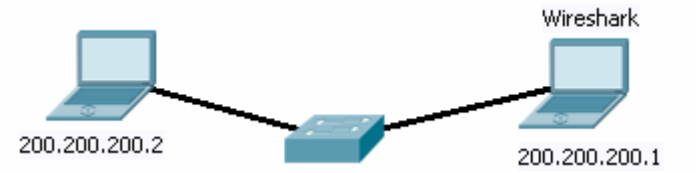
COMPUTER NETWORKS - LABORATORY 001

Topics:
Network traffic analysis.

Task A: Basic datagrams in IP networks

Prepare a packet tracking program your computer (e.g. Ethereal or Wireshark). After running it - configure the tracked network interface of the computer and enable datagram tracking. Prepare two computers by configuring Ethernet interface addresses so that they are in the same IP network segment.



1. Ethernet frame analysis

In an example caught analyze the content of the Ethernet frame:
- Pay attention to the source and destination MAC address field
- Pay attention to frame length limits
- Check the protocol identifier encapsulated in the frame

2. ARP query packets and ARP responses

Execute an ARP session in the local network and capture its results for analysis. To do this, after enabling packet tracing, delete the ARP table contents on one of the computers (in Windows using the arp -d command), force the packet to be sent to another computer with an unknown MAC address (ping). Check the contents of the MAC table in the PC station: arp –a
- Pay attention to the address fields in ARP packets (whether they're filled or not)
- Change one of the computer's IP addresses and observe the Gratitous ARP packet

3. Analyze any of IP packets caught (header fields), identifying:

- IP version (4?)
- Fragmentation and Fragmentation Shift
- TTL (time to live)
- Protocol number
- Source Address
- Destination address

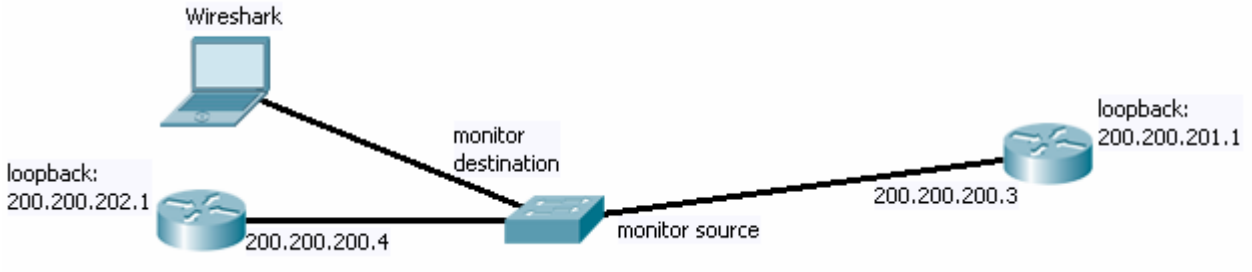
- Package Length
- Data in the package

Note the protocol type in the Ethernet frame: in case of an IP and ARP content.

Transmit a long Ip packet - several times longer than the MTU (Maximum Transmission Unit) value for the IS OSI layer 2 protocol used in the current network (in the case of Ethernet, the MTU will be 1500 bytes). After sending, carefully observe the fragmentation process of that IP packet (into IP datagrams). Sending the appropriate packet is possible, for example, by using the ping program with the -l (length) parameter added:
Ping –l 5000 200.200.200.2

Task B: Dynamic routing protocols in IP networks

To analyze the operation of dynamic routing protocols in IP networks it will be necessary to capture the traffic between IP routers (and redirect it to some computer containing a packet analyzer application). This can be done by using an Ethernet switch feature called “monitor session” or sometimes “port mirroring”. The network topology should be built according to the figure below (Wireshark is a packet analyzer app):



Configure the switch to forward copies of Ethernet frames received via some the monitored port (connected to one of the routers) to another port (going to the computer with Wireshark enabled):

Switch(config)# monitor session 1 source interface fa 0/1 rx
Switch(config)# monitor session 1 source interface fa 0/1 tx
Switch(config)# monitor session 1 destination interface fa 0/2

where fa 0/1 is the interface going to one of the routers and fa 0/2 - to the monitoring computer (PC). The PC will now receive a copy of all communications carried out between the routers inone direction.

1. RIP dynamic routing protocol
   Run the RIP protocol on the routers and then check:

- what protocol is used in ISO OSI layer 3 and 4,
- what are the IP addresses used in communication,
- how often subsequent packets are send after the connection has established,
- what does the content of the package look like

2. RIPv2 dynamic routing protocol

Run RIP version 2 (RIPv2) on your routers and then check:

- what protocol is used in ISO OSI layer 3 and 4,
- what are the IP addresses used in communication,
- what does the content of RIP packets look like,
- how the packet content changes after enabling router authentication

3. EIGRP dynamic routing protocol
   Enable the EIGRP protocol on the routers and then check:

- what protocol is used in ISO OSI layer 3 and 4,
- what are the IP addresses used in communication,
- what does the content of EIGRP packets look like,
- how the IP frame changes when you explicitly specify EIGRP neighbors (instead of using broadcasts)

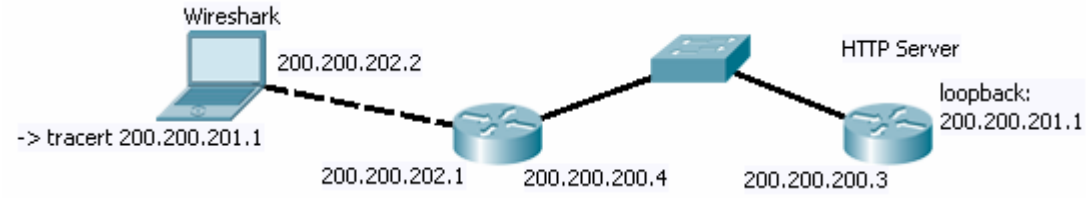
4. OSPFS dynamic routing protocol
   Start OSPF protocol and check:

- what protocol is used in ISO OSI layer 3 and 4,
- what are the IP addresses used in communication,
- what does the package content look like,

In UDP datagrams sent over OSPF locate the following fields:
- source port
- destination port
- data
- LSA Message Type

Task C: Network diagnostics tools

Build a network topology involving at least three IP network segments.



1. ICMP protocol operation

The most user-visible variant of the ICMP (Internet Control Message Protocol) packet is sent by the “ping” diagnostic program (Echo Request and Echo Reply).

- send several packets to a known IP address and analyze the packet contents (echo and response). locate the type field in the ICMP packet. Note the difference between the request and the response

- check the protocol number in the IP packet (for ICMP)

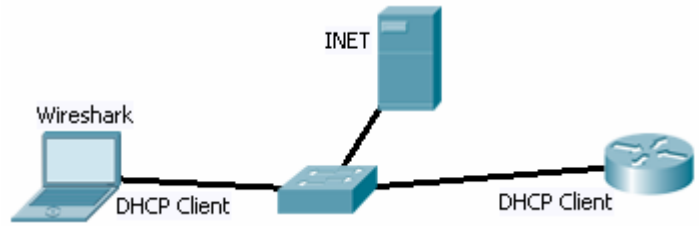
- send an ICMP Echo Request to a non-existent IP network and observe the response content (ICMP Network Unreachable)
- send an ICMP Echo Request to a non-existent host in an existing IP network and also observe the response content (ICMP Host Unreachable).
-

2. Traceroute operation

Run a traceroute program from on computer to the furthest available IP network. Then analyze the contents of communication carried out within the traceroute test, paying special attention to the TTL field values in all the packets sent by traceroute. Check the contents of router responses (what kind of ICMP packets are they?)

Task D: Network Services

In the current experiment there are network services needed. Use a router to implement some or alternatively - any server host located in the Internet. The computer should be used as a client to these services - with network traffic analysis tool enabled on it.



1. TELNET connection

Start the TELNET service on a router:

Router(config)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#transport input telnet

Then open a TELNET session from the computer to the router (server). After logging in and exchanging a few messages – disconnect the session. Observe the individual steps of the TCP connection establishment process (SYN, SYN ACK, ESTABLISHED, CLOSING etc.), and then:

- capture TELNET login and password
- check the protocol number in the IP packet (indicating TCP)
- locate the fields in the TCP packet: source port, destination port, sequence number and acknowledgements: identify a TCP fragmentation process example and track the values of subsequent sequence numbers during some longer transmissions.

Additionally, attempt to TELNET using a TCP port on which the TELNET service is not

available. What ICMP message do we receive from the router?

2. HTTP and HTTPS connection

On a router start the HTTP and HTTPS service

Router(config)#ip http server

Router(config)#ip http secure-server
Router(config)#ip http authentication local
Router(config)#username network privilege 15 password 0 network

Open HTTP session using a web browser on computer (to the router). After logging in and exchanging a few messages, disconnect the session. Observe the individual steps of HTTP session and analyze the contents of packets caught (request, reply, HTTP error codes, content-type, etc.).

3. SSH connection

Run the SSH service on a router

Router(config)#aaa new-model
Router(config)#aaa authentication local
Router(config)#hostname host
Router(config)#ip domain-name domain
Router(config)#crypto key generate rsa
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#transport input ssh

Open the SSH session from a computer to the router. After logging in and exchanging some messages, disconnect the session. Observe any changes in the contents captured, comparing it with a TELNET session.

4. SSL Session

The network traffic recorded in a file related to a previously conducted SSL session can be decoded when we have the so-called (Pre)-Master-Secret log file, created by some tools during the SSL session.
Download the sample SSL network traffic and the associated (Pre)-Master-Secret log file from the following addresses:

https://bugs.wireshark.org/bugzilla/attachment.cgi?id=11612
and
https://bugs.wireshark.org/bugzilla/attachment.cgi?id=11616

(these are dump.pcap and premaster.txt files respectively)

In the Wireshark tool, open the dump.pcap file and then select the corresponding (Pre)-Master-Secret (premaster.txt) file in the Edit→Preferences→Protocols→SSL options. As

the SSL debug file option, you should also provide the name of a new file to which the information generated in the process of decoding the SSL content will be saved. In this output, search for the phrase "decrypted app data". The first line in this search text contains the frame number with the SSL content, which should be indicated in the Wireshark filter (these are the frames we are interested in), e.g.
frame.number==1234
Then, select any frame with the mouse and choose the “follow SSL stream” option.

For Firefox, you can generate the premaster.txt file yourself. However, you must set the SSLKEYLOGFILE environment variable as the path to the premaster.txt file you are creating and restart Firefox.

5. FTP service operation

Download some pre-generated ftp traffic captures from:

http://wiki.xplico.org/doku.php?id=pcap:pcap

or generate traffic based on some open ftp server, e.g. ftp://ftp.agh.edu.pl

Analyze the FTP protocol commands: USER, PASS, PWD, PASV + LIST (the server's response to the PASV request – 227 Entering Passive Mode Note: byte1,byte2,byte3,byte4,byte5,byte6 indicates that the server is switching to passive mode and will prepare the data transmission service at the IPv4 address: byte1,byte2,byte3,byte4 and on the port number 256*byte5+byte6.
Applying filtering to trace results: in the Filter bar of Wireshark, enter the following text: ip.addr == server_IP_address && tcp.srcport == port
Now in any frame with trace results you can right-click and select Follow TCP Stream from the context menu. After applying the filter, find the command in the stream: PASV + RETR /carlo/sgacimartin/universocercano.jpg
(or a command for another downloaded file) and select the Follow tcp stream option again.

6. DHCP

Release the IP address assigned by the DHCP server on the PC station. The Windows cmd command is:

ipconfig /release

and then renew the address with cmd command:

ipconfig /renew

Check what Layer 3 and 4 protocols are used to communicate to obtain an IP address and what address was used for configuration. Also check the DHCP options selected in the DHCP request packets.

7. DNS Service

In the Windows cmd enter the following command to clear the DNS cache:

ipconfig /flushdns

Then select any page in the web browser and analyze the DNS traffic between the computer and DNS server. Instead of a WWW browser, you can use the DNS client tool available in the Windows operating system:
nslookup sieci.kis.agh.edu.pl

Check the status of the local DNS resolver registry:

ipconfig /displaydns

Determine what Layer 4 protocol is used to communicate with the DNS server, how the operating system finds out the IP address of the server it looks for and what does the AAAA, A, CNAME, MX response/query mean?
You can (alternatively) perform this analysis on some ready DNS traffic captures, downloaded from:

https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=dns.cap

8. POP3 and SNMP services

Check some traffic for the POP3 service in Wireshark app downloaded from:

http://wiki.xplico.org/lib/exe/fetch.php
?media=pcap:xplico.org_sample_capture_pop3_must_use_xplico_nc.cfg.pcap

Analyze the POP3 protocol commands: USER, CAPA, PASS, LIST, UIDL, RETR, QUIT (these commands can be found with a filter, e.g. pop.request.command == CAPA)

Download check a traffic conducted within the SMTP service in Wireshark:

https://wiki.wireshark.org/SampleCaptures ?action=AttachFile&do=get&target=smtp.pcap

Analyze the SMTP protocol commands: AUTH LOGIN, MAIL FROM, RCPT TO, DATA, QUIT.