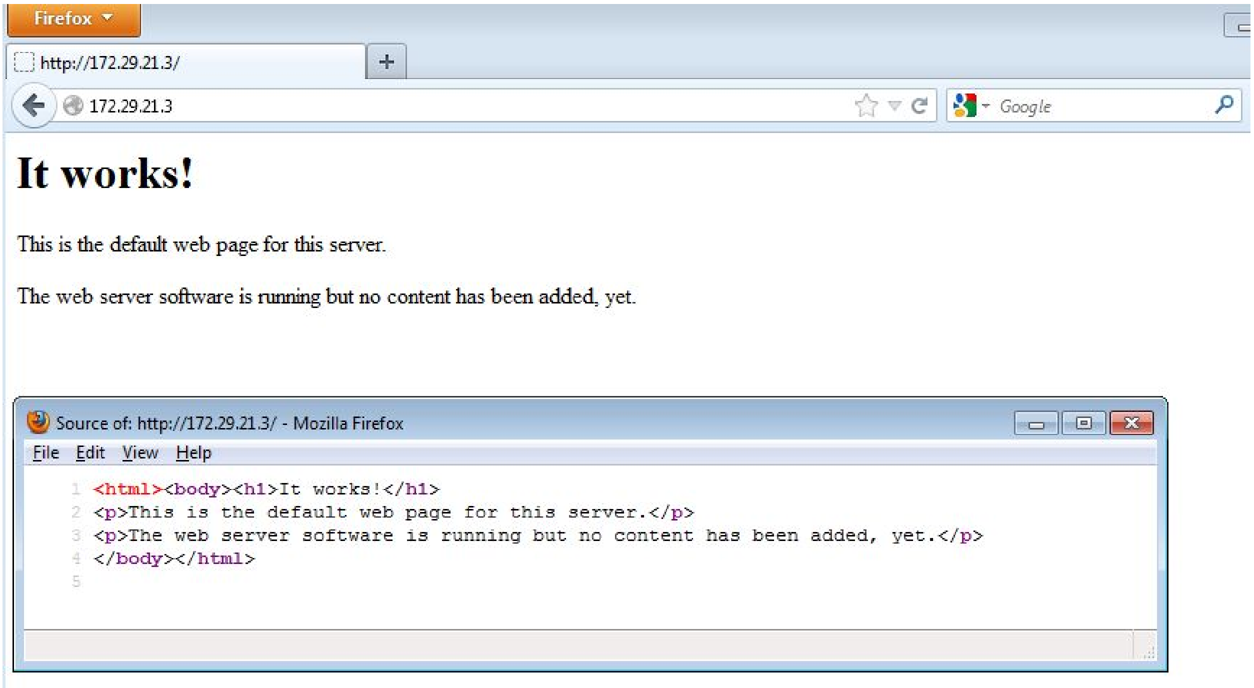
Three responses were identified coming from HTTP protocol

Can you identify any interesting metadata fields?

The second and third response was 404 Not found even though the apache was working.

Can you extract the transmitted HTML code of the visited web page?

We can extract by going on the web page , right click and view page source, the output was as follow:



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

```
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>
```

6.2 Application Layer: Self-assessment Questions

What are some common application layer protocols?

TELNET,FTP,SMTP,DNS,DHCP

How can you use a network protocol analyzing tool to extract and parse data about an application layer protocol?

By Capturing and analysing signals and data traffic over communication line (We used Wireshark)

7 IP Addressing and Subnets

IP address range of 172.29.X.0 and a subnet mask of 255.255.255.0 (/24 in CIDR notation), 172.29.21.0

172.29.21	**00000000**	**172.29.21.0**
172.29.21	**00000001**	**172.29.21.1**
172.29.21	**00000010**	**172.29.21.2**

...	**...**	**...**
172.29.21	**11111110**	**172.29.21.254**
172.29.21	**11111111**	**172.29.21.255**

Question 1

What is the lowest and the highest IP address that belong in this IP address range?

172.29.21.0

What is the broadcast address of this IP address range?

172.29.21.255

How many hosts can your network support?

256-2=254

Question 2

Write down the IP address that you have manually assigned to the 'Windows7' VM. Identify the network ID of this IP address as well as the host ID of it.

172.29.21.2

Question 3

Splitting the above IP address range in half, gives you two smaller subnets, each with a subnet mask of /25 (i.e. 255.255.255.128). ***What is the IP address range and the broadcast address of each subnet?***

IP ranges from 172.29.21.0-172.29.21.127 for subnet 1
Ip ranges form 172.29.21.128-172.29.21.155 for subnet 2

How many hosts can they support each?

Each of them can accumulate 126

Pick one IP address belonging to each subnet and write them down along with their network ID and host ID.

Subnet 1

172.29.21	**00000000**	**172.29.21.0**
172.29.21	**00000001**	**172.29.21.1**
172.29.21	**00000010**	**172.29.21.2**
...	**...**	**...**
172.29.21	**01111110**	**172.29.21.126**
172.29.21	**01111111**	**172.29.21.127**

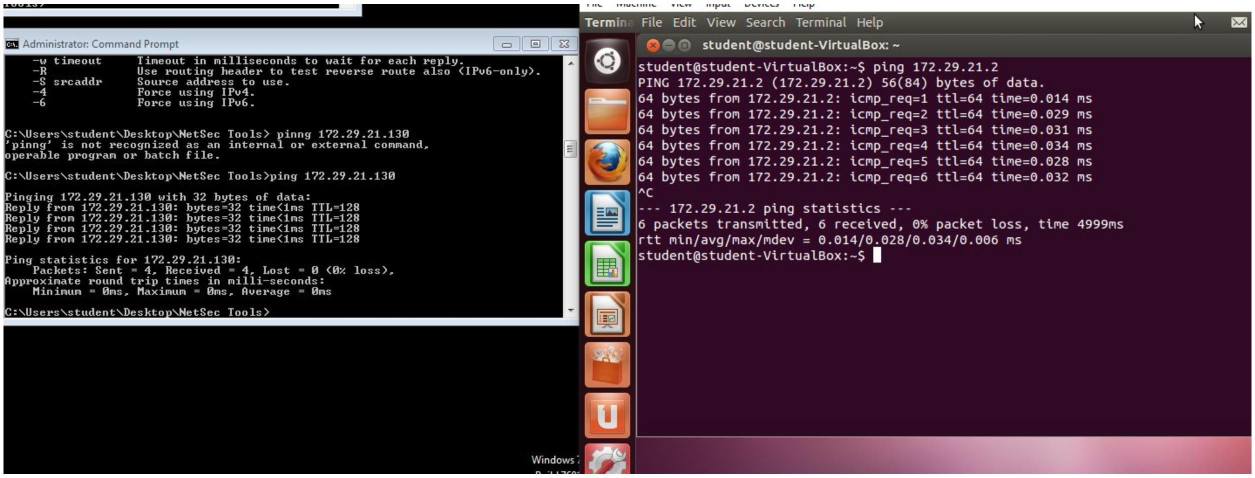
Subnet 2

172.29.21	**10000000**	**172.29.21.128**
172.29.21	**10000001**	**172.29.21.129**
172.29.21	**10000010**	**172.29.21.130**
...	**...**	**...**
172.29.21	**11111110**	**172.29.21.254**
172.29.21	**11111111**	**172.29.21.255**

7.1 Question 4

Is the ping successful? Why or why not? Can you capture ping packets on any of the links?

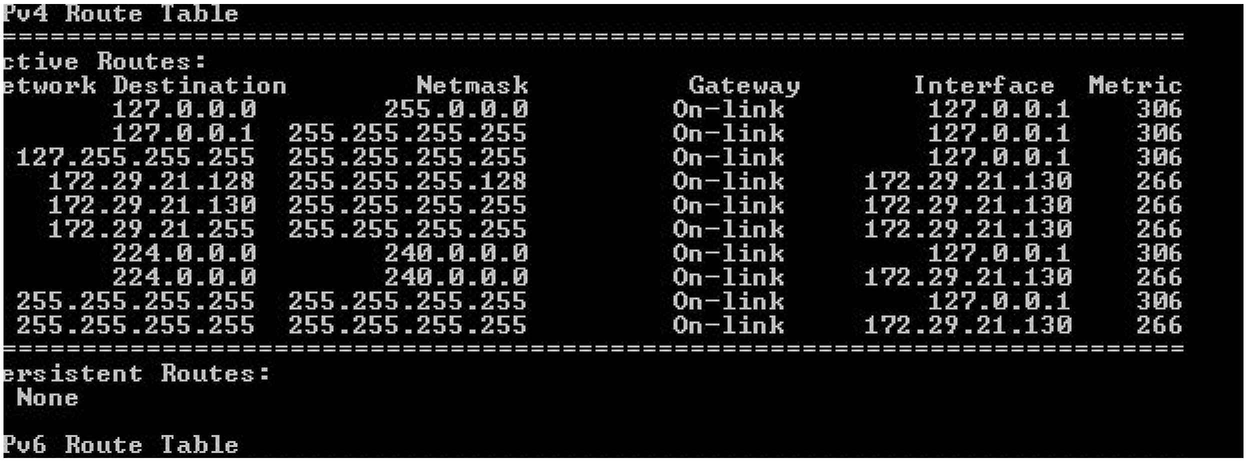
Its successful as they are in different subnet connected via switch
We captured following details:


Administrator: Command Prompt
Terminal File Edit View Search Terminal Help
student@student-VirtualBox: ~
Windows 7

```
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.


C:\Users\student\Desktop\NetSec Tools> pinng 172.29.21.130
'pinng' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student\Desktop\NetSec Tools>ping 172.29.21.130

Pinging 172.29.21.130 with 32 bytes of data:
Reply from 172.29.21.130: bytes=32 time<1ms TTL=128
Reply from 172.29.21.130: bytes=32 time<1ms TTL=128
Reply from 172.29.21.130: bytes=32 time<1ms TTL=128
Reply from 172.29.21.130: bytes=32 time<1ms TTL=128

Ping statistics for 172.29.21.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\student\Desktop\NetSec Tools>
```

```
student@student-VirtualBox:~$ ping 172.29.21.2
PING 172.29.21.2 (172.29.21.2) 56(84) bytes of data.
64 bytes from 172.29.21.2: icmp_req=1 ttl=64 time=0.014 ms
64 bytes from 172.29.21.2: icmp_req=2 ttl=64 time=0.029 ms
64 bytes from 172.29.21.2: icmp_req=3 ttl=64 time=0.031 ms
64 bytes from 172.29.21.2: icmp_req=4 ttl=64 time=0.034 ms
64 bytes from 172.29.21.2: icmp_req=5 ttl=64 time=0.028 ms
64 bytes from 172.29.21.2: icmp_req=6 ttl=64 time=0.032 ms
^C
--- 172.29.21.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.014/0.028/0.034/0.006 ms
student@student-VirtualBox:~$
```

7.2 Question 5



```
Pv4 Route Table
===========================================================================
ctive Routes:
etwork Destination        Netmask          Gateway       Interface  Metric
         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
     172.29.21.128  255.255.255.128         On-link     172.29.21.130    266
     172.29.21.130  255.255.255.255         On-link     172.29.21.130    266
     172.29.21.255  255.255.255.255         On-link     172.29.21.130    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     172.29.21.130    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     172.29.21.130    266
===========================================================================
ersistent Routes:
 None

Pv6 Route Table
```

Destination	Netmask	IP AND Netmask (A)	IP Address(B)	Is a Match?(A=B)
127.0.0.1	255.0.0.0	127.0.0.1	127.0.0.0	No
127.0.0.1	255.255.255.255	127.0.0.1	127.0.0.1	Yes
127.0.0.1	255.255.255.255	127.0.0.1	125.255.255.255	No
172.29.21.130	255.255.255.128	172.29.21.128	172.29.21.128	Yes
172.29.21.130	255.255.255.255	172.29.21.130	172.29.21.130	Yes
172.29.21.130	255.255.255.255	172.29.21.130	172.29.21.255	No
127.0.0.1	240.0.0.0	127.0.0.0	224.0.0.0	No
172.29.21.130	240.0.0.0	172.0.0.0	224.0.0.0	No

127.0.0.1	**255.255.255.255**	**127.0.0.1**	**255.255.255.255**	**No**
172.29.21.130	**255.255.255.255**	**172.29.21.130**	**255.255.255.255**	**No**

Is there any matching entry?

Yes , there are 3 matches.

What is the IP address range of systems with which the ‘Windows7’ system can communicate?

172.29.21.0-172.29.21.255

7.3 Subnetting: Self-assessment Questions

In terms of subnetting, what are the parts that compose an IP?

Network and Host

Why are subnets useful?

To relieve Network congestion

What elements are needed to describe a subnet?

- Number of subnets present
- Number of hosts needed
- Class of network
- A base IP address

How are IP addresses and subnet masks combined to form networks?

The class defines how remaining many bits can be used to define IP and subnet. In the remaining bits, the number of subnets define how many remaining bits can be used for host definition. The remaining last bits define the host within the subnet.

How does a host use its network configuration to make forwarding decisions?

There are 3 scenarios:

1. It pings to itself for loopback
2. It transfers within the network
3. It transfers in remote host

8 Basic Internetworking

8 Question 1

Issue a ping command from one VM to another. Is the ping completed successfully?

The ping was not successful.

Why or why not?

They are in two separate networks

If not how can the problem be solved? Which entry has been added to the VMs' host routing tables?

We will need to add routing protocol in the router to make sure the communication is possible between two servers in different subnet.

9 Application Layer Protocols (DHCP and DNS)

9.1 Question 1

What port does the DNS server use for communication?

Source port in windows is 63346 which is being used by dns server while it is replying from port 53.

Which transport layer protocol is used?

DNS protocol is used.

Which flag(s) did the DNS query header have enabled and what is the Transaction ID?

Flags :
Transaction ID: 0x0100
Of which type is the query?
Standard query, type A, class IN

9.1 Question 2

Which flag(s) are enabled on the DNS response header and what is the Transaction ID?

Transaction id: 0x87d4
Flag: 0x8580

What is the Time to Live value of the answer?

The TTL value is 64/

Which IP address does the DNS reply point to?

172.29.21.4

9.2 Question 3

Can the ‘LinuxClient’ VM that is on a different network access ‘www.example.com’?

Yes, it can access it.

Why or why not?

Because they are in the same network and the DNS server as well as web server are active in the Linux server.

REFERENCES

1. Daniel Aarno, Jakob Engblom, 2015 , accessed 24 March 2020 https://www.sciencedirect.com/topics/computer-science/network-simulation
2. TEC Team, May 22 2019, Accessed on 26 February 2020 https://www3.technologyevaluation.com/sd/category/virtualization-virtual-machine/articles/virtualization-vs-emulation-vs-simulation
3. Andrew Coleman, Julien Duponchelle , December 24, 2019 , Accessed on 17 February 2020 https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html
4. Accessed on 17 February 2020 *https://en.wikipedia.org/wiki/Time_to_live*
5. Accessed on 1 March 2020 https://www.javatpoint.com/ping-full-form
6. Accessed on 1 March 2020 https://www.sciencedirect.com/topics/computer-science/registered-port