German University in Cairo
DMET Department
Associate Prof.Amal ElNahas

Practical
Networks and Media Lab
MET Manual

Spring semester 2012

Contents

Lab Overview

1 Objectives

- Acquire practical understanding of the underlying concepts and principles of computer networks and network protocols.
- Understanding different network components, how they interact together to provide different application services
- Be familiar with different applications (video streaming, multicasting, mobile IP,..)

2 Experiments

The course consists of 8 experiments. The experiments cover many network protocols that span all network layers.

- Experiment 1: Streaming Technologies
- Experiment 2: Application and Link Layer Protocols
- Experiment 3: Network simulator (NS2)
- Experiment 4: Video conferencing system
- Experiment 5: Video streaming
- Experiment 6: QoS and Traffic Engineering
- Experiment 7: Mobile-IP
- Experiment 8: ns2 - Wireless Transmission

3 Lab Organization

- The lab consists of the 8 experiments, 4 of them are duplicated, plus the 2 pre-experiments
- Students are to be working in groups of 2, each group is to perform one experiment per lab slot
- Each lab slot is composed of 4 hours
- Each group will have 1 week (before lab time) to prepare, answer the preparatory questions, and submit answers written
- An oral discussion is conducted by the experiment supervisor at the beginning of each experiment.
- Failing the oral discussion deprives you from attending the lab (and resulting in an F for this experiment)

- The week after, a written report should be submitted describing the experiments and results
- Whenever a student receives a total of three Fs, he will not be allowed to continue the course and will receive a total of F in this course.

4 Grading Policy

Evaluation is done throughout the term. Final grade is based on the sum of the 8 different grades (7 + 1) obtained through the term. Each grade is based on:

- Preparatory questions report
- Oral discussion + Experiment
- Results report

5 Lab Software Overview

All network experiments in the lab are controlled from the PCs that are running the Ubuntu 10.10 Linux operating system. A brief overview to Linux is presented below for those who are not familiar with such operating system. If you have worked on Linux before, you may quickly browse this section.

5.1 Linux Overview

5.1.1 Linux File System

Linux is a free Unix-like open-source operating system. Files are organized in a hierarchical tree of directories with the root directory denoted by / as in Figure 1.
Each file and directory in a Linux file system is uniquely identified by a pathname. Pathnames can be absolute or relative. Absolute pathnames start at the root directory. The absolute pathname of the root directory is a slash (/). In the file hierarchy in Figure 2, the absolute pathname of directory home in the root directory is /home, that of directory user1 in /home is /home/user1, and the absolute pathname of file data.txt in /home/user1 is /home/user1/data.txt. Pathnames that do not begin with a slash are relative pathnames and are interpreted relative to a current (working) directory. For example, if the current directory is /home, then the pathname user1/data.txt refers to the absolute pathname /home/user1/data.txt.
When using relative pathnames, a single dot (.) denotes the current directory and two dots (..) denote the parent directory, which is the directory immediately above the current directory. With the parent directory, it is feasible to identify each file with relative pathnames. In Figure 2, if the current directory is /home/user1, the relative pathname .. refers to directory /home, the pathname ../.. refers to the root directory, and the pathname ../user2/data.txt refers to the file /home/user2/data.txt.
Each Linux account has a home directory. For regular accounts, that is, accounts which are different from the root account, the home directories are located in /home. So, /home/user1 is the home directory for an account with login user1. The home

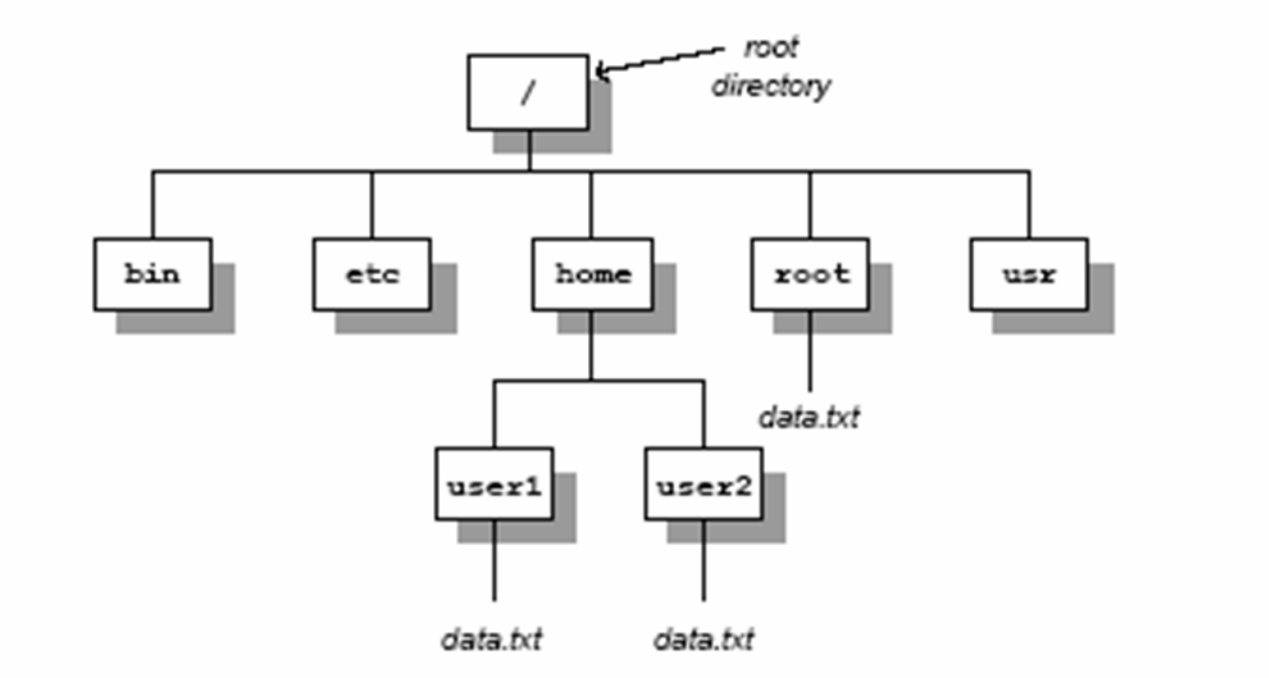


Figure 1: File Hierarchy System

directory of the root account is /root. When a new terminal window is created, the current directory in the terminal window is the home directory.
Linux configuration files are located in directories /etc, /usr/etc, /var and their subdirectories. Whenever you modify the configuration of a Linux system, you will work on files in these directories. Each file and each directory has an owner. A regular user only owns the home directory and all files created by the user. The root is the owner of all other files on the system (see Figure 2).
In Linux, each file has a set of access permissions. The permissions are read (r), write (w), and execute (x), and give, respectively, permission to read the contents of a file, modify the file, or execute the file as a program. Permissions are set by the owner of a file. Linux specifies access permissions separately for the owner of the file, a user group which is associated the file, and the set of all users. So, the owner of a file can set the permissions so that all users can read the files, but only the owner can modify the file. The root user can ignore all access permissions and can even change the ownership of files

5.1.2 Linux devices and network interfaces

Hardware devices, like disks, mouse and keyboard, are represented by device files which reside in the directory /dev. The software abstraction through which the Linux kernel accesses networking hardware is that of a network interface. For example, when assigning an IP address to an Ethernet interface cards, one manipulates the configuration parameters of the network interface which represents the Ethernet card. Just like other devices, each network interface is associated with a device driver.

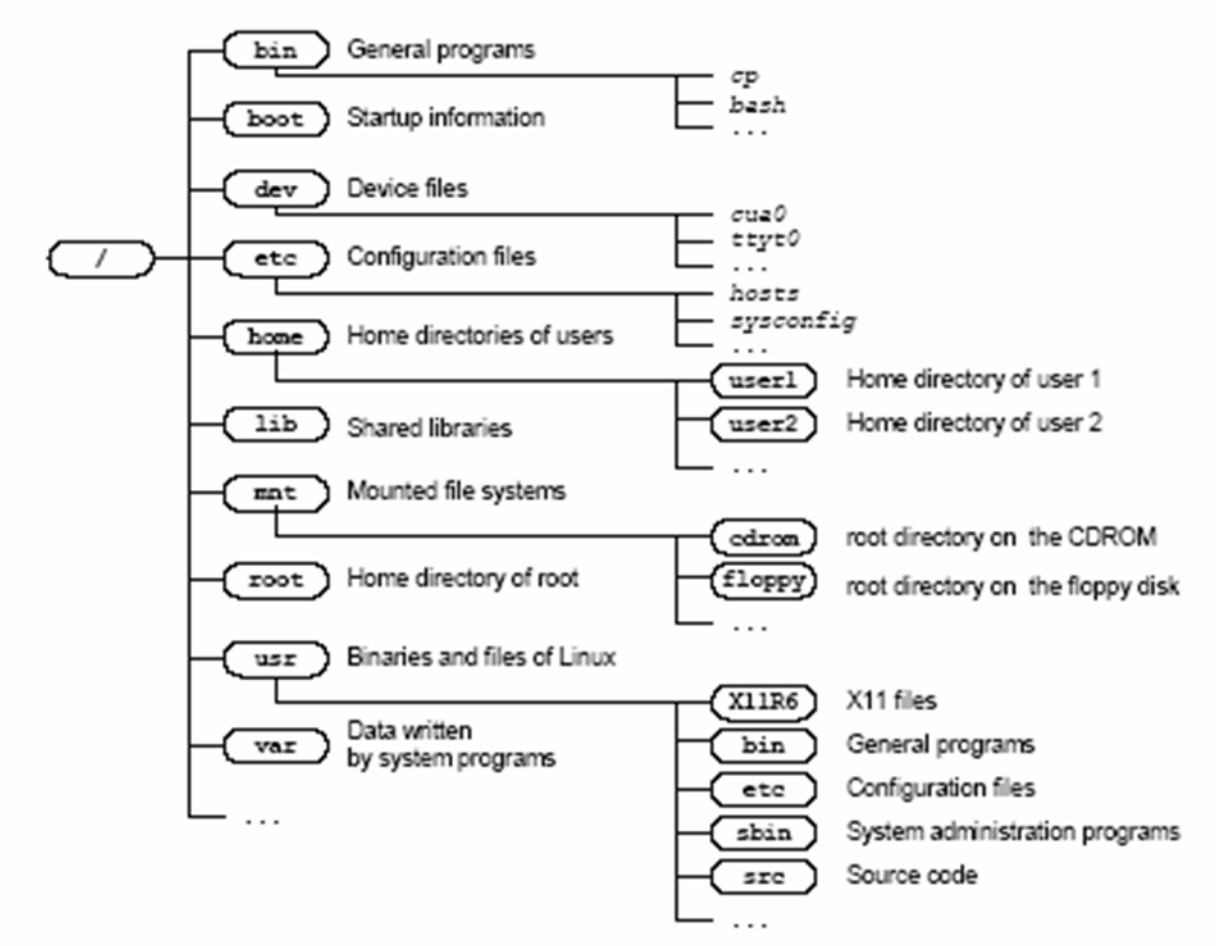


Figure 2: Directories Tree

In Linux, the names of network interfaces for Ethernet hardware are eth0 for the first Ethernet interface card, and eth1 for the second Ethernet interface card. There is a special network interface, the loopback interface, with name lo. The loopback interface is not connected to a real device, but is a virtual interface, which allows a PC to send messages to itself.

5.1.3 Linux Shell and Commands

The command line interface of the Linux operating system is called a Shell. A Shell is a program that interprets and executes Linux commands. The Shell displays a prompt at which the user can type commands. When you type a command at the prompt, and press the enter key, the Shell interprets the command, and, if it is a valid Linux command, executes the command. Linux offers a variety of Shell programs with names such as sh, csh, ksh, tcsh, or bash. For the purposes of the material covered here, the differences between these Shell programs are not relevant.
The only built-in help feature of a Linux system are the online manual pages for Linux commands, called the man pages. The man pages offer detailed information on a

command. Ex: man ls display manual page of command ls
Example of simple networking setup commands:

- `ifconfig` (for configuring the ethernet interface)
- `ifup`
- `ifdown`

5.2 Useful tools

5.2.1 ping command

One of the most simple, but also most effective, tools to debug IP networks is the ping command. Ping tests whether a given IP address is reachable by sending a short packet to an IP address and waits for a response from that IP address. The packets that are issued during a ping are ICMP Echo Request and an ICMP Echo Response messages. The ping command sends an ICMP Echo Request message to an interface with the specified IP address, and expects an ICMP Echo Response message in return. When issuing a ping command, a Linux system measures and displays the time between the transmission of the ICMP Echo Request and the return of the ICMP Echo Response. However, the main information provided by ping is not the time to receive a response, but whether a certain host is reachable at all. In most cases, if a ping command between two machines is successful, most Internet applications are likely to run without problems.

5.2.2 Network protocol analyzer (wireshark)

To make observations of the behavior of network protocols, we need to have tools that can monitor network traffic, and present the traffic in a human readable form. Tools that capture and display traffic on a network interface card are referred to as network protocol analyzers or packet sniffers. In the Network and Media Lab, you will extensively use wireshark which is a protocol analyzer with a graphical user interface that recognizes a large number of protocols. Wireshark main window, that is presented below, is divided into three parts as follows:

- `Packet list pane:` displays a summary of each packet captured. By clicking on packets in this pane you control what is displayed in the other two panes.
- `The packet details pane:` displays the protocols and protocol fields of the packet selected in the packet list pane in more detail.
- `The packet bytes pane:` displays the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane.

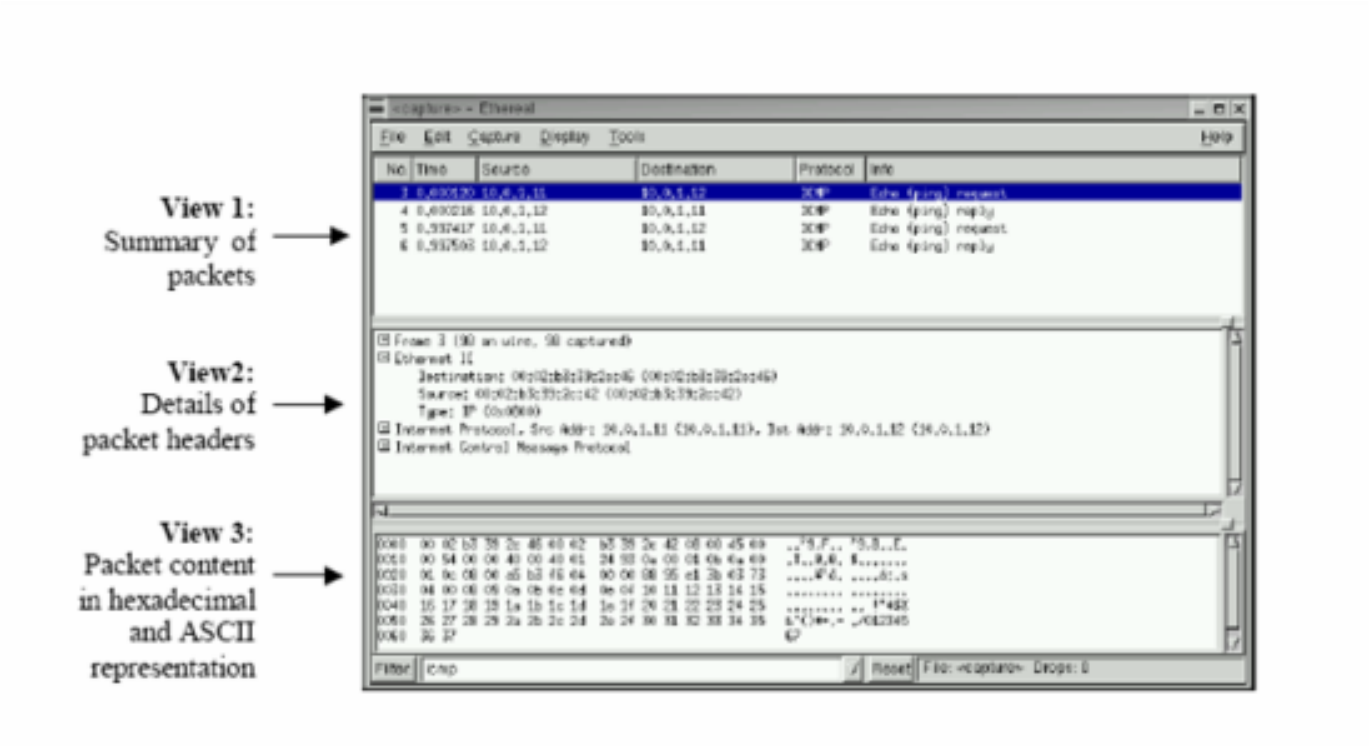


Figure 3: Wireshark

6 Lab Hardware Overview

The lab consists of 38 PCs, 2 routers, 2 hubs and 3 switches. Each PC has the Ubuntu 10.10 Linux operating system and one network interface card with an Ethernet port.

- The 3Com routershave 6 Ethernet interfaces operating at 100 Mbps
- The 2 switches in the lab, have 24 ports each where these ports are divided between 2 VLANs.
- The 2 hubs in the lab, each is 16 ports, and support data transmission at 10/100 Mbps. PCs and routers connected to the same hub forms a Local Area Network (Ethernet Segment)

General References

- The IP- addresses in this lab are built in the following way:172.x.y.z, where X is the test number; Y the subnet in the experiment and Z is a computer in the subnet.
- Computers with more than one network-Interface are defined in this lab as routers. The interfaces names in Linux are eth0, eth1, ...
- All RFCs are available on the internet under http://www.ietf.org/rfc.html.

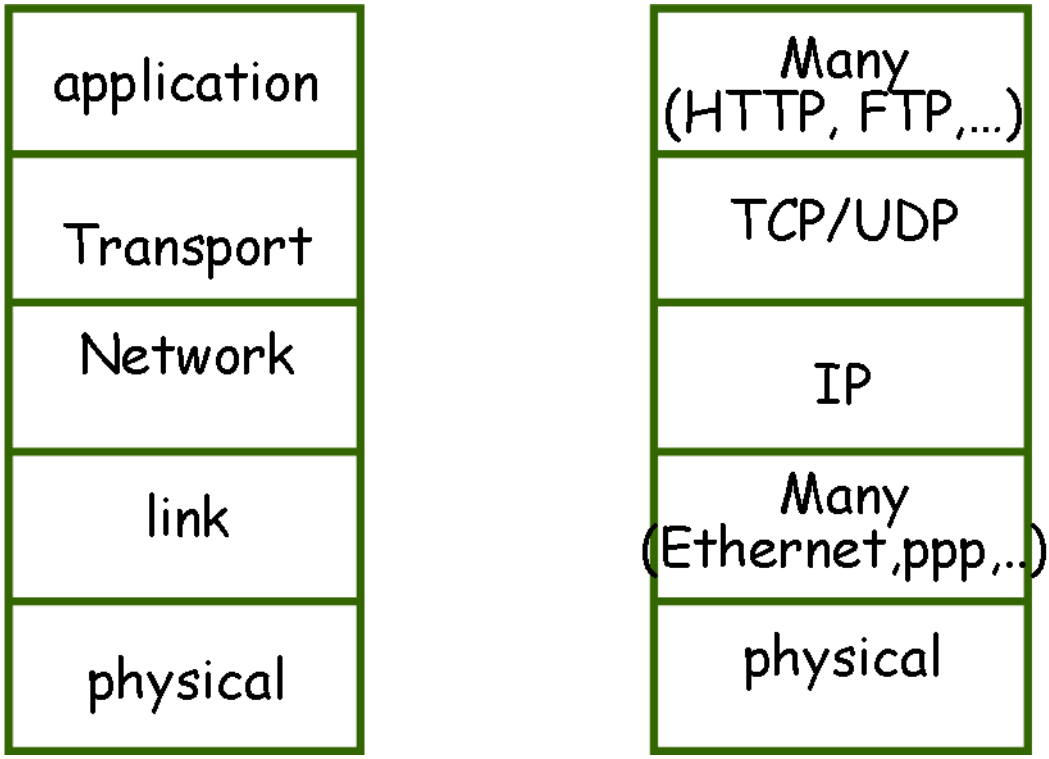


Figure 4: TCP/IP protocol suite

Network Protocols

Communication in the Internet is performed according to TCP/IP protocol suite presented below.

1 Internet Protocol (IP)

The Internet Protocol at the network layer, is the one providing connectionless packet delivery service from a sender machine to a destination machine through routing.
IP defines three important items, mainly:

- Internet addressing scheme
- Packet format
- Packet forwarding

1.1 Internet addressing scheme

Every network interface is assigned an IP address that is 32 bit long (in IPv4). Each address is divided into two parts: network identification part (netid) and host identification part (hostid). All machines connected to the same network have the same netid part, but differ in the hostid part.

The partitioning into two parts were done first according to the network classes that define how many bits are allocated for the netid part and how many are allocated for the hostid part. The 3 classes are as follows:

- `Class A:` starts with 0, and has 8 bits allocated for the netid and 24 bits for the hostid
- `Class B:` starts with 10, and has 16 bits allocated for the netid and 16 bits for the hostid
- `Class C:` starts with 110, and has 24 bits allocated for the netid and 8 bits for the hostid

Later, this classful addressing turned out to be inflexible, and the CIDR (Classless Inter Domain Routing) approach proved to be successful, where the concept of classes have been got rid of. Instead, netid part can be of any arbitrary length. Accordingly, an IP address has to be specified by the address and a network mask.

1.2 IP Packet Format

Each IP packet, called datagram, is encapsulated with an IP header. The IP header has a minimum 20 bytes long and is composed of the fields shown below.

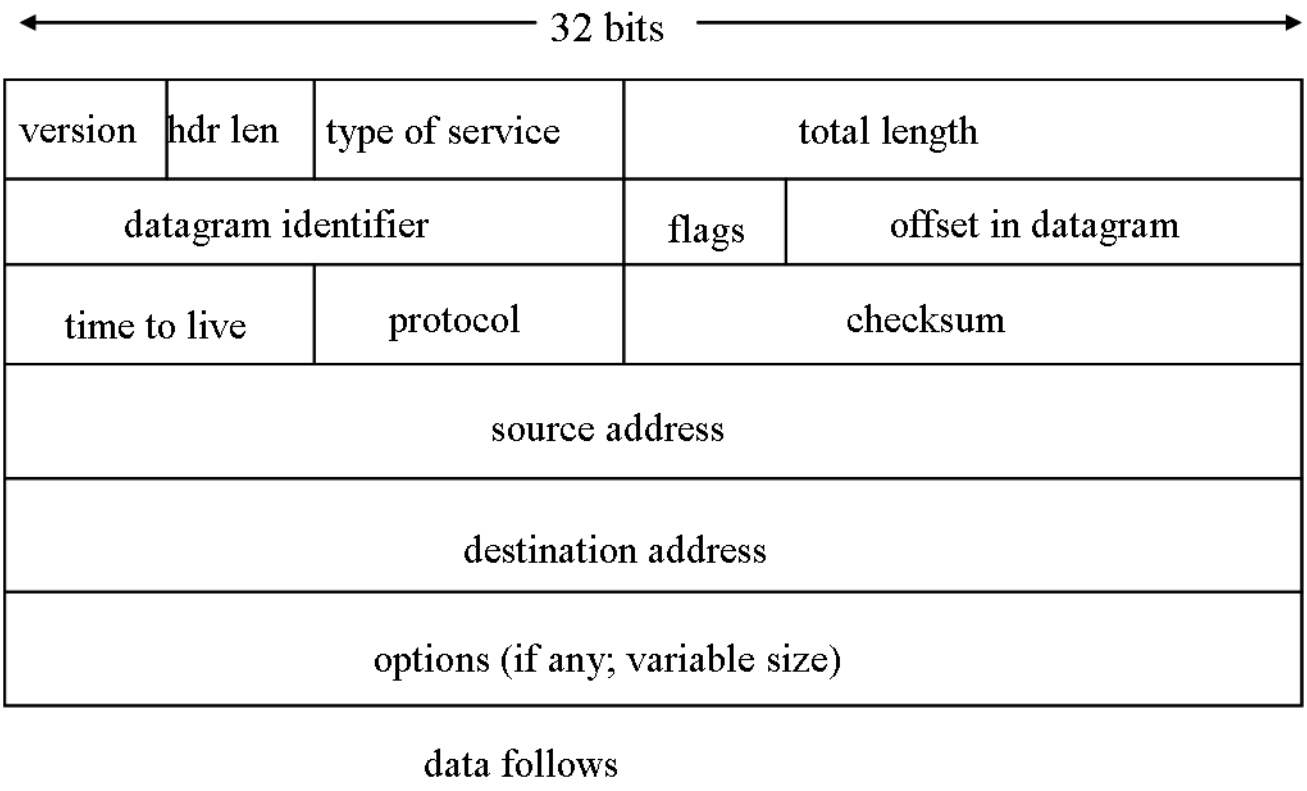


Figure 5: IP header

The IP version is stored in the first field, while the second field specifies the length of the header in multiple of 4 bytes (word length). The Type of Service field describes the priority of the datagram, and usually ignored by the routers but efforts are undergoing to allow priorities and differential services to datagrams based on this field. The total length of the datagram (including the header) is defined in the total length field in bytes. Information needed for fragmentation and reassembling is included in the identifier, flags, and offset fields. The time to live (TTL) field defines the maximum number of hubs a datagram can travel before being discarded. The protocol field defines the upperprotocol and checksum field is for the header part only. The source and destination IP-addresses follow for routing purposes.

2 ARP/RARP and ICMP

Other protocols, called sometimes companion protocols, co-exist with IP for exchanging control information. Examples are ARP, RARP and ICMP.

2.1 ARP/RARP

Sending packets between machines is done using hardware addresses (MAC addresses) while communication between applications is done using IP addresses. Thus, a mapping between IP address and hardware address is needed which is called "address resolution". The Address Resolution Protocol (ARP) is responsible for mapping IP address to MAC address (Ethernet address in our lab).

Consider the following example: machine A wants to send a packet to machine B. Machine A consults its internal address resolution table to check whether B's MAC address is stored in the table or not. If not, a MAC broadcast message, ARP-REQUEST, is sent containing the IP address of B. When B receives the message, a unicast message is sent to A, ARP-REPLY, containing its MAC address. At the same time, the MAC-IP address pair of A is stored in B's table (if it didn;t exist before).When A receives the reply, the MAC-IP address pair of B is stored in A's table.

On the other hand, RARP is the reverse of the ARP mechanism. It allows a host to learn its own IP address after it boots (intended for bootstrap). A computer sends its Ethernet address to a RARP server (maintained by an administrator) asking for its IP address. The server responds by sending computer's IP address. This protocol is replaced now by DHCP

2.2 ICMP

ICMP protocol is intended to report errors to routers. Example of such errors are: destination unreachable, time exceeded. Another use of ICMP is to gather statistics on a certain end-to-end path. Two types of ICMP messages exist: Query and Error reporting. An important example of a query message is the echo request and reply mesages (used by ping) for testing the reachabilty of an IP-address on the network.

3 Transport Protocol

In TCP/IP protocol suite, two different transport protocols exist: UDP (User Datagram Protocol) and TCP (Transport Control Protocol). UDP is a fast and unreliable transport protocol that is suitable for some applications like multimedia applications. On the other hand, TCP is a connection-oriented protocol that ensures reliable and in-order delivery of packets. Also it provides both flow control and congestion control. Both TCP and UDP are end-to-end protocols. A message formed by the application layer is sent either to TCP or UDP where it is encapsulated with the corresponding header, then sent to the network layer. The TCP and UDP headers are shown below.

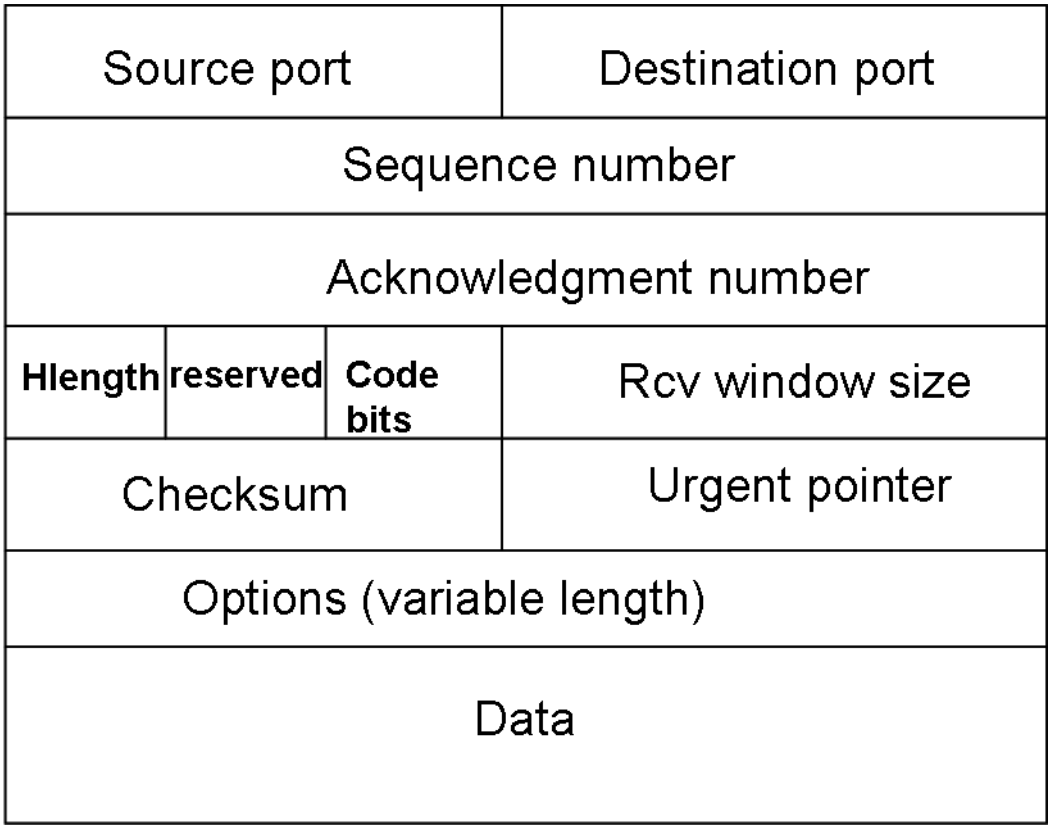


Figure 6: TCP header

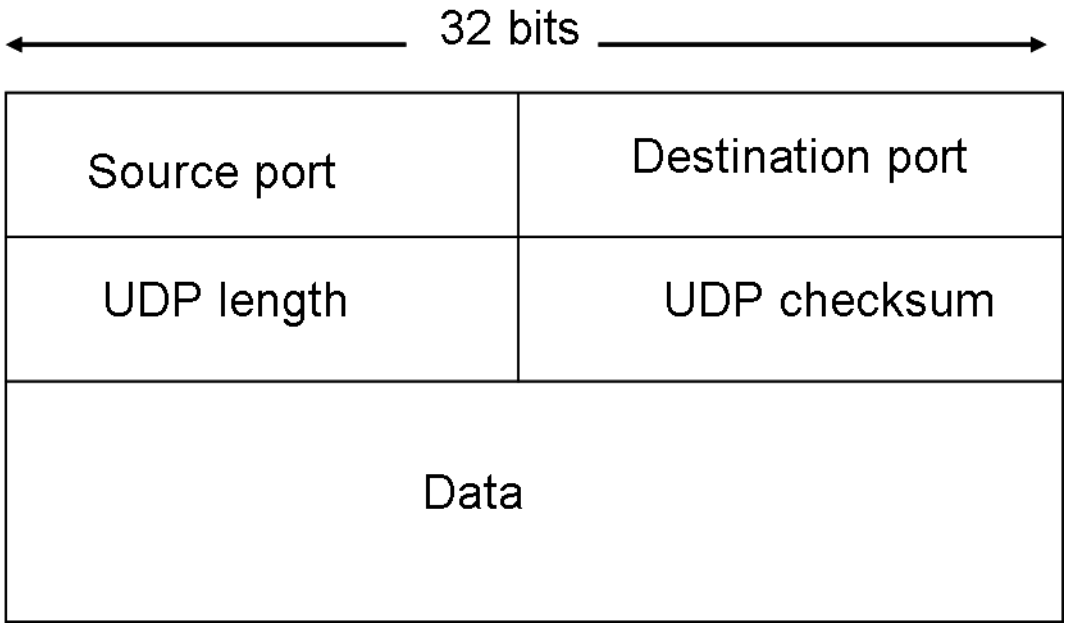


Figure 7: UDP header

4 Application Protocols

The application layer in the Internet is the layer that provides application services to the users. A number of these services will be presented and experiences in this lab among which:

- DNS
- FTP
- SMTP
- HTTP

4.1 Domain Name System

People usually tend to remember names easier than remebering IP addresses. That's why we need a mechanism to translate between machine name and its IP address. DNS defines the structure of Internet names and their association with IP addresses, as well as the association of mail and name servers with domains. The Domain Name System is composed of a hierarchical database system that forms a tree topology of name servers. The root name server is responsible for the whole domain name space. There exists 13 of such root servers. The IP addresses of the root name servers are known to all name servers.
Beside mapping names to IP addresses (called A records), the DNS is able to do more. The DNS different records are as follows:

- SOA: Start of Authority record - The "SOA" record is the most crucial record in a DNS entry. It conveys more information than all the other records combined. This record is called the start of authority because it denotes the DNS entry as the official source of information for its domain.

- MX: Mail eXchange records - They allow all mail for a domain to be routed to one host.

- PTR: In-addr.arpa PTR records are the exact inverse of A records. They allow your machine to be recognized by its IP address. Resolving a machine in this fashion is called a "reverse lookup".

- NS: Name server records - They state the authoritative name servers for the given domain.

4.2 File Transfer Protocol (FTP)

FTP is a protocol used to acces files between a user (client) and a remote server

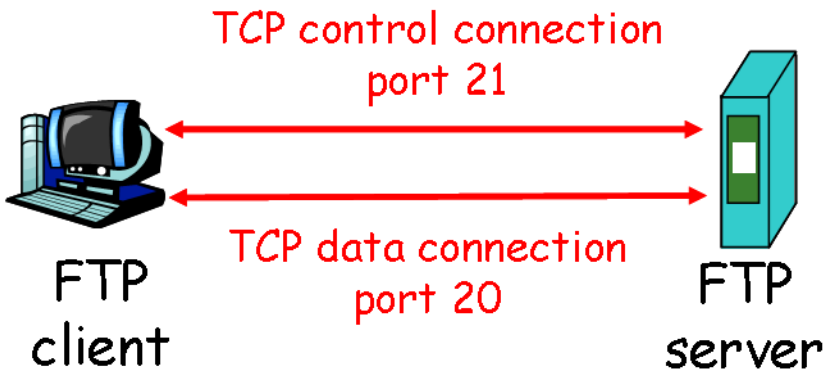


Figure 8: FTP

The protocol works as follows:

- FTP client contacts FTP server on port 21, establishing a TCP connection.

- Client provides user name and password which are sent to server.

- Server authorizes client.

- Client browses remote directory (commands sent on control connection).

- Server receiving a command for a file transfer, opens a TCP data connection to client, transfers the file, then closes the connection.

- Transferring another file needs another data connection.

4.3 Simple Mail Transport Protocol (SMTP)

SMTP is an application layer protocol for sending messages between mail servers. It uses TCP connection (between sender and receiver servers, no intermediate servers) The protocol has 2 sides: client and server. Both sides run on every mail server.

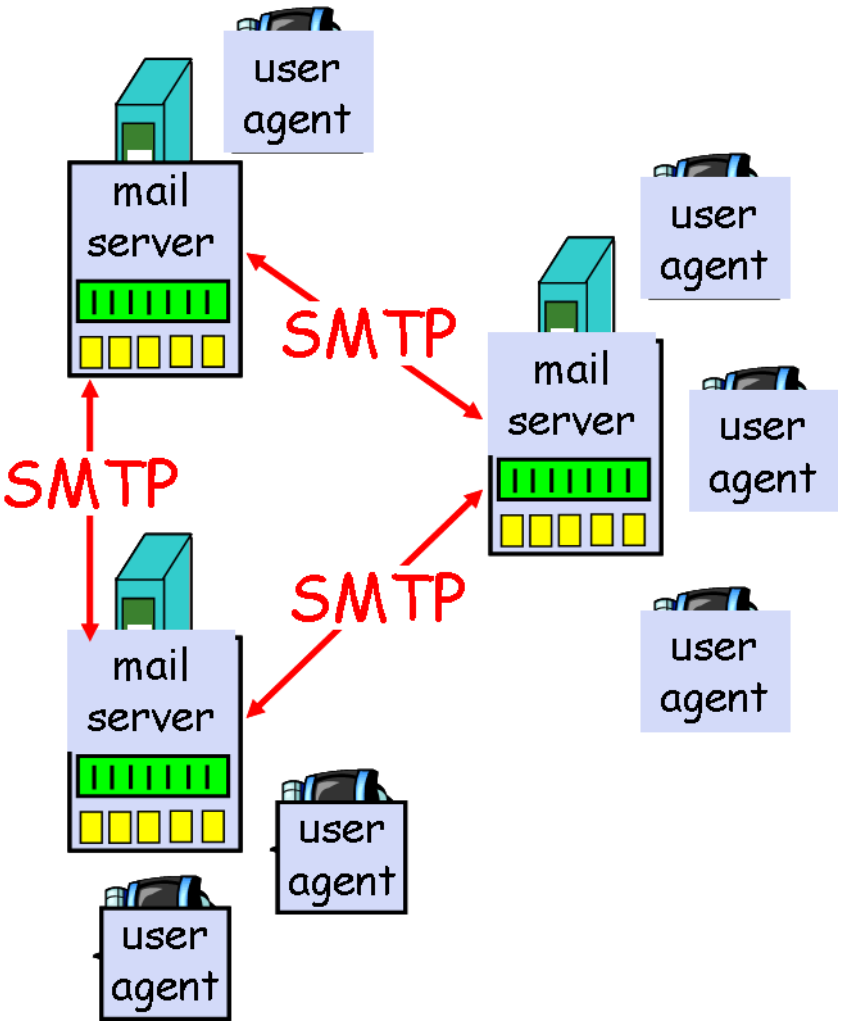


Figure 9: SMTP

The SMTP commands are in ASCII text. Example: HELO, MAIL FROM, RCPT TO, DATA The response is formed of status code and phrase. Example: 220 server name, 250 hello client name, Messages must be in 7-bit ASCII (MIME used for non-ASCII content)

4.4 HyperText Transfer Protocol (HTTP)

HTTP is a protocol that defines how web clients request web pages from the server and how web servers transfer web pages to clients. This protocol is based on the client/server model where the client is the browser that requests, receives, displays

Web objects (explorer, netscape,..), and the server is the Web server that sends objects in response to requests (Apache, microsoft IIS,..)

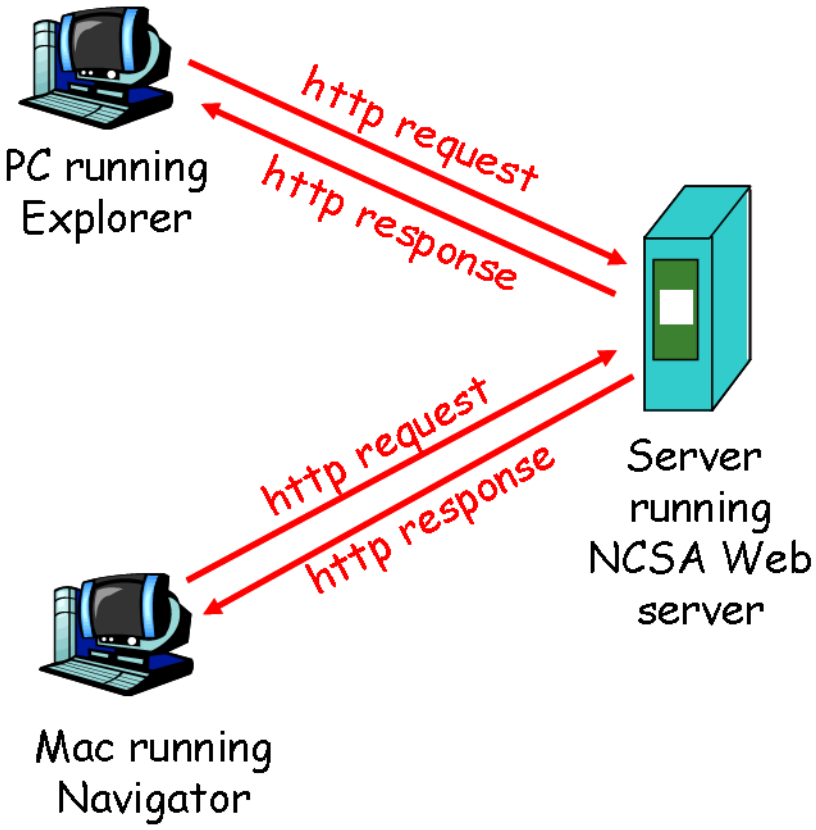


Figure 10: HTTP

The protocol works as follows:

- Client initiates TCP connection (creates socket) to server at port 80
- Server accepts TCP connection from client
- http messages exchanged between browser (http client) and Web server (http server)
- TCP connection closed

Experiment 1:
Streaming Technologies

References

- Andrew S. Tanenbaum: Computer Networks
- RFC0768: UDP – User Datagram Protocol
- RFC0791: IP – Internet Protocol
- RFC0793: TCP – Transmission Control Protocol
- Netem the network emulator

Preparatory Questions

1. What is meant by real-time applications?
2. Explain the difference between packet delay and packet jitter?
3. What are the causes of packet jitter?
4. How can packet jitter be recovered?
5. Why is packet that is received after its scheduled play-out time considered lost?
6. Identify and explain the five parameters of RTP header.
7. Why are sequence number and timestamp fields both used in the RTP header?

Experiment Setup

This experiment consists of three computers.Two of them are connected to a third computer that has a configuration of a router with **netem** installed. **Netem** is a software that provides network emulation functionality for testing protocols by emulating the properties (like packet delay and packet loss) of wide area networks.

- source
- serverexp1
- sink

On setup A1/7 the three computers are:

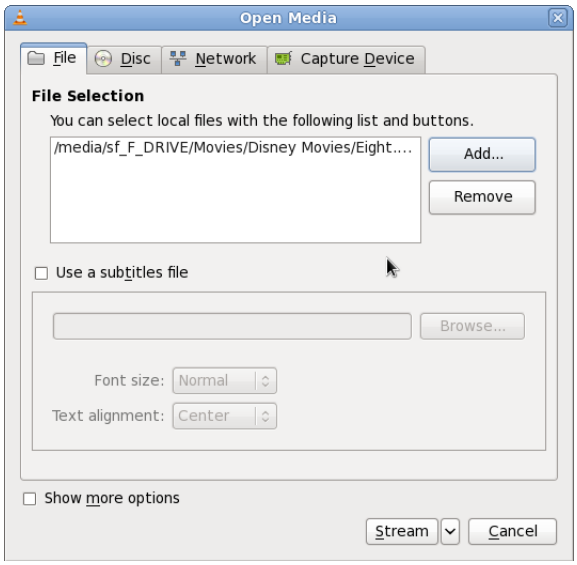
- source -ha
- serverexp17
- sink -cn

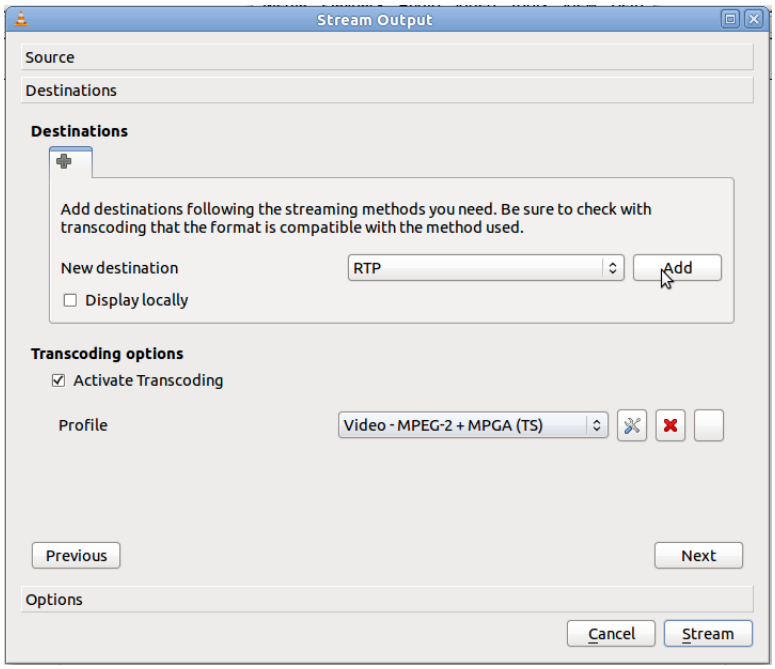
Experiment Procedure

Part 1: Video Streaming

Start streaming video from source node to sink node as follows: At the source node:

- Run vlc.
- Open the video file and stream it to the sink node.

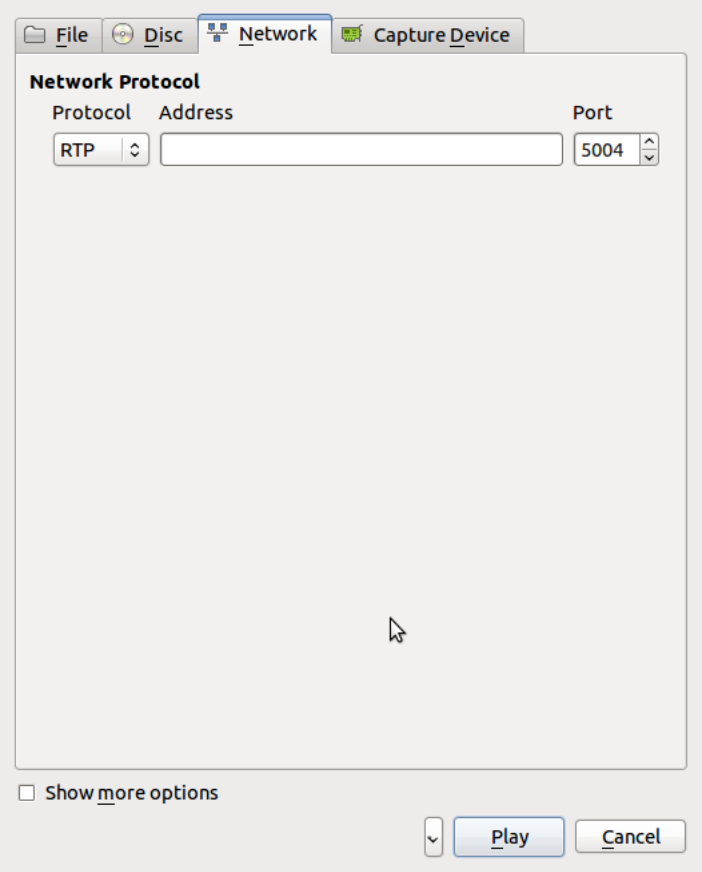




- Choose RTP and click add
- Click next and write the ip address of the sink node.

At the sink node:

- Run vlc
- Open Network Stream
- Choose RTP, click play



Observe the quality of the streamed video.

Part 2: Effect of jitter

At the source node:

- Ping the sink node.
- Apply jitter on the network between the source and the sink as follows:
- Using netem at the serverexp node, type the following command to re-order the packets
  `sudo tc qdisc add dev eth2 root netem delay 500ms reorder 25% 50%`

  1. What does this command do?
  2. Ping the sink node again after you added jitter, what changes were applied?

- Stream the video (follow the same steps of part 1).

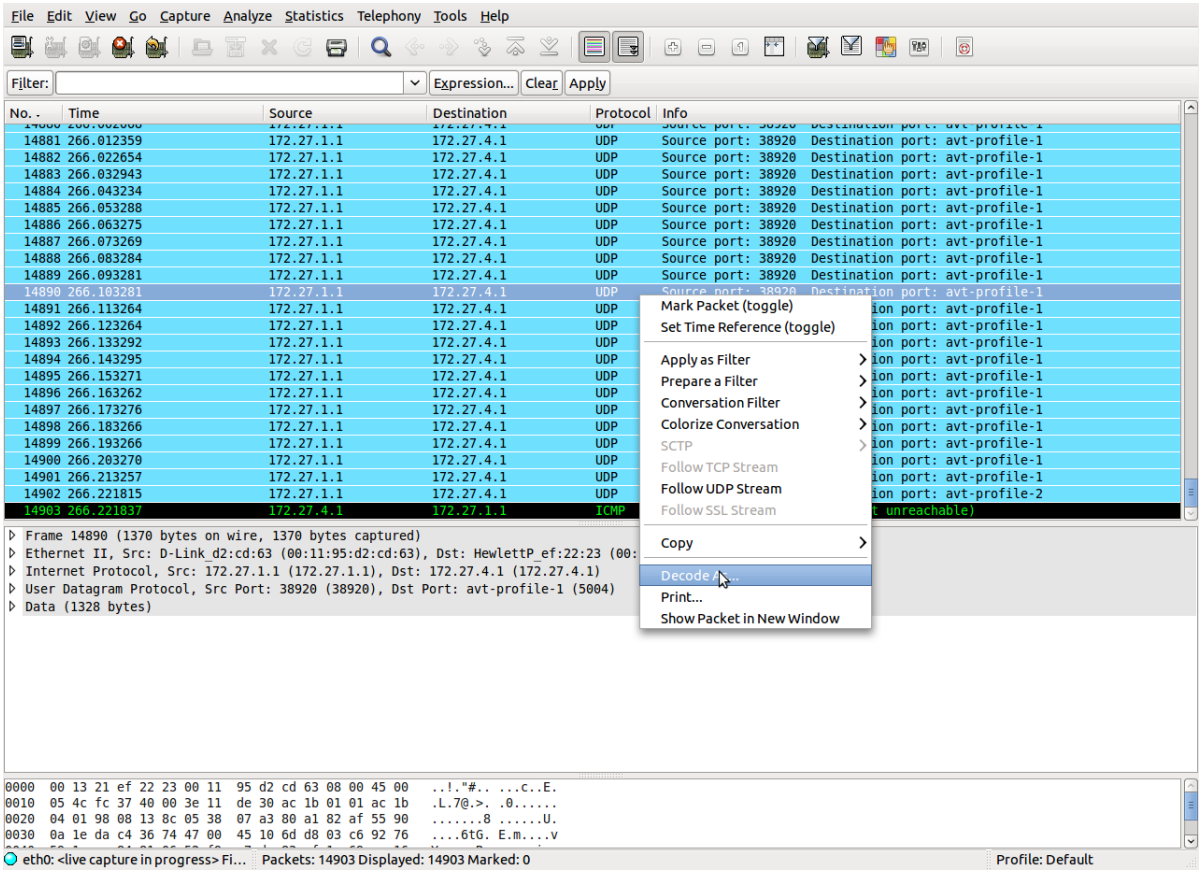
  1. What is the effect of jitter on the streamed video?
  2. What do you observe? Compare between this case and [1].Explain your observation.

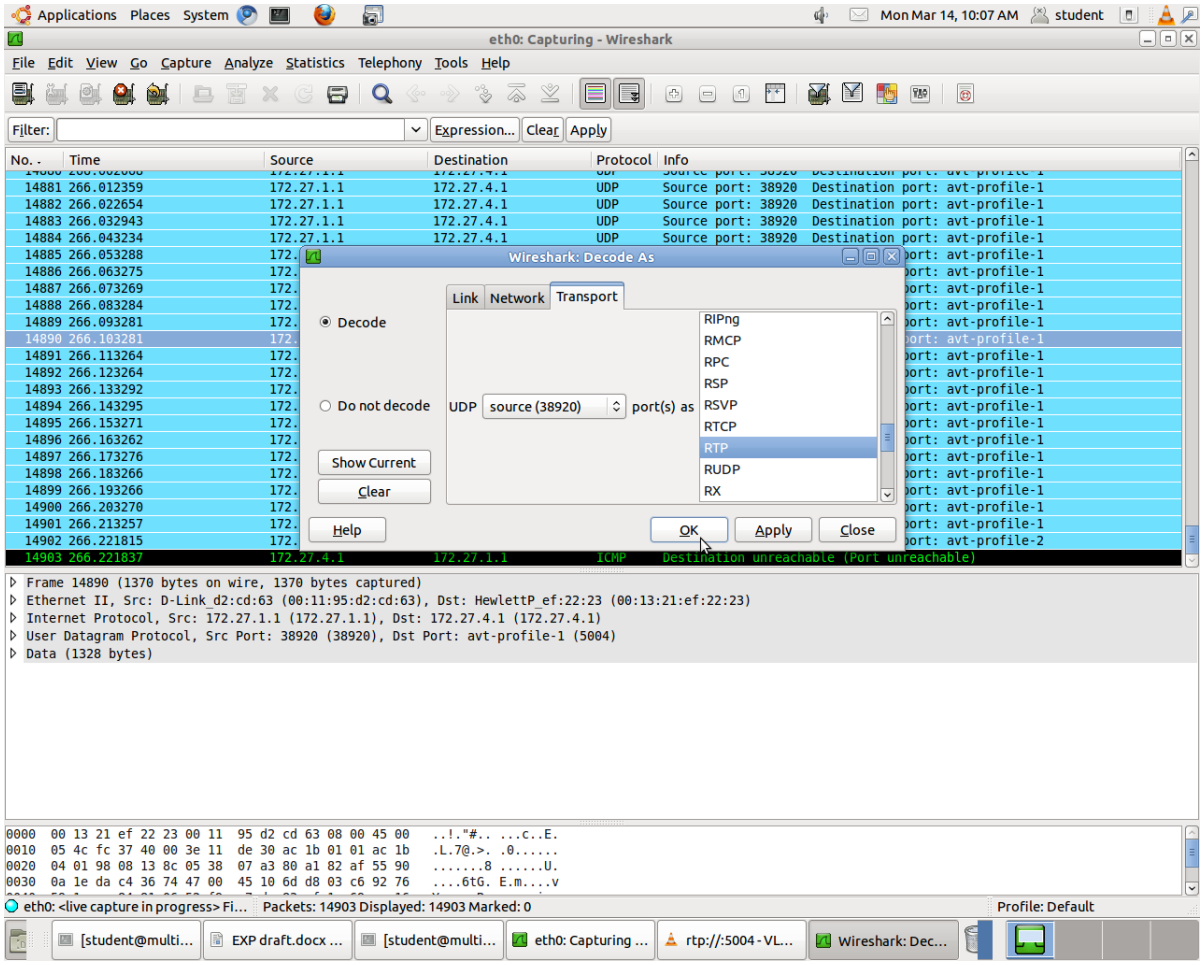
- Remove jitter
  `sudo tc qdisc del dev eth2root netem delay 500ms reorder 25% 50%`

Part 3 : RTP/UDP vs UDP

Streaming over RTP/UDP

- Run wireshark and start packet sniffing on the sink node.
- Start video streaming.
- Decode the udp packets as follows:


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. . Time Source Destination Protocol Info
14881 266.012359 172.27.1.1 172.27.4.1 UDP Source port: 38920 Destination port: avt-profile-1
14882 266.022654 172.27.1.1 172.27.4.1 UDP Source port: 38920 Destination port: avt-profile-1
14883 266.032943 172.27.1.1 172.27.4.1 UDP Source port: 38920 Destination port: avt-profile-1
14884 266.043234 172.27.1.1 172.27.4.1 UDP Source port: 38920 Destination port: avt-profile-1
14885 266.053288 172.27.1.1 172.27.4.1 UDP Source port: 38920 Destination port: avt-profile-1
14886 266.063275 172.27.1.1 172.27.4.1 UDP Source port: 38920 Destination port: avt-profile-1
14887 266.073269 172.27.1.1 172.27.4.1 UDP Source port: 38920 Destination port: avt-profile-1
14888 266.083284 172.27.1.1 172.27.4.1 UDP Source port: 38920 Destination port: avt-profile-1
14889 266.093281 172.27.1.1 172.27.4.1 UDP Source port: 38920 Destination port: avt-profile-1
14890 266.103281 172.27.1.1 172.27.4.1 UDP
14891 266.113264 172.27.1.1 172.27.4.1 UDP
14892 266.123264 172.27.1.1 172.27.4.1 UDP
14893 266.133292 172.27.1.1 172.27.4.1 UDP
14894 266.143295 172.27.1.1 172.27.4.1 UDP
14895 266.153271 172.27.1.1 172.27.4.1 UDP
14896 266.163262 172.27.1.1 172.27.4.1 UDP
14897 266.173276 172.27.1.1 172.27.4.1 UDP
14898 266.183266 172.27.1.1 172.27.4.1 UDP
14899 266.193266 172.27.1.1 172.27.4.1 UDP
14900 266.203270 172.27.1.1 172.27.4.1 UDP
14901 266.213257 172.27.1.1 172.27.4.1 UDP
14902 266.221815 172.27.1.1 172.27.4.1 UDP
14903 266.221837 172.27.4.1 172.27.1.1 ICMP
Mark Packet (toggle)
Set Time Reference (toggle)
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window
Frame 14890 (1370 bytes on wire, 1370 bytes captured)
Ethernet II, Src: D-Link_d2:cd:63 (00:11:95:d2:cd:63), Dst: HewlettP_ef:22:23 (00:
Internet Protocol, Src: 172.27.1.1 (172.27.1.1), Dst: 172.27.4.1 (172.27.4.1)
User Datagram Protocol, Src Port: 38920 (38920), Dst Port: avt-profile-1 (5004)
Data (1328 bytes)
0000 00 13 21 ef 22 23 00 11 95 d2 cd 63 08 00 45 00 ..!."#.. ...c..E.
0010 05 4c fc 37 40 00 3e 11 de 30 ac 1b 01 01 ac 1b .L.7@.>. .0.....
0020 04 01 98 08 13 8c 05 38 07 a3 80 a1 82 af 55 90 ....8 ......U.
0030 0a 1e da c4 36 74 47 00 45 10 6d d8 03 c6 92 76 ....6tG. E.m....v
eth0: <live capture in progress> Fi... Packets: 14903 Displayed: 14903 Marked: 0
Profile: Default



1. How are the audio and video packets differentiated?
2. Include a snapshot from each packet.
3. How can you determine that the audio and video packets belong to the same session ?

Streaming over UDP

- Start packet sniffing.
- Start video Streaming, choose udp instead of rtp.
- What is your observation.

Part 4: Effect of network parameters

In this part you are required to change some network parameters using netem and explain the effect of these changes on the quality of the streamed video.

A. Effect of packet loss

- Change the **packet loss** parameter on the router machine using netem,you can refer to following link:

  `http://www.linuxfoundation.org/collaborate/workgroups/networking/netem`

- Write down the command that you used to add packet loss in the network
- Delete the packet loss you added.

B. Effect of packet corruption

Repeat the above steps for **packet corruption**

C. Effect of packet duplication

Repeat the above steps for **packet duplication**

Explain the effect of changing the three parameters on the quality of the streamed video.

Experiment 2:
Application and Link Layer Protocols

References

- Andrew S. Tanenbaum: Computer Networks
- RFC0768: UDP – User Datagram Protocol
- RFC0783 / RFC1350: TFTP – Trivial File Transfer Protocol
- RFC0791: IP – Internet Protocol
- RFC0951: BOOTP – Bootstrap Protocol
- RFC1034 / RFC1035: DNS – Domain Name System
- RFC2131: DHCP – Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- Preboot Execution Environment (PXE) Specification, Version 2.1
  `ftp://download.intel.com/labs/manage/wfm/download/pxespec.pdf`
  `http://www.pix.net/software/pxeboot/archive/pxespec.pdf`

Preparatory Questions

1. What is the hierarchy of DNS?
2. Are the IP adresses distributed in a hierarchical way?
3. What are the most important DNS record types?
4. What does authoritative and nonauthoritative reply mean?
5. What does 'Leasing' mean?
6. How does BOOTP function?
7. What problem did the original BOOTP version have?
8. Explain the meaning of the following packets:
   DHCP-DISCOVER, DHCP-OFFER, DHCP-REQUEST, DHCP-ACK, DHCP-NACK, DHCP-DECLINE and DHCP-RELEASE
9. What is the purpose of DHCP relay agent?
10. What is TFTP and how does it function?
11. What is PXE (Preboot Execution Environment)?
12. How does the process of boot run when using PXE ?

13. Do all Internet Applications today need secure connections? State your opnion and why might applications need/need not to have secure connections.

14. What is the SSL protocol and how is it used with HTTP?

15. Explain briefly the concept of load-balancing and how it can be used with different protocools and/or networking applications.

Experiment Setup

This experiment consists of two computers connected to a hub. The hub acts as a replicator where it gets the packets from one port and sends to all other ports without any consideration of where the destination host is.

Experiment Procedure

PC (Diskless Client) boot via DHCP/TFTP

1. Stop the capture process in wireshark and restart the process as follows

   - from the wireshark menu click Capture → Options
   - make sure that interface `eth0` is selected and the checkbox of Capture packets in promiscous mode is set
   - click on the start button to start capturing packets

2. Set the packets filter to `bootp or tftp`

3. Boot netboot from the network by starting it and pressing F12

4. When the Splash screen appears, select Advanced Options → rescue mode

5. When the blue screen loads, press left-alt + left-ctrl + delete to send the reboot signal [1]

6. Answer the following questions:

   - What is the meaning of the packets sent?
   - What Information is transmitted?
   - What problem arises for TFTP when using UDP as a transport layer protocol? How is this problem solved?
   - Which files are transmitted via TFTP? What are these files required for?
   - Why is a DHCP query started again after the transmitting of the boot file?
   - What is the role of the detected protocols in the network booting process?

[1] Note that this is step is not related to the experiment itself

Latency measurement

httping is a tool for measuring network latency when establishing http connections. Along with ping you are going to make different measurements and comment on the values based on your theoratical background.

1. start capturing on wireshark
2. In the terminal type ping met.guc.edu.eg -c 5
3. Take a record of the average time.
4. Now type httping met.guc.edu.eg -c 5
5. Take a record of the average time.
6. Answer the following:
   - To what do you account the difference in values of the latency?
7. Using the httping manual, find and test the following:
   - getting the http status codes
   - measuring ssl connections
8. Test the ssl connection with `mail.guc.edu.eg`[2]

Sniffing an FTP session

1. Start a new live capture in wireshark
2. Connect to netwserver as follows:

   ftp netwserver
3. Login in as student with the password student
4. navigate throughout the directories using the command `cd folder_name`

   to navigate to the parent directory use `cd ..`
5. Download a file from the server using `get filename`
6. Filter the ftp connection/s in wireshark.

   Use the expression button for that purpose in wireshark
7. Using the follow tcp stream function get data transmitted throughout the ftp session
8. Answer the following questions and attach snapshots

[2]If you get an error concerning shutting the down then you won't have the real time needed to establish a secure connection. However, you can test the results again at home with mail.yahoo.com for verification and if you happen to be interested.

- How many connections are there for the ftp session? Are they of the same type?
- How did you filter the ftp connection/s?
- Can you see the password that you entered for remote account or is it encrypted?

Sniffing an SSH-session

1. Start a new live capture in wireshark
2. Connect to netwserver as follows:

   ssh netwserver
3. Login with the same user credentials given for the ftp section
4. Interact with the remote shell and navigate through the directories
5. Filter the ssh session packets in wireshark
6. Answer the following questions and attach a snapshot:
   - Can you get the user password for the session?
   - What are the phases for establishing an ssh connection?
   - Which phases are unecrypted?
   - Provide a brief comparison between ftp and ssh

Load Balancing

Most domains today use load balancing techniques to smooth out the requests between all available servers. You are going to test today DNS load balancing and HTTP load balancing. There are three methods by which HTTP load balancing can be checked:

Cookies verification Checking the cookies settings and the information that is maintained by them

Servers replies timestamp If they don't appear in sequence then they are from different servers

Http header Observing the server line in the replies in one TCP connection and verifying that they are from different servers

where we are going to use the third method only. The domains to be tested are:

- yahoo.com
- google.com
- linkdsl.com

- guc.edu.eg

1. Open a terminal and type `dig ns <domain name>`
2. Check how many ns records dig retrieved for the domain? If more than one, then the domain applies dns load balancing

1. Open www.youtube.com and select any video of your choice
2. Using the Download helper plugin in firefox, click on the *Download* link and select *Copy url*
3. Save the copied url and get the IP address of the link using the dig command.
4. Is the IP fetched associated to an area or a country near you?

To do at home

The following excercises require the absence of a proxy between you and the Servers with which you are going to contact to fetch information. Therefore you will be doing them at home using any operating system and wireshark.

1. Repeat the excercise that you did with youtube during the lab session. If you don't have the Download helper plugin, install it on firefox. Note that you and your teammate must do this excercise indiviually
2. Investigate the url of the link, does it contain the name of your ISP?
3. If yes, then do realize that Google applied a Geographical load balancing algorithm to process your request.
4. In the post-lab report state all the links that you and your teammate fetched at home and during the lab session. And list the geographical location of the servers.

1. Open firefox and type a domain name in the address bar
2. Trace the http packets of the domain in wireshark and get the full tcp stream
3. In the reply section for an object from the server check the header for a field named `Server`
4. Is the value for all retrieved objects the same? If no, then the domain applies http load balancing
5. Answer the following:
    - How can the reply be from different servers using one tcp connection?
6. Post a snapshot of the reply you got for a given tcp connection elaborating the different servers in the reply section.

Experiment 3:
Network Simulator Version 2 (NS-2)

References

- Website of NS http://www.isi.edu/nsnam/ns/index.html

Preparatory Questions

1. What is the functionality of Simulations?
2. What is NS Version 2 and what is it based on?
3. What do the keywords `proc`, `set`, `puts` in OTcl mean? What are `$`- and `#`- signs used for?
4. What is the duty of a `Network Animator` (NAM)?
5. What is the expression:
   ```
   set nf [open out.nam w]
   $ns namtrace-all $nf
   ```
   used for?
6. What is the content of `.nam` data and what can you use it for?
7. What is a `node`? What does `link` serve?
8. What is the meaning of `queue-type` and `queue-size`?
9. Explain according to OTcl the network that consists of 2 nodes and has the following characteristics:
   (a) Duplex channel with Bandwidth of 1,5 mbps, 12 ms Delay
   (b) Queue Type: RED
   (c) Queue Size: 10
10. How does a TCP (UDP) Connection in OTcl look like?
11. How do you order the NAM of the data streams according to their corresponding colors? Which statement settles the orientation of the nodes of a NAM?
12. How does a finish method that starts a Network Animator (NAM) look like?
13. What is the meaning of packet loss? Can packet loss be avoided ?

Experiment Setup

The experiment will run on one of ns2 hosts. These ns2 hosts have Network Simulator version 2 (ns2) installed. ns2 hosts are: ns2-1, ns2-2, videons2-1, videons2-2

Experiment Procedure

- `First Simulation using ns2 and NAM`

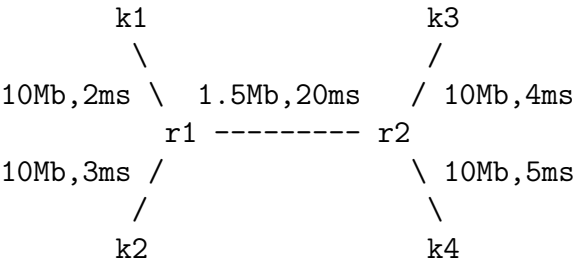
  1. In your home folder there is a folder called `DMET602-MET`, make a copy of it with your name
  2. Open a terminal (console) and navigate to your folder.
  3. Type "`gedit example1a.tcl &`" to open example1a in kate text editor.
  4. Run the simulation by typing "`ns example1a.tcl`".

  Are you able to see any output? if yes why? if no why not?
  Now open "example1b.tcl" and describe the single steps that ns2 carries out as well as the the result of NAM. What caught your attention during the animation?

- `Slight Changes in a Simulation`
  Examine the file `example2.tcl`

  1. What is DropTail and SFQ?
  2. Change SFQ to DropTail and repeat step?
  3. What do you see after 1.1 secs of simulation start? Explain why this is hapenning.
  4. How can you change this script in order that all packets reach node 3?

- `Construct your own Simulation`
  Construct your own Simulation.
  You have the following network structure consisting of 4 nodes and 2 Routers:



  The Given data represents bandwidth and delay. Work on the following exercises:

  1. Write the Tcl script to draw the network according to the above description. Add a TCP connection from the no des k1 and k2 to the node k3. Also add a FTP data channel(Start time 0.5 or 0.8).
  2. What type of queue can be used in this experiment?
  3. Add a buffer of 25 between the connections r1 and r2. Repeat step 2. What can you realize? What are the commands needed to limit the buffer size? You will be provided with a simulation file for the rest of this experiment.

4. What variables are traced and how can you trace such variables?
5. What is xgraph and how can you use it to visulaize the queue size and average queue size?
6. State at least 2 differences between the finish procedure in the file you are provided with and in the previous experiments.

Experiment 4:
Videoconference System: Setup and Protocol Analysis

References

- Andrew S. Tanenbaum: Computer Networks
- RFC0768: UDP – User Datagram Protocol
- RFC3261: SIP: Session Initiation Protocol
- Asterisk – Open-source PBX software documentation
- AN overview over SIP `http://www.voip-info.org/wiki/view/SIP`

Preparatory Questions

1. Why do video conferences and IP telephony have high network requirements?
2. What does SIP stand for? What are the applications of the SIP protocol?
3. Is SIP transmitted over TCP or UDP or Both? And why is that?
4. How is the SIP connection initiated?
5. List some SIP status codes and briefly state what they indicate. Name an application layer protocol that employs status codes too.
6. How is SDP employed by VOIP protocols?
7. Explain briefly the concept of open-source and patents
8. What is Theora?
9. What is Speex?
10. What is the role of the Gateways and Registrars with SIP connections?
11. How do VOIP connections differ with and without Registrars?

Experiment Setup

The experiment consists of two computers, each of them connected to a camera. Running on the server is asterisk, a PBX software. On setup 4 these two computers are:

- videoconf1
- videoconf2

On setup 4/8 these two computers are:

- videons2-1
- videons2-2

Experiment Procedure

Peer to Peer Video Conferencing

1. Open the video conferencing software `ekiga` and make sure that the two computers are not registered at the gatekeeper.

2. Open wireshark and start sniffing.

   - You can start wireshark by typing `sudo wireshark & disown`
   - Start capturing packets
   - Set the filter to `sip or rtp`

3. Establish a connection between the two computers using ekiga.

   - On one of the two computers type the ip address of the other and click the call button.

4. Answer the following questions based on the sniffed packets and attach Snapshots:

   - How was the session initiated? What was the protocol used?
   - Did you find SDP packets? If so clarify over which protocol.
   - Did you need to contact a server or was the whole session peer-to-peer?
   - What was the trasnport layer protocol of the SIP packets?
   - Over which protocol where the video and audio packets transmitted?
   - What were the codecs used for the video and audio streams?
   - How can you determine if the packets are for the same session?
   - What is the role of the sequence number in the packets sent?
   - According to the packets sniffed, state the sequence of packets exchanged to establish a SIP session.

Video Conferencing using a Gatekeeper

1. Restart sniffing on wireshark and leave the filter as is.

2. From the accounts menu, enable alice and bob on if you are on videoconf1 and videoconf2. If you are on videons2-1 and videons2-2 then enable laila and sameh.

3. Now make a call to one of the enabled accounts

4. Answer the following questions and attach snapshots:

   - How was the session initiated now?
   - Is there a new IP in the process? If yes, what is the role of the new host?

- According to the packets sniffed, state the sequence of packets exchanged to establish a SIP session.
- Based on your observations:

  What are the differences between the current call and the previous one?

  Now what are the similarities?

Experiment 5:
Videostreaming: Setup using Multicast/Unicast

References

- Andrew S. Tanenbaum: Computer Networks
- RFC0966: Host Groups: A Multicast Extension to the Internet Protocol
- RFC1075: DVMRP – Distance Vector Multicast Routing Protocol
- RFC1112: Host Extensions for IP Multicasting
- RFC2117 / RFC2362: PIM-SM – Protocol Independent Multicast - Sparse Mode
- RFC2236: Internet Group Management Protocol, Version 2
- RFC3376: Internet Group Management Protocol, Version 3
- Documentation about Streaming-Software VLC

Preparatory Questions

1. How do you define Unicast, Multicast and Broadcast?
2. What address range is for Multicast expected? Why are further IP-addresses needed, when every member has his own IP address?
3. What is the specific meaning of TTL (Time to Live) during a Multicast-Transmission?
4. To which MAC-Address will be a Multicast-Packet adressed? Explain how a Mac-Address is formed.
5. What is the function of IGMP?
6. DVMRP is based on Reverse-Path-Forwarding.Explain briefly how the router decides on the path tree. What are the disadvantages of this technique?
7. Explain briefly the differences between PIM Sparse Mode and PIM Dense Mode.
8. What problems result from Reliable Multicast?
9. Why do not ISP's (Internet Service Provider, e. g. T-Online) offer Multicast or even prevent its usage, although it stores the bandwidth?
10. What is IPTV and how does it make use of the multicast technology?

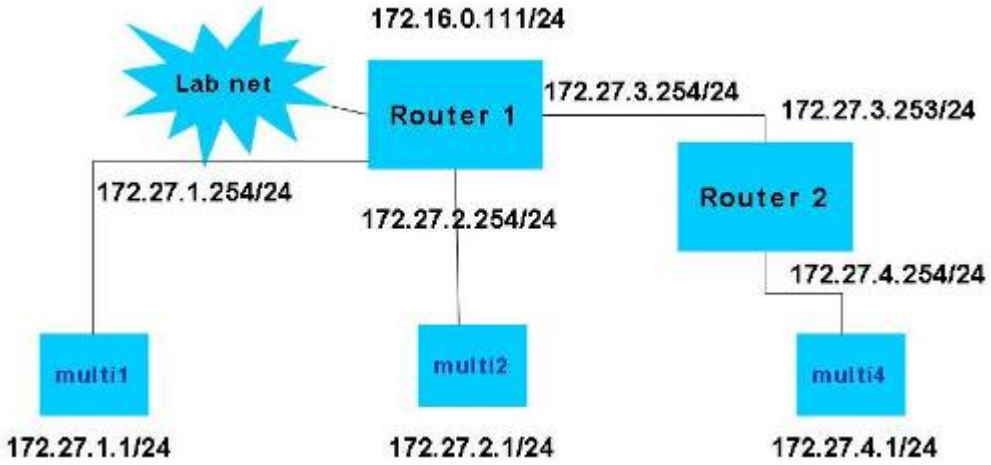


Figure 11: Multicast-Setup

Experiment Setup

Each node of the 4 nodes (multi1, multi2, multi4) is in a different subnet. Each host uses its own Router-Connection with the IP-addresses 172.21.X.254 as Gateway. Router1 is conected to the three hosts(multi1, multi2, multi3). Router2 is connected to one host (multi4). There is also a direct connection between the 2 routers (Router1 and Router2). Connection to the internet is established through the server 172.16.0.254. This server uses the address 172.16.0.105 of the Router as Gateway to all packets to be sent to the IP-address 172.21.X.Y.

In this experiment the DVMRP will be implemented.

Experiment Procedure

1. `Main Router Configuration`
   Type the following commands on multi2 or multiqos2 in order to allow multicasting:

```
minicom
system-view
multicast routing-enable
interface Ethernet 0/0
igmp enable
pim sm
interface Ethernet 0/1
igmp enable
pim sm
interface Ethernet 1/0
igmp enable
pim sm
interface Ethernet 1/1
```

```
igmp enable
pim sm
display pim routing-table
quit
pim
c-rp Ethernet 1/0 priority 50
c-bsr Ethernet 0/1 30 50
```

2. Start receiving the stream with the help of wireshark at one of the hosts.

   type `sudo wireshark & disown`

3. What was the type of the observed packets?

4. To whom where the packets sent?

5. `Second Router Configuration`

   At routerm2 type the following:

   `sudo /usr/lib/xorp/bin/xorp_rtrmgr`

6. `Video on Demand`

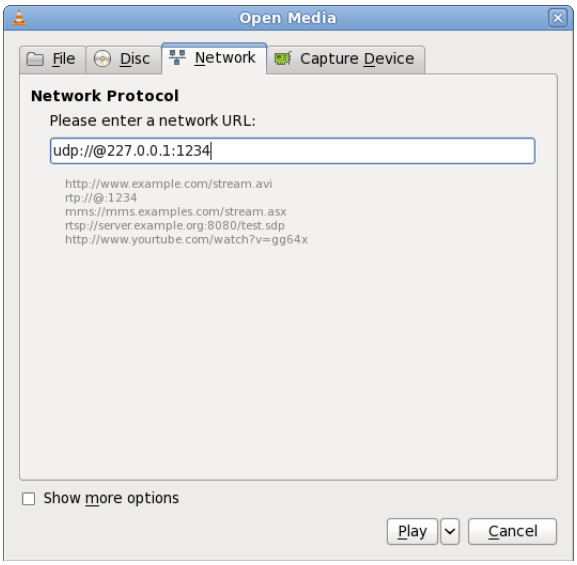
   - On multi2 or multiqos2 start streaming a video by typing the following command into the terminal
   - `vlc -vvv "input_file_between_quotations" --sout udp:227.0.0.1:1234 --ttl integer_value`
   - Check the home folder for a video and get it's absoulte path
   - Test with ttl values of 1, 2, 3 and 4

7. On all PCs of the setup start the streaming process as follows

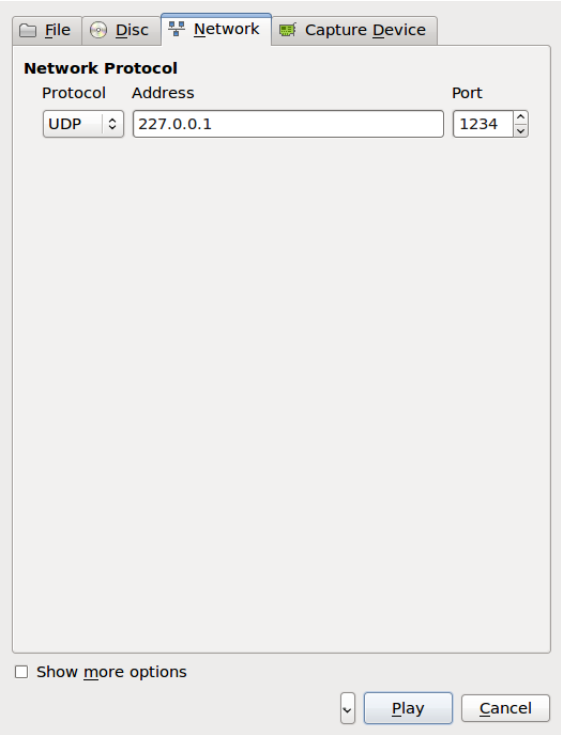
   - Open vlc by clicking ALT+F2 and typing vlc into the popped window
   - Another way of opening vlc would be by typing the following into a terminal

     `vlc & disown`

   - From the menu select Media → Open Network Stream
   - If a Window appears with an address bar only like the following type into it udp://@227.0.0.1:1234



- Otherwise, if a window appears with a protocol selection dropdown menu and two textboxes then select udp as a protocol. Place in the second box 227.0.0.1 and 1234 in the last textbox.



8. Using wireshark, check the time to live of the udp packets on all hosts.

   Attach a snapshot in your report for each ttl value

9. Answer the following question:

   - To what do you account the difference in the ttl values?

10. Stop one of the receiving hosts and restart wireshark on it.

11. Now configure the host again and check how a host joins a group.

12. How does this procedure affect the network of the sender?
13. Click after a while on PAUSE at the sender and observe how the receiver acts to the process.
14. Now click pause at one of the receivers. What happens now?
15. Click on STOP at one of the receivers.
    - How does the transmission end?
    - How does the receiver notify the sender to stop sending packets

Experiment 6:
Quality of Service (QoS), Traffic Engineering

References

- Andrew S. Tanenbaum: Computer Networks
- RFC0791: IP – Internet Protocol
- RFC1349: Type of Service in the Internet Protocol Suite
- RFC2212: Specification of Guaranteed Quality of Service
- RFC2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- Manual-Pages: tc, tc-cbq, tc-htb
- Linux Advanced Routing & Traffic Control HOWTO, Chapter 9
  `http://lartc.org/howto/`
- Documentation about Software Iperf to measure the network traffic
  `http://dast.nlanr.net/Projects/Iperf/`

Preparatory Questions

1. Explain the meaning of expression 'Quality of Service'?
2. According to which point of view can we distribute the different Services of Service classes(CoS – Classes of Service) to handle them differently?
3. What specific demands, that few applications add to the network, one tries with the help of QoS to fulfill?
4. Explain shortly the following basic processes: Admission Control, Traffic Shaping, Preferential Queuing, Selective Forwarding and Random early detection mechanism.
5. What is the meaning of classless Queueing Disciplines and classful Queuing Disciplines? Mention some examples and illustrate them.
6. Define the following two concepts DiffServ and IntServ.
7. Following is a QoS-configuration in which the tool `tc` is used. Try to figure out which traffic will have the highest priority and draw the corresponding tree structure.

```
tc qdisc add dev eth0 root handle 1: cbq bandwidth 10mbit avpkt 1000 cell 8

tc class add dev eth0 parent 1: classid 1:1 cbq bandwidth 10mbit                              \
   rate 8mbit weight 0.8mbit prio 8 allot 1514 cell 8 maxburst 20 avpkt 1000 bounded

tc class add dev eth0 parent 1:1 classid 1:3 cbq bandwidth 10mbit                             \
   rate 5mbit weight 0.5mbit prio 4 allot 1514 cell 8 maxburst 20 avpkt 1000
tc class add dev eth0 parent 1:1 classid 1:4 cbq bandwidth 10mbit                             \
   rate 3mbit weight 0.3mbit prio 2 allot 1514 cell 8 maxburst 20 avpkt 1000
tc class add dev eth0 parent 1:1 classid 1:5 cbq bandwidth 10mbit                             \
   rate 1kbit weight 0.1kbit prio 8 allot 1514 cell 8 maxburst 20 avpkt 1000

tc qdisc add dev eth0 parent 1:3 handle 30: sfq perturb 10
tc qdisc add dev eth0 parent 1:4 handle 40: sfq perturb 10
tc qdisc add dev eth0 parent 1:5 handle 50: sfq perturb 10

tc filter add dev eth0 parent 1:0 protocol ip prio 2 u32 match ip dport 1234 0xffff flowid 1:3
tc filter add dev eth0 parent 1:0 protocol ip prio 1 u32 match ip tos 0x08 0xff flowid 1:4
tc filter add dev eth0 parent 1:0 protocol ip prio 3 u32 match ip src 0.0.0.0/0 flowid 1:5
```

Experiment Setup

In setup C6

This experiment consists of a Linux-Router `routerq1` to which 3 subnets beside the uplink are connected to. In one subnet a host `qos1` that is used as Videostreaming and FTP-Server is found. The other 2 subnets with the hosts `qos2` and `qos3` is connected to the router `routerq1`. This router serves as a bottleneck to show QoS in a congested situation.

In setup B5/6

The Router `routermq2` to which 2 subnets beside the uplink are connected to. In one subnet a host `multiqos1`, that is used as Videostreaming and FTP-Server is found. The other subnets with the hosts `multiqos2` and `multiqos3` is connected to the router `routermq2`. This hub serves as a bottleneck to show QoS in a congested situation.

Experiment Procedure

Observing the TOS-Field / DS-Field

In this section, you are going to observe the QoS requested for different protocols and connections.

1. Start wireshark on multiqos2 by typing `sudo wireshark & disown`
2. Set the filter to `http`
3. Start firefox and open the met website
4. Now check for the Differentiated Services Field (DS-Field) as follows:
   - Right-click any http packet
   - Select show packet in a new window
   - Expand the Internet Protocol layer

- Take a snapshot for your report

5. Now change the filter in wireshark to `ftp and ip.dsfield > 0`
6. Start an ftp session with multiqos1 as follows
   - `ftp multiqos1`
   - `Username : student`
   - password is student
7. List the files available at multiqos1 by typing `ls`.
8. Start downloading the file ubuntu.iso by typing the following command :

   `get ubuntu.iso`

9. Look again for the DS-Field and take a snapshot.
10. Again change the filter to `ftp-data and ip.dsfield > 0`
11. For any packet, take a record of the DS-Field
12. Now to observe the QoS requested for ssh packets, change the filter to `ssh and ip.dsfield > 0`
13. Connect to netwserver as follows:
    - `ssh netwserver`
    - when prompted for a password enter `student`
14. Record the DS-Field value for any ssh packet.
15. Discuss with your Supervisor the values and write down your conclusion

QoS with CBQ

The following four cases should be examined :

1. without QoS and without Congestion(using Videostreaming)
2. without QoS and with Congestion(using FTP of largefile, ping)
3. with QoS and with Congestion(run CBQ script)
4. with QoS and without Congestion(run script, stop the ping and Videostreaming, restarting ping)

Experiment Procedures

1. CASE 1: Without QoS and without Congestion(using Videostreaming) Observe the ideal case, where there is no network congestion and only a video streaming session is running

- Start the Videostreaming with vlc from multiqos1 to multiqos4.
- Stream a file using the commands given in experiment 5 but place the ip address of multiqos4 instead of the given multicast address.
- You can also stream using the GUI interface, search online if you are interested.

2. CASE 2: Without QoS and with Congestion(using FTP of largefile, ping)
   There will be two scenarios to check While the video steam is still running increase the congestion of the network:

   - @multiqos4 Download the file "ubuntu" again from multiqos1 through gftp instead of ftp
   - @multiqos1 start flood ping by typing the following command(Make more than one)

     `sudo ping -f <ip_address_multiqos4> -s 65000`

   - Make more than one flood ping to increase the network congestion

   The second scenario to check is by decreasing the bandwidth between the two routers as follows:

   - @multiqos2 type the following to decrease the bandwidth
     - `sudo minicom`
     - `<Router> system`
     - `[Router] interface e1/1`
     - `[Router] qos gts any cir 10000000`

   Observe what happened in both cases, and write your conclusions

   - Increase the bandwidth again and go to case 3.

     `[Router] qos gts any cir 100000000`

3. CASE 3: With QoS and with Congestion(run CBQ script)

   - Start ftp download
   - @multiqos1 start flooding ping
     `sudo ping -f <ip_address_multiqos4> -s 65000`
   - Start video streaming
   - Run the CBQ SCRIPT on routermq2 and observe what happen to the flood ping, the TCP stream and the vlc video streaming. To run the script navigate to /home/student/tc scripts and type:

     `sudo ./tc_cbq start`

   - try starting and stopping the cbq script and observe the results. You can stop the script by typing

```
sudo ./tc_cbq stop
```

- If you would like to have a look at the dropped packets and flow control type:

```
sudo ./tc_cbq info
```

4. CASE 4: With QoS and without Congestion(run script, stop the ping and Videostreaming)

   - Stop the vlc videostreaming and the flood ping and observe what happens to the TCP stream (FTP). Verify according to the FTP transmission rate output if the QoS leads to performance loss and try to guess why did you have loss of packets when transmitting the tcp stream.
   - Try again with the TCP stream and flood ping
   - For each case check the dropped packets using `sudo ./tc_cbq info` and provide your conclusions.

Experiment 7:
Mobile IP

References

- Andrew S. Tanenbaum: Computer Networks
- RFC0791: IP – Internet Protocol
- RFC0792: ICMP – Internet Control Message Protocol
- RFC1853: IP in IP Tunneling
- RFC2002: IP Mobility Support
- RFC2003: IP Encapsulation within IP
- RFC2344 / RFC3024: Reverse Tunneling for Mobile IP
- Documentation about Dynamics Mobile IP
  `http://dynamics.sourceforge.net/`
- Netem the network emulator
  `http://www.linuxfoundation.org/collaborate/workgroups/networking/netem`

Preparatory Questions

1. What is the application environment of Mobile IP?
2. Define the following expressions: Mobile Node (MN), Home Agent (HA), Foreign Agent (FA) and Care-of Address (COA)
3. What is the role of Agent Discovery? What are the two possibilities?
4. What happens at the Registration?
5. What is Tunneling needed for and how does it function?
6. How does IP-within-IP Tunneling function and what is its job towards Mobile IP?
7. How do you define Reverse Tunneling and Triangle Tunneling of Mobile IP?

Experiment Setup

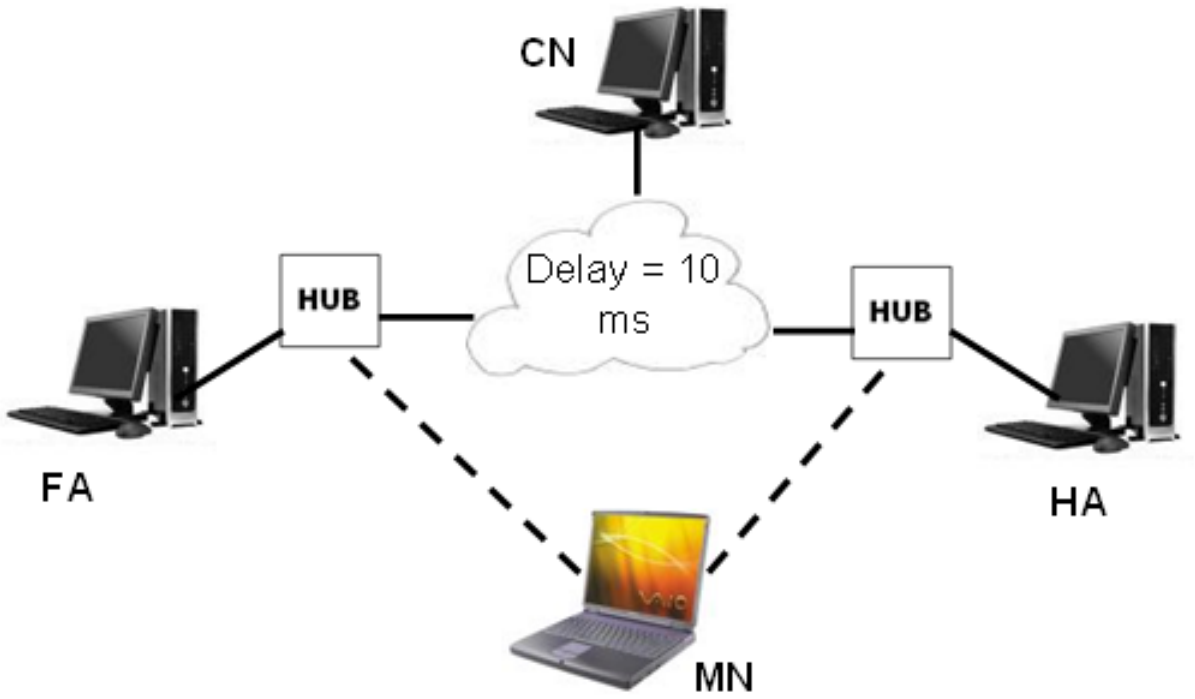


Figure 12: Mobile IP-Setup

Experiment Procedure

- Start sniffing on all hosts by typing `sudo wireshark & disown`
- Set the filter to `icmp or mip`
- Start the Mobile-IP-Software.

  a. Start the Dynamics Home Agent (`dynhad`) by typing the following commands at the home agent.
  ```
  sudo modprobe ipip
  sudo dynhad --fg --debug
  ```

  Start the Dynamics Foreign Agent (`dynfad`).

  ```
  sudo modprobe ipip
  sudo dynfad --fg --debug
  ```

  Start the Dynamics Mobile Node (`dynmnd`).
  ```
  sudo dynmnd --fg --debug
  ```

Note: fg is an option that means 'do not fork the daemon', in other words the process will not be the child of the terminal process. And debug means 'print debug information'.

b. Observe the Network-traffic of the three hosts.
NOTE: each of the mobile node, home agent and foreign agent are separately connected. How does each host try to draw attention (Agent Discovery)? To whom are the packets sent?

c. Look at the configuration of the network card and the routing table on your mobile node.

- MN in Home-Network

a. Connect the mobile node to a Home-Network. How does the MN know that it is currently in the Home-Network? How does the HA know that MN is currently in the Home-Network? Which packets are to be sent?

b. Look again at the configuration of the network card and the Routing-Table.

- MN in Foreign Network

a) Connect the mobile node to a Foreign-Network. How do MN, FA & HA communicate together to fulfill the registration process?
NOTE: Do not only look at the packets that are sent, but also consider the configuration of the network card at all three hosts as well as at the Routing-Table.

b) Measure the Handover-time of switching between the Home-Network and Foreign-Network. How can this time be increased/decreased?

- Network Emulation

a. Open a shell on serverexp7 or serverexp17

1. add the following delays

```
sudo tc qdisc add dev eth0 root netem delay 10ms
sudo tc qdisc add dev eth1 root netem delay 10ms
sudo tc qdisc add dev eth2 root netem delay 10ms
```

b. Measure the latency from Mobile Node to correspondent Node. Look at the following situations:
   - MN in Home-Network
   - MN in Foreign-Network.

c. In case you would like to remove the delay type the following

```
sudo tc qdisc del dev eth0 root netem delay 10ms
sudo tc qdisc del dev eth1 root netem delay 10ms
sudo tc qdisc del dev eth2 root netem delay 10ms
```

- IP within IP-Tunneling

  a. Attach MN to the Foreign-Network. Send a Ping to the Correspondent Node and sniff the traffic passing through the cloud. You can do that by observing the traffic on the home agent or the foreign agent. Which path do the packets follow from Mobile Node to Correspondent Node (including all routers)?
  Could you define the two nodes that tunnel the packets coming from and going to them?
  What type of tunneling is used?

  b. Configure the MN to use the other type of tunneling. Send a Ping to CN. Which packets are routed through the cloud?

     NOTE: To edit the tunneling mode, type at the **mobile node**:
     `gedit /etc/dynmnd.conf`

Experiment 8:
(NS-2) - Wireless Transmission

References

- Website of NS `http://www.isi.edu/nsnam/ns/index.html`

Preparatory Questions

1. What is an ad hoc network??
2. What is meant by random waypoint mobility model?
3. What does DSR stands for? and how it works?
4. Explain briefly the difference between DSR and DSDV routing for ad hoc networks
5. What is the "GOD" object? Explain briefly.

Experiment Overview

In this experiment you will examine and simulate several wireless transmission scenarios. To start navigate to the folder `/home/student/DMET602-MET` and copy the folder `exp8` to any place of your convenience. Rename the folder to your team name.

Simple Network Creation

1. Navigate to your folder and examine the file `simple-wireless.tcl`
2. Discuss with your supervisor what do you understand from the written code
3. State your conclusions.
4. Change the simulation area from `500*500 m` to `670*670 m`.
5. Change the pause time of `node_(1)` from 50 to 30 seconds.
6. Set the maximum speed of `node_(1)` to 12 mps
7. Generate an ftp over tcp connection between `node_(0)` and `node_(1)` using cbrgen.tcl
8. To see how you can use cbrgen.tcl search for `cbrgen.tcl` in `ns_doc.pdf`
9. Make sure that the following parameters are set as follows:
   - type to tcp
   - nodes to 2
   - connections to 1

- rate to 100k

10. Start running the script. Record and state your observations.

    refer to experiment 3 to recall how to use ns2 simulator

11. To visualize the output using nam proceed as follows :

    (a) add the following two lines before the topography section

    ```
    set namtrace    [open simple.nam w]
    $ns_ namtrace-all-wireless $namtrace 670 670
    ```

    (b) Open `example1a.tcl` from your local folder and copy the finish procedure. Paste it to the current file.

    (c) Adjust the code of the finish procedure to match the following:
    - ns object simulator
    - nam file handle
    - output file to be run by nam

    (d) Save the file and run it using ns

    (e) If you would like to increase the node size add the following for loop:

    ```
    for {set i 0} {$i < $val(nn)} {incr i} {
       $ns_ initial_node_pos $node_($i) 60
    }
    ```

12. Take several snapshots of the running simulation and explain what happens at each one.

13. Make sure that you provide answers for the following questions:

    (a) When did the nodes start sending packets to each other?

    (b) How do the nodes advertise themselves?

    (c) Was there any packet loss during the simulation?

    (d) What was the routing algorithm used for the simulation?

Packet Delivery Ratio

1. Open the file `simple-xgraph.tcl` and study the code
2. Discuss the new file with your supervisor
3. Extend the new file to have a cbr over udp connection

   `cbrgent.tcl` can be used for that purpose but you need to set the rate to 1

4. Modify the written/genertated code to have the receiver name as `null0` and of type `Agent/LossMonitor`
5. Run the file and record the results
6. Make sure that you provide the steps done to create the aforementioned connection.